NATIONAL ASSOCIATION OF INSURANCE COMMISSIONERS

Draft date: 10/01/26

Virtual Meeting

INFORMATION TECHNOLOGY EXAMINATION (E) WORKING GROUP
October 8, 2026
12:00 – 1:00 p.m. ET / 11:00 a.m. – 12:00 p.m. CT / 10:00 – 11:00 a.m. MT / 9:00 – 10:00 a.m. PT

ROLL CALL

Ber Vang, Chair	California	Kim Dobbs	Missouri
Shane Mead, Vice Chair	Kansas	Andrea Johnson	Nebraska
Chris Erwin	Arkansas	Wayne Longmore	New York
Ken Roulier / Michael Shanahan	Connecticut	Colton Schulz	North Dakota
Ricardo Mancilla	Illinois	Metty Nyangoro	Ohio
Jerry Ehlers	Indiana	Eli Snowbarger	Oklahoma
Dmitriy Valekha	Maryland	Diana L. Sherman	Pennsylvania

NAIC Support Staff: Travis Lenz/Elise Klebba

AGENDA

1. Consider Exposure of Handbook Updates – *Shane Mead (KS)*
    a. Exhibit C – Part Two Evaluation of Controls in Information Technology (IT) Work Program — Attachment 1
    b. Exhibit C – Part Three Prospective Cyber Risk Evaluation of Controls Work Program — Attachment 2
    c. Corresponding Handbook Updates — Attachment 3

2. Discuss Any Other Matters Brought Before the Technical Group – *Shane Mead (KS)*

3. Adjournment

© 2026 National Association of Insurance Commissioners

PART TWO – EVALUATION OF CONTROLS IN INFORMATION TECHNOLOGY (IT) WORK PROGRAM – ALIGN, PLAN, AND ORGANIZE (APO)

Risk Stmt #	Risk Statement	Ctrl #	Control Objective Identifier	Common Controls	Preliminary Information Request	Possible Test Procedures
APO 01	IT organizational structure and staffing is inadequate to support business objectives.	APO 01.01~~3~~-APO 01.02~~4~~	A	The company has established and communicated IT standards to ensure consistency and to drive compliance across the organization.	Provide IT policies and procedures, including security, HR policies and IT training program documentation, including for specialized roles such as cybersecurity professionals.	Assess policies and procedures to ensure currency and completeness. Determine whether IT security is embedded in HR policies for all employees. Review training programs and schedules to confirm that management and employees, as well as those in specialized roles, are provided with sufficient training to understand the importance of compliance with IT and cybersecurity policies, including awareness of concepts of phishing, malware, and data loss prevention, as appropriate. ~~Assess the level of security awareness throughout the organization, including the awareness of the board of directors and senior management, as appropriate to their distinct roles.~~
		APO 01.03~~1~~ – APO 01.05~~2~~	B	The company's IT management organizational structure, with clearly defined roles and responsibilities, supports business objectives and IT priorities (including cybersecurity)	Provide the IT organization chart showing job title and names of IT executives and managers and reporting lines to CEO and the BOD. Provide job descriptions for key IT positions, including	Review and assess adequacy of IT governance model. Review and assess adequacy of cybersecurity staffing and/or resources. Consider segregation of duties and clearly defined roles and responsibilities.

Commented [TH1]: This and other comments in my name are sourced from a drafting group member who worked on Part 3.

Also covered in Risk 3 in Part 3:

GV.PO-01: Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced.

GV.PO-02: Policy for managing cybersecurity risks is reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission.

Commented [TH2]: Also covered in new APO 7 entry below

Commented [TH3]: Cybersecurity staffing is included in Risk 2:

GV.RR-02: Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced.

GV.RR-03: Adequate resources are allocated commensurate with the cybersecurity risk strategy, roles, responsibilities, and policies.

© 2026 National Association of Insurance Commissioners

Risk Stmt #	Risk Statement	Ctrl #	Control Objective Identifier	Common Controls	Preliminary Information Request	Possible Test Procedures
				and enables efficient decision-making.	cybersecurity, plus resumes or biographical information for incumbents of those positions. Provide a list of IT governance committees (e.g., IT strategy, steering committees, etc.)	Review IT governance committees to determine whether business is adequately represented to facilitate IT priorities in supporting business objectives.
APO 02	Enterprise business objectives cannot be attained due to the development of an IT strategy that is inadequate, ineffective and not in alignment with business objectives, including inadequate management oversight over the achievement of the IT strategy.	APO 02.01-APO 02.05	A	The IT strategic planning processes considers the current enterprise environment and business processes, as well as the enterprise strategy and future objectives. Additionally, consideration is given to the external environment of the enterprise (e.g., industry drivers, relevant regulations, basis for competition).	Provide copies of IT strategic plans and evidence of strategic planning meetings, including membership, attendance, agendas and minutes.	Verify that strategic plans are developed by an IT steering committee (or its equivalent) with adequate input and involvement of IT management and key executive personnel from all significant business units. Interview senior IT personnel and review the IT strategic plan development process to understand how the IT strategic plan is developed and updated in alignment with the business. Interview IT steering committee members to verify the following: 1) The strategic IT plan is consistent with business objectives. 2) Contributing committee members are aware of corporate short-term and long-term goals. 3) The IT strategic plan is based on a current understanding of systems, including input from stakeholders.

© 2026 National Association of Insurance Commissioners

Risk Stmt #	Risk Statement	Ctrl #	Control Objective Identifier	Common Controls	Preliminary Information Request	Possible Test Procedures
						4) Risk and cost/resource implications of the required IT capabilities were considered.
APO 03	Enterprise goals may not be met because the data and systems architecture is poorly defined and/or fragmented.	APO 03.01 – APO 03.03, APO 03.05	A	The company has an information architecture model that addresses the creation, use and sharing of data between applications that maintain data integrity, flexibility, functionality, cost-effectiveness, timeliness, security and availability.	Provide documentation to support the company's information architecture model and the associated standards.	Review the information architecture model and verify that the model considers all significant business processes, including user-developed applications such as spreadsheets and Access databases. Compare the information architecture model to the system summary grid to verify that all significant areas are addressed. Review the information architecture model to verify that the company has created standards that address data integrity, flexibility, functionality, timeliness, cost-effectiveness, availability, and security between applications.
					Provide a copy of the membership, agendas, and minutes of the meetings of the information architecture board.	Review membership, agendas and minutes of the Information Architecture Board to verify that they are involved in the oversight of technology.
APO 04	Company operations may lack efficiency and competitive advantage because system technology is	APO 04.02	A	The company has an IT steering committee (or equivalent) that provides direction and input to IT for system and application solutions.	Provide a copy of the membership, agendas, and minutes of the meetings of the IT steering committee.	Review membership, agendas and minutes of the IT steering committee to verify that they are exercising the appropriate oversight of IT, including prioritization of IT investments and consideration of innovation.
		APO 04.04 – APO 04.06~~5~~	B	The company has a technology advisory board (or equivalent) that	Provide a copy of the membership, agendas and minutes of the meetings of	Review membership, agendas and minutes of the technology advisory board to verify that they are providing

© 2026 National Association of Insurance Commissioners

Risk Stmt #	Risk Statement	Ctrl #	Control Objective Identifier	Common Controls	Preliminary Information Request	Possible Test Procedures
	obsolete and poorly aligned with business objectives.			identifies and monitors emerging technologies and/or other IT innovations.	the technology advisory board.	information on emerging technologies and other IT innovations, as well as evaluating and monitoring the results of proof of concept initiatives.
APO 06	The IT budget and expense allocation are~~is~~ not representative of the organization's goals and business needs~~, and IT expenses are not properly allocated~~.	APO 06.01 - APO 06.05	A	The IT budget is developed based on strategic plan initiatives and representative of industry best practices and industry peers.	Provide evidence that the IT budget is based on supporting the strategic plan and industry best practices.	Review budget documentation to verify consistency with the IT strategic plan and industry best practices. Interview senior IT management to verify that the IT budget is created based on the IT strategic plan. Determine if a chargeback system exists and verify that the IT costs appropriately transfer to business units for IT services rendered.
			B	The company has a formal budget monitoring process to identify and address budget variations.	Provide evidence of the budget monitoring process.	Review company documentation to verify that the company is adequately monitoring IT costs, service levels, and service improvements.
					Provide a copy of the budget variance report, or similar document.	Review the company's budget and variance explanations for reasonableness. Identify whether the variances were the result of control deficiencies that need to be addressed.
APO 07	The insurer does not foster an atmosphere of IT security in general, and individuals do not recognize IT security	APO 07.03	A	The Company promotes an enterprise-wide culture of IT security through implementation of a consistently applied IT security awareness training program.	Provide a copy of the policies and procedures relating to security awareness training and phishing simulation. Provide a list of high-risk targeted courses presented over the past 12 months and	Verify the effectiveness of the IT security awareness training program. 1) Verify that all active personnel complete mandatory training within deadlines and regularly recurring training at least annually. 2) Verify that the company assesses user interactions (email opens, malicious link

© 2026 National Association of Insurance Commissioners

Risk Stmt #	Risk Statement	Ctrl #	Control Objective Identifier	Common Controls	Preliminary Information Request	Possible Test Procedures
	concerns and respond accordingly.				the personnel participation rosters.	clicks, and credential submissions) to identify user vulnerabilities and track failure rates. 3) Verify that the technical reporting mechanism is in place. 4) Verify that the company has remedial provisions for repeat simulation failures.
APO 09	IT-enabled services and internal service levels are not managed to ensure that IT services align with enterprise needs and expectations.	APO 09.01-APO 09.05	A	The company has a defined framework that provides a formalized service level management process between the customer and service provider. The framework should: 1) Provide for the creation internal service level agreements (SLAs) that formalize IT services provided, including performance measures. 2) Provide for continuous alignment with business requirements. 3) Include processes and procedures such as monitoring of availability, reliability, performance, capacity for growth, levels of support, continuity planning, security and demand restraints.	Provide a copy of policies and procedures relating to support provided for IT services.	Verify that the performance standards are being achieved. For performance standards that are not met, ensure that there is a proper resolution process.
					Provide a listing of internal SLAs, supporting IT services provided to business customers.	Select a sample of SLAs from the listing obtained. Inspect and verify SLA policies and procedures to ensure that agreements: 1) Are approved by responsible company personnel. 2) Contain measurable performance standards. 3) Align SLA objectives and performance measures within business objectives and IT strategy. Ensure that SLAs are reviewed and revised when needed.

Formatted: Centered

Risk Stmt #	Risk Statement	Ctrl #	Control Objective Identifier	Common Controls	Preliminary Information Request	Possible Test Procedures
				4) Ensure that regular reviews of SLAs and supporting contracts are performed to ensure that formalized IT services are being provided.		
APO 10	Third-party service provider risks are not properly assessed, addressed, and mitigated.	APO 10.01 - APO 10.05	A	The company has a formal process in place to manage all vendors and affiliated service providers~~service providers~~. The company creates formal agreements with the vendor or affiliated service providers ~~service provider~~ to identify roles and responsibilities, expected deliverables, performance standards and credentials. Contracts conform to business standards in accordance with legal, regulatory, and/or statutory requirements. Nondisclosure agreements, escrow accounts and conformance with security requirements are included as considered necessary.	Provide a copy of the company's vendor-management policies and/or procedures. Provide a list of third-party service providers (suppliers), including the type of services provided, their significance and criticality.	Inspect a sample of third-party provider contracts (agreements), including those who are considered affiliated service providers~~s~~ or significant to the company, SLAs and other documentation to ensure that the contracts: 1) are current; 2) have been properly approved and correspond with the company's policies and procedures; and 3) conform to business, legal and regulatory requirements. Through review of company policies and procedures, along with interviews of staff, verify that the company adequately addresses ownership or relationship management responsibilities for ensuring that the outside service provider continues to be viable, and that contracts are maintained, monitored and renegotiated as required to continuously meet business requirements.

© 2026 National Association of Insurance Commissioners

Risk Stmt #	Risk Statement	Ctrl #	Control Objective Identifier	Common Controls	Preliminary Information Request	Possible Test Procedures
			B	Reviews ~~are~~ performed on ~~outside service providers~~ vendors during the contracting process to evaluate the appropriateness and effectiveness of their control environment (including cybersecurity).	Provide details of vendor risk reviews performed during the vendor selection or contracting process.	Review available reports to help verify that the company reviews the effectiveness of ~~service provider~~vendor controls. Consider the impact of any exceptions identified.
			C	The company has a formal process in place whereby: 1) An inventory of the company's vendors and affiliated service providers~~service providers~~ is completed and maintained and includes information concerning their risk and their material adverse impact to the business, operations, or security. 2)~~-~~ Risk is assessed based on the company's understanding of the ~~third-party~~affiliated service providers information security program as well as by the company's ability to verify elements of the ~~third-party~~affiliated service provider's security program and the data exposed to	Verify an inventory of vendors and ~~service providers~~vaffiliated service providers is created and maintained and includes sufficient information to group and classify providers based on both risk and material adverse impact to the business, operations, or security. Provide a summary of the company's ~~third-party~~ affiliated service provider management process. Provide copies of the most recent SOC 2 and SLA reports for significant affiliated service providers.	Review the company's third-party vendor and ~~service~~ affiliated service provider management process including consideration of: 1) Whether the listing of third-party service providers is comprehensive and complete; 2) Whether the listing considers both risk and material adverse impact in classifying or grouping; 3) Whether the company, service, or program has appropriately determined access rights based on its risk assessment and material adverse impact; and 4) Whether the company has designed appropriate controls that are consistent with the company's classifying or grouping. Review SOC 2 and SLA reports for significant affiliated service providers to determine whether management has identified implemented, and monitored

Commented [TH4]: Also included in Risk 5 of Exhibit C Part 3:

GV.SC-06: Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships.

(Note that this specific common control is on the control environment, not the business.)

© 2026 National Association of Insurance Commissioners

Risk Stmt #	Risk Statement	Ctrl #	Control Objective Identifier	Common Controls	Preliminary Information Request	Possible Test Procedures
				the third party, such as PFI, PHI, and PII; 3) Material adverse impact to the business, operations, or security is assessed based on mission function, and availability of alternatives. 4) Based on the company's risk and material adverse impact to the business, operations, or security, the company groups and classifies vendors and uses a vendor's ranking to determine depth and frequency of review procedures performed related to ongoing vendor relationships (e.g., reviews SOC reports or equivalents); 5) The company determines appropriate access rights, based on the risk assessment and company needs; 6) The company designs specific mitigation strategies, including network monitoring specific to ~~third-party service providers~~ vendors		applicable user entity control considerations.

Commented [TH6]: Also included in Part 3:

GV.SC-07.3: Verify that critical suppliers are monitored to ensure that they are fulfilling their security obligations throughout the supplier relationship lifecycle using a variety of methods and techniques, such as inspections, audits, tests, or other forms of evaluation.

© 2026 National Association of Insurance Commissioners

Risk Stmt #	Risk Statement	Ctrl #	Control Objective Identifier	Common Controls	Preliminary Information Request	Possible Test Procedures
				and affiliated service providers, and access controls, where appropriate.		
APO 12	IT-related enterprise risks have not been integrated into the overall enterprise risk management (ERM) program.	APO 12.02 – APO 12.05	A	The company maintains a documented and functioning ERM program that identifies IT-related enterprise risks.	Obtain copies of the ERM program.	Review the ERM program to determine IT integration. Interview IT senior management to verify that an IT risk and control framework has been adopted throughout the organization and to verify that appropriate reports relating to adoption of the framework have been provided to the board of directors or a committee of the board, as appropriate.
			B	An IT risk profile is actively maintained describing known risks and risk attributes and of related resources, capabilities and current control activities.	Provide the company's IT risk profiles. Obtain a copy of the most recent risk assessment.	Review risk profile and assessments for timely and relevant information on the organization's most significant IT risks, including cybersecurity and third-party risk, and subsequent mitigating controls. Determine whether threats and vulnerabilities identified through information -sharing forums are periodically assessed and incorporated into the risk profile.
			C	There is c~~C~~ontinual communication on the current state of IT-related exposures and opportunities.	Obtain risk analysis and risk profile reports provided to all stakeholders.	Review evidence that the company is providing risk-analysis information to stakeholders to communicate the current state of significant IT risks and the adequacy of risk response. Assess management awareness of risk analysis and risk profile reports and, if applicable, review and/or verify initiatives

Commented [TH5]: This one isn't as clear. We have a lot in Risk 5, but that focuses on the cyber aspect, whereas this part should focus on the business aspect. This is one where we may want to keep this entire part and then reference it in Exhibit C Part 3, with potentially more work to be performed in Exhibit C Part 3.

© 2026 National Association of Insurance Commissioners

Risk Stmt #	Risk Statement	Ctrl #	Control Objective Identifier	Common Controls	Preliminary Information Request	Possible Test Procedures
						as a result of IT-related exposures and opportunities.
			D	The company maintains an enterprise IT architecture governance program that mandates predefined solution standards, documents all intentional deviations as tracked risks, and allocated operational resources to retire legacy infrastructure, administrative systems, databases, configurations, or out-of-support dependencies across all deployed IT systems-.	Provide documentation supporting the identification, monitoring, and remediation of technical debt. Provide documentation supporting approved risk acceptances, compensating controls, or extended support agreements related to legacy or unsupported technologies.	Verify the company identifies, tracks, prioritizes, and remediates technical debt, including deferred upgrades, architectural deviations, legacy systems, and end-of-support technologies. Determine whether management has implemented appropriate remediation plans, compensating controls, or approved risk acceptances for identified technical debt. For a sample of identified technical debt items, verify associated security and operational risks have been evaluated, and mitigating controls, extended support agreements, or replacement plans have been implemented, where appropriate.
APO 14	The company does not effectively manage its data across the data life-cycle.	APO 14.01	A	The company defines and communicates its data management strategy, roles, and responsibilities.	Provide a copy of the data management strategy, policies, and procedures. Identify personnel filling identified roles and responsibilities.	Review the policies and procedures for completeness. Obtain organizational charts and job descriptions for personnel with responsibilities for data management.
		APO 14.08 – 14.09	B	The company has established data protection policies and procedures in place to support data confidentiality, integrity,	Provide a copy of the company's policies or procedures to protect data ~~in use~~ from unauthorized access, modification, or denial of availability.	Review the procedures for production data encryption, access controls, or data masking techniques in use.

© 2026 National Association of Insurance Commissioners

Risk Stmt #	Risk Statement	Ctrl #	Control Objective Identifier	Common Controls	Preliminary Information Request	Possible Test Procedures
				and availability, including data at rest, in transit, and in offline storage.		
			C	The company has established and adheres to data archival and retention policies and procedures.	Provide a copy of the company's data archival and retention policies and procedures.	Review company documentation to verify that there are data archival and retention policies in place. Review company documentation to verify that the company follows its data archival and retention policies.

PART TWO – EVALUATION OF CONTROLS IN INFORMATION TECHNOLOGY (IT) WORK PROGRAM – BUILD, ACQUIRE, AND IMPLEMENT (BAI)

Risk Stmt #	Risk Statement	Ctrl #	Control Objective Identifier	Common Controls	Preliminary Information Request	Possible Test Procedures
BAI 01	IT projects may fail to meet business objectives/ERM goals ~~or run over budget~~ in the absence of an effective program and	BAI 01.01–BAI 01.08, BAI 1~~0~~1.1~~15,~~ ~~BAI 01.07–BAI 01.10, BAI 01.12, BAI 01.14~~	A	A methodology exists to maintain the portfolio of projects that includes identifying, defining, evaluating, prioritizing, selecting, initiating, managing and controlling projects.	Provide a copy of the existing IT project-management and System Development Life Cycle (SDLC) methodologies.	Review the project life cycle and SDLC methodologies and verify that it addresses the key aspects of projects, including responsibilities, project plans, project resources, timeliness, deliverables, approval requirements, benchmarking based on key indicators (including risk management and project quality plans) and post-implementation reviews.

Formatted Table

Formatted Table

Risk Stmt #	Risk Statement	Ctrl #	Control Objective Identifier	Common Controls	Preliminary Information Request	Possible Test Procedures
	project-management methodology.					Review a sample existing project to verify adherence to the project-management standards and methodology.
BAI 02	Projects are initiated without proper authorization and/or analysis.	BAI 02.01–BAI 02.03	A	The company has a defined process to identify and approve automated solutions, which include business functional and technical requirements, risk analysis reports and feasibility studies.	Provide evidence that business functional and technical requirements, risk analysis reports and feasibility studies are appropriately considered in the project approval process.	Evaluate the documentation received from the company for existence, approval, timeliness and appropriateness.
					Provide evidence of IT procurement policies and procedures.	Review the company's IT procurement policies and procedures to verify that management approval, cost justification, business suitability needs, legal review of contractual issues and viability of the vendor are addressed.
					Provide a listing of recently completed projects that have been created or acquired within the past 18 months.	Select a significant project(s) to verify that documentation supports the process defined by the company. Gain an understanding of the process and verify whether it appears reasonable. Verify that the company's process requires cost/benefit analyses be adequately reviewed by project stakeholders and senior management. For a selected significant development project(s), verify the completeness,

© 2026 National Association of Insurance Commissioners

Formatted Table

Risk Stmt #	Risk Statement	Ctrl #	Control Objective Identifier	Common Controls	Preliminary Information Request	Possible Test Procedures
						timeliness and reasonableness of the cost justification and related project approval.
		BAI 02.04	B	Senior management and other stakeholders approve project plans before work commences on each significant phase of the development process used for all automated solutions.	Provide evidence of management approval for project plans.	From the project(s) selected above, verify that senior management and other stakeholders approved work prior to commencement of each significant phase of the development process.
BAI 03	Project deliverables fail to meet business objectives due to inadequate design and/or ineffective oversight of implementation.	BAI 03.01	A	Design specifications translate proposed solutions into business processes, supporting services, applications, infrastructure and information repositories capable of meeting business and enterprise architecture requirements. Quality assurance, project stakeholders and the sponsor/business process owner approve final designs, based on agreed-on criteria.	For significant programs and projects selected by the examiner, provide copies of design specifications.	Review the significant programs and projects selected by the examiner and determine whether the design specifications are approved by management and whether business and enterprise architecture requirements are addressed. Review the quality assurance support for appropriate approval, based on agreed-upon criteria. Verify that the system design includes specification of transaction types and business processing rules, automated controls, data definitions/business objects, use cases, external interfaces, design constraints and other requirements. Verify that the tools used to monitor costs are effective and properly used. Verify that the cost-monitoring process is adequately comparing actual hours and expenses to budgeted amounts.

© 2026 National Association of Insurance Commissioners

Formatted Table

Risk Stmt #	Risk Statement	Ctrl #	Control Objective Identifier	Common Controls	Preliminary Information Request	Possible Test Procedures
		~~BAI 03.02~~		~~Programs and projects are designed to address system redundancy, recovery and backup, and provide for the ability to audit transactions and identify root causes of processing errors.~~	Provide documentation to evidence the existence of adequate business continuity, recovery and backup plans.	Determine if the company has adequate business continuity, recovery and backup plans. Select a sample of significant programs and projects and verify that the ability to audit transactions and identify the root cause of processing errors exists.
		BAI 03.05	B	Business and IT solution components, ~~and~~ information repositories, and software are integrated and configured in line with detailed specifications and quality requirements. The role of users, business stakeholders and process owners are considered in the configuration of business processes. Audit trails are implemented during configuration and integration of hardware and infrastructural software to protect resources and ensure availability and integrity. ~~Acquired application software is configured to meet business processing requirements.~~	Provide a listing of automated controls that provide for accurate, complete, timely, authorized and auditable processing.	Determine if programs and system are configured to allow for accurate, complete, timely, authorized and auditable processing.
					Provide the company's data classification, information architecture, information security architecture and risk tolerance guidelines.	Review the company's data classification, information architecture, information security architecture and risk tolerance guidelines. Assess if system configuration provides for availability and integrity.
					Provide the company's development procedures and standards guidelines that address items such as procurement process and acquisition strategy, hardware, software and services, etc.	Validate that IT procurement procedures address the services needed by the business, while also meeting security requirements.
		BAI 03.06	C	The company has a quality assurance (QA) process to review software to ensure that business requirements are met.	For a sample of significant programs and projects selected by the examiner, provide	Review the software QA practices relative to program and system development to ensure related processes align with the organization's QA practices.

© 2026 National Association of Insurance Commissioners

Formatted Table

Risk Stmt #	Risk Statement	Ctrl #	Control Objective Identifier	Common Controls	Preliminary Information Request	Possible Test Procedures
					evidence and documentation of the QA function.	Review documentation of the software QA process for appropriateness. Review the detail QA testing for adherence with company standards.
		BAI 03.07–BAI 03.08	D	Integrated test plans and practices are commensurate with the enterprise environment and strategic technology plans. The company has secure pre-production development environments to maintain security throughout the software development life-cycle.	Provide evidence that would support the use of integrated testing and strategic technology plans. Provide a copy of the company's policies and procedures, including security, for pre-production environments.	Validate that integration test plans and practices enable the creation of suitable testing and simulation environments. Validate that the pre-production environments adequately support the application requirements and mirror real-world conditions, including the business processes and procedures, range of users, transaction types and deployment conditions. Review completed test work to determine if security test plans were followed in accordance with standards.
		BAI 03.08	E	The company performs testing in accordance with its defined plan, prior to migration to the production environment. Testing outcomes are recorded and the results communicated to stakeholders in accordance with the test plan.	For a sample of the significant programs and project selected by the examiner, provide evidence that supports the completed test plans and related stakeholder communications.	Review the completed test documentation to ensure that plans were followed and that business process owners and end users participated in the testing.
BAI 04	Systems fail to meet current and future business needs	BAI 04.01	A	The company has established a planning and review process for continuous performance and capacity monitoring of IT resources.	Provide a copy of the policies and procedures regarding performance	Review policies and procedures and interview key staff members involved in the development of the performance and capacity plan to verify that the appropriate

© 2026 National Association of Insurance Commissioners

Formatted Table

Risk Stmt #	Risk Statement	Ctrl #	Control Objective Identifier	Common Controls	Preliminary Information Request	Possible Test Procedures
	due to inadequate planning for capacity, cybersecurity events, performance, and availability.			Management ensures that contingency plan procedures are in place to properly address availability, capacity, cybersecurity events, and performance of individual IT resources.	and capacity management.	elements (e.g., customer requirements, business requirements, cost, application performance requirements and scalability requirements) were considered during the development of the plan. Inquire of key staff members as to whether emergency problems have occurred in the recent past and, for those instances (if any), verify compliance with the contingency plan procedures and verify that they were effective.
		BAI 04.02	B	Solutions and services that are critical in the availability and capacity management process are evaluated as part of business impact analysis procedures.	Provide evidence to support the completion of business impact analysis procedures for key business units.	Verify that business impact analysis procedures for critical systems have been recently performed. Assess the results of these procedures to determine if business needs (performance and capacity) are being adequately addressed.
				Scenarios are defined and evaluated to address the likelihood that the systems' availability performance objective will not be achieved. The business line, function and regional leaders evaluate the impact of recovery scenarios on the business performance measures (e.g., revenue, profit, customer services).	Provide copies of the company's business continuity plan, disaster recovery and IT contingency plans.	Review the company's business continuity and disaster recovery plans. Verify that the IT continuity framework provides for: 1) Continuity management. 2) Defined roles, tasks and responsibilities of management, and internal and external service providers. 3) The ability to document, test and execute the disaster recovery and IT contingency plans. 4) Identification of critical resources, noting key dependencies. 5) Monitoring and reporting of the availability of critical resources, alternative processing. 6) The principles of backup and recovery.

© 2026 National Association of Insurance Commissioners

Formatted Table

Risk Stmt #	Risk Statement	Ctrl #	Control Objective Identifier	Common Controls	Preliminary Information Request	Possible Test Procedures
		BAI 04.03	C	Capacity and performance plans are updated and reviewed by management periodically, and define current and forecasted performance, and are used for service trend analysis.	Obtain capacity and performance plans, including modeling techniques that define current and forecasted performance, capacity and throughput of the IT resources. Obtain evidence of periodic update and review by management.	Determine if a review of capacity and performance plans is performed. Assess if the review considers cost-justifiable capacity and performance based upon agreed-upon workloads, as determined by the SLAs.
		BAI 04.04	D	The IT operations team performs trend analysis reporting and provides management with monitoring and reporting information for availability, performance and capacity workload of all information-related resources.	Provide trend analysis reports that identify any significant issues and variances.	Validate the effectiveness of continuous monitoring efforts through the review of IT management's use of trend analysis reports.
		~~BAI 04.05~~		~~The company maintains vendor product manuals that define: 1) an appropriate level of performance availability for peak processing and workloads; 2) corrective actions (e.g., shifting workload, prioritizing tasks or adding resources, when performance and capacity issues are identified); and 3) escalation procedures for swift resolution in case of emergency capacity and performance problems.~~	~~Provide capacity and performance reports and vendor manuals that take into account aspects such as normal workloads, contingencies, storage requirements and IT resource life cycles.~~	~~Review and assess items obtained for definition of corrective actions, appropriate level of performance availability and adequacy of escalation procedures.~~

© 2026 National Association of Insurance Commissioners

Risk Stmt #	Risk Statement	Ctrl #	Control Objective Identifier	Common Controls	Preliminary Information Request	Possible Test Procedures
BAI 06 & 07	A lack of proper change management threatens system stability and/or integrity.	BAI 06.01, BAI 06.03–BAI 06.04	A	The company has a process in place to record, authorize, manage, monitor and implement requests for application and infrastructure changes. ~~Procedures exist to ensure documentation is appropriately updated and distributed to affected users and IT staff upon completion of change.~~	Provide documentation regarding the company's change-management process, including copies of any forms used in this process. Provide documentation of how management monitors open change requests. Provide a current list of completed change requests, during the period under review.	Verify that the company's procedur a change request to be evaluated, authorized and tested. Review evidence of management's monitoring of open change requests. Select a sample of completed changes to verify that documentation of such items as requests, authorizations, business objectives, areas impacted, prioritizations, deliverable dates, change descriptions, deliverables, testing, back-out plans, closures and documentation are properly included in accordance with company standards.
		BAI 06.02	B	The company has a separate process in place to handle emergency changes.	Provide documentation regarding the company's process to handle emergency change requests. Provide a copy of any forms used in this process.	Verify that access to make emergency changes is revoked in a timely manner. Verify that the company completes a post-implementation review on all emergency changes.
		BAI 07.01	A	The company has established standards for an implementation and backout plan.	Provide procedures and guidelines for implementation. Provide procedures in the event of implementation failure.	Select a sample of completed projects and verify that the company has documented implementation and backout procedures that meet company standards.
		BAI 07.02	B	The company has a defined process to ensure data is converted accurately and completely.	Provide procedures detailing system and data conversion.	Verify that the conversion procedures ensure that data is converted accurately and completely and can be recovered.

Formatted Table

Formatted: Centered

© 2026 National Association of Insurance Commissioners

Formatted Table

Risk Stmt #	Risk Statement	Ctrl #	Control Objective Identifier	Common Controls	Preliminary Information Request	Possible Test Procedures
					Provide a listing of data conversion projects.	Select a sample of conversion projects and confirm that data was validated and converted accurately.
		BAI 07.04	C	The company has established a test environment that is representative of the production environment and takes into consideration security, workloads and data quality.	Provide a description of the development, test and production environments.	Verify that production, test and development environments are appropriately segregated. Verify that the test environment has appropriate physical and logical access controls. Verify that changes cannot be made to the code in the test environment. Verify that the data used in the testing environment meets the company's security requirements. Verify that there are required approvals to move objects from the development environment to the test environment.
		BAI 07.05	D	The company performs testing in accordance with its defined plan, prior to migration to the production environment.	Provide evidence of standard testing documentation, including copies of any forms used.	Select a sample of completed projects and verify that test plans and other testing evidence complied with testing standards and guidelines and were appropriately approved and review Verify that all relevant stakeholders are involved in the testing process and that changes were not implemented until the relevant stakeholders approved the testing results. Verify that testing performed considers security and performance (stress testing).

© 2026 National Association of Insurance Commissioners

Formatted Table

Risk Stmt #	Risk Statement	Ctrl #	Control Objective Identifier	Common Controls	Preliminary Information Request	Possible Test Procedures
		BAI 07.06	E	The company has controls in place to ensure that changes are released into production in accordance with the implementation plan.	Provide evidence of controls that ensure production release in accordance with the implementation plan	Review the company's implementation process. Select a sample of completed projects and verify that changes were released into production in accordance with the implementation plan.
		BAI 07.08	F	The company conducts a post-implementation review as outlined in its standards and as detailed in an individual implementation plan.	Provide evidence of post-implementation review procedures, including copies of any forms utilized in the process.	Review procedures to verify that a review is performed to address positives, negatives and lessons learned. Select a sample of completed projects and verify that the post-implementation review process is performed in accordance with company standards and the individual implementation plan.
~~BAI 08~~	~~Systems cannot be properly managed and optimized due to inadequate documentation and training.~~	~~BAI 08.01–BAI 08.04~~		~~The company has policies and procedures in place that require technical, operational and user documentation and training to be available for all significant systems~~ ~~The company provides training as part of system development, implementation or modification projects.~~	~~Provide evidence that appropriate technical, operational and user documentation and training is available for new system implementations or changes to existing systems.~~	~~For a sample of new or changed significant systems, verify that a training plan is incorporated into the project plan and that technical, operation and user documentation and training is provided by appropriate personnel.~~
BAI 10	A lack of configuration management threatens system stability, integrity and recovery.	BAI 10.01–BAI 10.05	A	The company has procedures in place over configuration management, which includes establishing and monitoring baselines for every system and service, in addition to the logging of any changes.	Provide a copy of policies, procedures and guidelines for configuration management.	Verify that senior management sets scope and measures for configuration management functions and assesses performance. Verify that a tool is in place to enable the effective logging and monitoring of configuration management information.

© 2026 National Association of Insurance Commissioners

Risk Stmt #	Risk Statement	Ctrl #	Control Objective Identifier	Common Controls	Preliminary Information Request	Possible Test Procedures
						Verify that configuration baselines for components are up-to-date, as defined and documented. Verify that configuration management data match the procurement records. Verify that a policy is in place to ensure that all configuration items are identified, maintained and in accordance with policy.
			B	Installed software is periodically compared to the policy for software usage to determine compliance with software licensing agreements or to identify the use of unauthorized software.	Provide information regarding the policies and procedures for, and results of, periodic reviews of software usage to the company's software policy and actual software licensing agreements.	Verify that periodic reviews are performed comparing software used to the company's policy for software usage to detect exceptions and the resolution of any discrepancies.

Formatted Table

PART TWO – EVALUATION OF CONTROLS IN INFORMATION TECHNOLOGY (IT) WORK PROGRAM – DELIVER, SERVICE, AND SUPPORT (DSS)

Risk Stmt #	Risk Statement	Ctrl #	Control Objective Identifier	Common Controls	Preliminary Information Request	Possible Test Procedures
DSS 01	The quality, timeliness and availability of business data is reduced due to an ineffective data-	DSS 01.01	A	All data expected for processing is received and processed completely, accurately and in a timely manner, and all output is delivered in accordance with business requirements.	Provide evidence of the controls that ensure all data expected for processing is available and processed completely and in a timely manner.	Interview company personnel to verify the process controls over data management to determine whether there is responsibility over the availability and completeness of data and the timeliness and accuracy of data processing.

Formatted Table

© 2026 National Association of Insurance Commissioners

Formatted Table

Risk Stmt #	Risk Statement	Ctrl #	Control Objective Identifier	Common Controls	Preliminary Information Request	Possible Test Procedures
	management process.		B	Procedures are defined, implemented and maintained for IT operations.	Provide a copy of the policy and procedures for IT operations.	Review the standard IT operational procedures and verify the propriety and effectiveness of the procedures for abnormal operating system termination, the inclusion of a callout list in the case of emergency, etc. Verify that batch job duties and responsibilities for each computer operator exist along with shift schedules.
			C	Claims and policy admin data is stored in a format that allows it to be transferred and utilized, if necessary (e.g., in the event of a receivership, audit or changing vendors, etc.)	Provide documentation regarding the accessibility and transferability of company claims and policy admin data.	Review the claims and policy admin data and determine if there would be any accessibility or transferability issues if the company needed to move its data.
			D	The scheduling and completion of jobs is organized into a sequence, maximizing throughput and utilization to meet business requirements.	Provide a copy of the job run log showing batch job execution.	Verify that the log is reviewed on a routine basis and on a timely manner.
					Provide a copy of documentation showing contact information and codes for job failures.	Verify that procedures include points of contact in the case of job failures, along with a running list of job failure codes.
	~~The operation of outsourced IT services is not managed to maintain the protection of enterprise information and reliability of service delivery.~~	~~DSS 01.02~~		~~The company has a well-defined vendor-management process to ensure adherence to policies for security of information, operational business and IT processing requirements and integration of critical processes.~~	~~Provide a copy or description of the company's vendor-management process.~~	~~Review the company's vendor-management process and verify that it adheres to best practices and company policies for information.~~
					~~Provide copies of SLA and SSAE 18 SOC 2 reports for each key or critical outsourced service provider.~~	~~Review the SLA for key or critical outsourced services and verify that the contracts include a right-to-audit provision.~~ ~~Interview personnel and verify that the company monitors SSAE 18 SOC 2 reports for its critical outsourced processes and services. Review a sample of SOC 2 reports~~

© 2026 National Association of Insurance Commissioners

Formatted Table

Risk Stmt #	Risk Statement	Ctrl #	Control Objective Identifier	Common Controls	Preliminary Information Request	Possible Test Procedures
						~~and verify that the effectiveness of controls was attested to by the auditor. If key control failures were identified by the auditor in the SOC 2 report, discuss with personnel how the control failure is being compensated at the company.~~
	~~Lack of infrastructure monitoring may result in the inability to detect and/or recognize security incidents.~~	~~DSS 01.03~~		~~IT infrastructure activity is logged with sufficient detail to reconstruct, review and examine operational activities; this activity is monitored on a regular basis.~~	~~Provide a copy of reports used to monitor the IT infrastructure.~~	~~Verify that the infrastructure assets that need to be monitored are identified based on service criticality and the relationship between configuration items and services that depend on them.~~ ~~Verify that automated tools are used to monitor IT infrastructure and whether alerts, reports and logs are generated for significant events.~~
	Inadequate physical and environmental controls may result in unauthorized access and inadequate protection of data.	DSS 01.04–DSS 01.05	E	The data center contains proper physical and environmental controls to protect the equipment, data and personnel located within.	Provide information regarding the physical and environmental controls in place at the company's data center and other sensitive IT sites.	Tour the data center, inspect documents and interview the appropriate personnel to verify that physical security and environmental controls are in place and monitored. Verification may include the following: Physical sites for IT equipment have been selected through consideration of such issues as geographic position, neighbors, infrastructure and risks (e.g., theft, temperature, fire, smoke, water, vibration, terrorism, vandalism, chemicals and explosives). A process is defined and implemented that identifies and monitors the potential risks and threats to the organization's IT sites and assesses the potential business impact on

© 2026 National Association of Insurance Commissioners

Formatted Table

Risk Stmt #	Risk Statement	Ctrl #	Control Objective Identifier	Common Controls	Preliminary Information Request	Possible Test Procedures
						an ongoing basis, taking into account the risks associated with natural and man-made disasters. A policy is defined and implemented for the physical security and access control measures to be followed for IT sites and that the policy is regularly reviewed to ensure that it remains relevant and up-to-date. Access to information about sensitive IT sites and their design plans are restricted to essential personnel. External signs and other identification of sensitive IT sites are discreet and do not obviously identify the site from outside. Organizational directories/site maps do not identify the location of sensitive IT sites. A process supported by the appropriate authorization is defined and implemented for the secure removal of IT equipment. IT facilities are situated and constructed in a way to minimize and mitigate susceptibility to environmental threats. Suitable devices are in place to detect environmental threats. Evaluate the effectiveness of continuous monitoring performed through these devices.

© 2026 National Association of Insurance Commissioners

Risk Stmt #	Risk Statement	Ctrl #	Control Objective Identifier	Common Controls	Preliminary Information Request	Possible Test Procedures
						Alarms or other notifications are raised in case of an environmental exposure, procedures in response to such occurrences are documented and tested, and personnel are adequately trained. A process exists that examines the IT facilities' needs for protection against environmental conditions and power fluctuations and outages, in conjunction with other business continuity planning procedures. Verify that a policy and procedure exists for recording, monitoring, managing, reporting and resolving physical security incidents, in line with the overall IT incident management process. Uninterruptible power supplies (UPS) are available, regularly tested and meet business continuity requirements. In facilities housing sensitive IT systems, more than one power supply entry is available and the physical entrance of power is separated. A process is in place to ensure that IT sites and equipment are maintained per the supplier's recommended service intervals and specifications.

Formatted Table

© 2026 National Association of Insurance Commissioners

Formatted Table

Risk Stmt #	Risk Statement	Ctrl #	Control Objective Identifier	Common Controls	Preliminary Information Request	Possible Test Procedures
						IT sites and server rooms are kept clean and in safe condition.
			F	Procedures are defined and implemented to grant, modify, and revoke access to premises, buildings, and areas, according to business needs, including during emergencies.	Provide a copy of the procedures for system and facility access.	Verify that physical access rights are appropriately authorized and administered. This may include the following: 1) A process is in place that governs the requesting and granting of access to the computing facilities. 2) Formal access requests are completed and authorized by management of the IT site, the records are retained, and the forms specifically identify the areas to which the individual is granted access. This may be verified by observation or review of approvals. 3) Procedures are in place to ensure that access profiles remain current. Verify that access to IT sites (server rooms, buildings, areas or zones) is based on job function and responsibilities. 4) A policy exists requiring visitors to be escorted at all times by a member of the company whilst on-site, and individuals who are not wearing appropriate identification are pointed out to security personnel. 5) Access to sensitive IT sites is restricted through perimeter restrictions, such as fences/walls and security devices on interior and exterior doors. 6) Devices record entry and sound an alarm in the event of unauthorized access. Examples of such devices include badges or key cards, keypads, closed-circuit television and biometric scanners.

© 2026 National Association of Insurance Commissioners

Formatted Table

Risk Stmt #	Risk Statement	Ctrl #	Control Objective Identifier	Common Controls	Preliminary Information Request	Possible Test Procedures
					Provide a copy of the facility access logs.	Verify that there is a process to log and monitor all entry points to IT sites, registering all visitors, including contractors and vendors, to the site.
DSS 02	Inadequate or ineffective response and resolution to user requests and incidents could result in interruption of services or inefficient usage of technology solutions.	~~DSS 02.01~~		~~The company has a defined security incident response plan process that clearly communicates characteristics of potential security incidents so they can be properly classified, treated, and addressed. The incident response plan outlines resources available and responsibilities for addressing security incidents. The incident response plan also considers and addresses third parties, including vendors and service providers.~~	~~Provide a copy of the company's security incident response plan including escalation procedures.~~	~~Verify the existence and completeness of a cybersecurity incident response plan, including whether it addresses third-party service providers (backup vendors and other contingency plans).~~ ~~Verify that an appropriate level of resources is in place to recognize and effectively manage security emergencies. The following areas should exist as part of an effective incident response process:~~ ~~1) Incident handling – General and specific procedures and other requirements to ensure effective handling of incidents, including prioritization, and reported vulnerabilities.~~ ~~Determine if there are procedures related to handling of cyber-security incidents.~~ ~~2) Communications – Requirements detailing the implementation and operation of emergency and routine communications channels amongst key members of management.~~
					~~Provide a list of security incidents during the period under review.~~	~~Select a sample of incidents to verify that the security incident management process includes:~~ ~~1) Event detection and containment.~~ ~~2) Correlation of events and evaluation of threat/incident.~~

© 2026 National Association of Insurance Commissioners

Formatted Table

Risk Stmt #	Risk Statement	Ctrl #	Control Objective Identifier	Common Controls	Preliminary Information Request	Possible Test Procedures
						~~3) Resolution of threat, or creation and escalation of an appropriate work order.~~ ~~4) Criteria for initiating the organization's incident response process.~~ ~~5) Verification and required levels of documentation of the resolution.~~ ~~6) Post-remediation analysis.~~ ~~7) Work order/incident closure.~~
					~~Provide evidence of the company's security incident tracking process.~~	~~Verify that the security incident management process appropriately interfaces with key organizational functions, including the help desk, external service providers and network management.~~
				~~Response and recovery activities are coordinated with internal and external stakeholders, including affected external parties or business associates (e.g., vendors or service providers), and law enforcement agencies, as appropriate.~~	~~Provide a copy of the company's incident response plan and procedures.~~	~~Review the company's incident response plan and procedures and verify whether:~~ ~~• Personnel know their roles and order of operations when a response is needed.~~ ~~• Events are reported consistent with established criteria.~~ ~~• Information is shared consistent with response plans.~~ ~~• Coordination with stakeholders occurs consistent with response plans.~~ ~~Voluntary information sharing occurs with external stakeholders in accordance with the organization's data classification criteria to achieve broader cybersecurity situational awareness.~~
				~~The company has established procedures for performing a~~	~~Provide a copy of the company's computer~~	~~Review and confirm whether the company's procedures follow a process of identifying,~~

© 2026 National Association of Insurance Commissioners

Formatted Table

Risk Stmt #	Risk Statement	Ctrl #	Control Objective Identifier	Common Controls	Preliminary Information Request	Possible Test Procedures
				~~forensic investigation of the security incident or crime (if deemed necessary). Investigations are performed by a qualified professional trained in incident detection and management (e.g., certified forensic computer examiner, certified ethical hacker, etc.).~~	~~forensic investigation procedures.~~	~~preserving, analyzing and presenting digital evidence in a manner that is acceptable in any legal proceedings (i.e., a court of law).~~
				~~The company incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing (including sharing with affected external parties) and implements the resulting changes into the risk management controls (APO 12).~~	~~Provide information regarding lessons learned from current and previous incident response activities and how they are incorporated into the organization's response activities.~~	~~Verify that lessons learned are incorporated into the security incident response plan and verify, where appropriate.~~ ~~Verify the communication of the results of post-remediation analysis to management and the board of directors or board committee, thereof, as appropriate.~~
		DSS 02.02–DSS 02.03	A	The company has a service function to record, classify and prioritize requests ~~and incidents~~ (e.g., service desks).	Provide a copy of the policy and procedures for the service function.	Verify that the processes and tools are in place to register ~~incidents~~requests~~,~~ status and actions for resolution. Review the standards for communication of ~~incidents~~ requests and verify that they were complied with.
					Provide a listing of open and closed user reported user requests~~incident records~~.	Review a sample of open and closed customer ~~incidents~~ requests to verify compliance with the process and service commitments. For the sample selected, verify that all resolved ~~incidents~~ requests are described in detail, including a detailed log of all steps taken to resolve the incident.

© 2026 National Association of Insurance Commissioners

Formatted Table

Risk Stmt #	Risk Statement	Ctrl #	Control Objective Identifier	Common Controls	Preliminary Information Request	Possible Test Procedures
					Provide documentation on the workflow used to handle ~~incidents~~requests	Review procedures for reporting significant ~~incidents~~ requests to management. Verify with management that significant ~~incidents~~ requests are reported to them.
		~~DSS 02.05~~		~~The company has a formal recovery process in place that documents, applies, and tests the identified solutions or workarounds for recovery. The process includes recovery actions to restore all critical IT-related services.~~	~~Provide documentation on the workflow used to handle recovery.~~	~~Review the company's documented recovery process for completeness and verify it is reviewed and updated regularly. Verify that recovery processes include:~~ ~~• Ensuring all other elements of the incident response plan have been fulfilled prior to proceeding with recovery.~~ ~~• Proper communication to internal/external stakeholders prior to and following the restoration of services.~~ ~~• Checking restoration assets for indicators of compromise, file corruption, and other integrity issues before use.~~ ~~• Verification of the correctness, integrity, and adequacy of the restoration actions taken before placing a restored system online.~~ ~~• Defined criteria for declaring the recovery processes complete.~~ ~~If applicable, select from a sample of recent security incidents to verify that documented processes related to recovery were appropriately followed. Otherwise, request documentation regarding recent testing of the recovery processes.~~

Formatted Table

Risk Stmt #	Risk Statement	Ctrl #	Control Objective Identifier	Common Controls	Preliminary Information Request	Possible Test Procedures
		~~DSS 02.07~~		~~A reporting function has been established to monitor and measure service performance, service response times and user satisfaction with the service function.~~	~~Provide information on how the performance of the service function is monitored.~~	~~Verify that a process is in place to evaluate the performance of the service function in the areas of response time and user satisfaction.~~
DSS 03	The company has an ineffective problem-management process that increases operating costs and reduces system availability and~~,~~ service levels. ~~and customer satisfaction~~.	DSS 03.01	A	The company maintains problem-management policies and procedures, including escalation triggers, with adequate audit trails and analysis to identify, report and classify problems ~~incidents~~ by category, impact, urgency and priority.	Provide a copy of the policy and procedures used to identify, classify and track problems~~incidents~~.	Verify that adequate processes supported by appropriate tools are in place to identify and monitor ~~incidents~~problems. For TPA problem management, review SLAs, SSAE 18, contracts, etc.
		DSS 03.02	B	The company has implemented a problem-management system that identifies and initiates solutions addressing the root cause of the problem and provides adequate audit trail facilities that allow tracking, analyzing and determining the root cause of all reported problems.	Provide a copy of the company's problem-management policies and procedures.	Review the company's policies and procedures to verify that problems were tracked and solutions addressed the root cause of problems.
					Provide a listing of all problem tickets for the period under review. The listing should include a ticket number, description of the problem, date the problem was reported, date the problem was closed and, if open, current priority.	Select a sample of tickets for appropriate prioritization, identification of root cause, timely completion, documentation of actions taken and any necessary approvals.
					Provide evidence of the company's monitoring of the problem-management system.	Review the evidence to verify that the company (ideally business management) is monitoring the timeliness and the quality of the selected problem solutions.

© 2026 National Association of Insurance Commissioners

Formatted Table

Risk Stmt #	Risk Statement	Ctrl #	Control Objective Identifier	Common Controls	Preliminary Information Request	Possible Test Procedures
		DSS 03.03–DSS 03.04	C	Problem disposition procedures are in place to address problem~~error~~ resolution.	Provide a listing of all problem tickets opened during the period under review.	Review the log for sequential gaps and identify the causes. Select a sample of problems and verify, through interviews with stakeholders, that they were informed completely, and in a timely manner, of problem remediation activity and closures.
		DSS 03.05	D	Change management is integrated with problem management to ensure effective management of problems and to enable improvements.	Provide a copy of the company's problem~~incident~~ management policy.	Review the policy to verify that the problem-management process is integrated with the change-management process to ensure that problems~~incidents~~ are addressed. Select a sample of problem tickets to verify that there was an associated change ticket.
DSS 04	Inadequate business continuity planning ~~management~~ may result in the inability to ensure critical business functions.	DSS 02.05, DSS 04.01–DSS 04.02, DSS 04.05	A	The company has a defined and documented framework that provides: 1) A consistent company-wide process for business~~IT~~ continuity management. 2) A planning process that creates the rules and structures to document, test and execute the IT disaster recovery and business continuity plans. 3) The identification of critical resources, noting key dependencies, the monitoring and reporting of the availability of critical resources, alternative processing, and the principles of backup and recovery. 4) Considerations for continuity management in the event of a cybersecurity incident.	Provide copies of ~~IT~~ business continuity plans, including disaster recovery plan or procedures. Provide a copy of the business impact analysis (BIA) study. Provide a copy of contracts and SLAs supporting the business~~IT~~ continuity plan. Provide the procedures and evidence for testing and periodic plan updates.	Verify that a company-wide business continuity plan is in place. As part of this overall plan, an ~~IT~~ business continuity plan should be completed to include: 1) BIA study. 2) Prioritized recovery strategy. 3) Necessary operational support. 4) Any compliance requirements. 5) Comprehensive and appropriate disaster recovery plan. 6) Cross reference to the incident response plan Possible elements of the disaster recovery plan that need to be verified may include: 1) The conditions and responsibilities for activating and/or escalating the plan. 2) A prioritized recovery strategy, including the necessary sequence of activities.

© 2026 National Association of Insurance Commissioners

Formatted Table

Risk Stmt #	Risk Statement	Ctrl #	Control Objective Identifier	Common Controls	Preliminary Information Request	Possible Test Procedures
				Change control procedures are in place to ensure that the ~~IT~~ continuity plan is kept up-to-date and continually reflects actual business requirements.		3) Minimum recovery requirements to maintain adequate business operations and service levels with diminished resources. 4) Emergency procedures. 5) IT processing resumption procedures, subject to incident response plan conclusion. 6) A maintenance and testing schedule. 7) Awareness, education and training activities. 8) Responsibilities of individuals. 9) Regulatory considerations. 10) Critical assets, resources and up-to-date personnel contact information needed to perform emergency, fallback and resumption procedures. 11) Alternative processing facilities, as determined within the plan. 12) Alternative suppliers for critical resources. 13) Chain of communications plan. 14) Roles, tasks and responsibilities defined by SLAs and/or contracts for internal and external service providers. Verify that plans are accessible to authorized personnel. Verify that the plans are up to date and all copies of the ~~IT~~ business continuity and disaster recovery plans are updated with revisions and are stored on- and off-site.
		DSS 02.05, DSS 04.04	B	The company tests the ~~IT~~ business continuity and disaster recovery	Provide evidence of management's review of	Verify that IT continuity tests are scheduled and completed on a regular basis and after

Formatted Table

Risk Stmt #	Risk Statement	Ctrl #	Control Objective Identifier	Common Controls	Preliminary Information Request	Possible Test Procedures
				plans on a regular basis to ensure that IT systems can be effectively recovered. The process includes recovery actions to restore all critical IT related services. The company has policies in place to ensure that test results and deficiencies are communicated to management and the plan is updated as required.	continuity recovery test results. Provide evidence of continuity test deficiency resolutions.	significant changes to the IT infrastructure or business applications. Verify that test results are reported to management and that necessary changes are made.
		DSS 04.07 – DSS 04.08	C	All critical backup media, documentation and other IT resources necessary for IT recovery and continuity plans are stored off-site in a secure location. Policies and procedures are in place to maintain an inventory of stored and archived media. The company has procedures in place for backup and restoration of systems, applications, data and documentation that are consistent with its business requirements and continuity plan. The backup environment should be isolated, air gapped, and inaccessible from the internet so information cannot be accessed or changed remotely.	Provide a copy of policies and procedures relating to the backup of systems and data, including copies of recovery procedures for off-site backups and information about off-site backup locations and/or service providers. Provide an inventory of backups and media and evidence that the company periodically validates the inventory. When outsourcing significant systems of functions, provide a copy of contracts and SLAs supporting the IT	Inquire and verify that data is protected and secured when taken off-site and while in transit to the storage location. Inquire and verify that the backup facilities are not subject to the same risks as the primary site. Inquire and verify that there is an air gap, or other protection mechanisms, between the company's production environment and backup systems. The air gap, whether logical or physical, should be designed in a manner that if a ransomware attack infects the company's main production systems, the immutable, offline backups could be deployed to replace the infected systems. Inquire and verify that an inventory of backups and media exists and that the company verifies its accuracy.

© 2026 National Association of Insurance Commissioners

Formatted Table

Risk Stmt #	Risk Statement	Ctrl #	Control Objective Identifier	Common Controls	Preliminary Information Request	Possible Test Procedures
					business continuity and disaster recovery plans. When outsourcing significant systems of functions, provide a copy of contracts and SLAs supporting the IT business continuity and disaster recovery plans. Provide a copy of the media inventory and data dictionary for the warehouses supporting all financially significant systems. If the company uses third-party vendors to provide off-site media storage, provide copies of the service contracts. Provide evidence that backup and storage requirements for critical systems, applications, data and related documents are periodically reviewed and aligned with risks and the continuity plan.	Inquire and verify that the backup media contain all information required by the IT business continuity and disaster recovery plans. Verify data replication product being used and review documentation from testing the utilization of the replicated data to recover the system. Review retention periods for data and verify that they are in line with contractual, legal and regulatory requirements. Review the media inventories and, on a sample basis, verify that media on the inventory list can be identified and items in storage can be traced back to the inventory. Verify, through a review of contracts, that the company's access to its storage media cannot be restricted by the service provider. Verify that critical systems, applications, data and related documents that affect business operations are periodically reviewed for alignment with the risk management model and IT service continuity plan. Verify that adequate policies and procedures for backup of systems, applications, data and documentation exist and consider factors including:

© 2026 National Association of Insurance Commissioners

Formatted Table

Risk Stmt #	Risk Statement	Ctrl #	Control Objective Identifier	Common Controls	Preliminary Information Request	Possible Test Procedures
					Provide evidence that backup and storage environments are properly isolated.	1) Frequency and age of backups. Older backups can be used in the event that a newer backup copy is infected. 2) Type of backups (e.g., disk mirroring, external media, full, incremental, air gapped, immutable, offline copy, etc.). 3) Automated online backups. 4) Data types (e.g., voice, optical). 5) Creation of logs. 6) Critical end-user computing data (e.g., spreadsheets). 7) Physical and logical location of data sources. 8) Security and access rights. 9) Encryption.
					~~Provide an inventory of backups and media and evidence that the company periodically validates the inventory.~~	~~Inquire and verify that an inventory of backups and media exists and that the company verifies its accuracy.~~ ~~Inquire and verify that the backup media contain all information required by the IT business continuity and disaster recovery plans.~~
					~~When outsourcing significant systems of functions, provide a copy of contracts and SLAs supporting the IT business continuity and disaster recovery plans.~~	~~Verify data replication product being used and review documentation from testing the utilization of the replicated data to recover the system.~~
		~~DSS 04.08~~		~~Effective and efficient data storage, retention and archiving policies and procedures are available to meet business objectives.~~	~~Provide a copy of the data retention policy.~~	~~Review retention periods for data and verify that they are in line with contractual, legal and regulatory requirements.~~

© 2026 National Association of Insurance Commissioners

Formatted Table

Risk Stmt #	Risk Statement	Ctrl #	Control Objective Identifier	Common Controls	Preliminary Information Request	Possible Test Procedures
				~~Policies and procedures are in place to maintain an inventory of stored and archived media.~~	~~Provide a copy of the media inventory and data dictionary for the warehouses supporting all financially significant systems.~~	~~Review the media inventories and, on a sample basis, verify that media on the inventory list can be identified and items in storage can be traced back to the inventory.~~ ~~On a sample basis, verify that external labels correspond with internal labels, or otherwise validate that external labels are affixed to the correct media.~~
					~~If the company uses third-party vendors to provide off-site media storage, provide copies of the service contracts.~~	~~Verify, through a review of contracts, that the company's access to its storage media cannot be restricted by the service provider.~~
				~~The company has procedures in place for backup and restoration of systems, applications, data and documentation that are consistent with its business requirements and continuity plan.~~ ~~The backup environment should be isolated, air gapped, and inaccessible from the internet so information cannot be accessed or changed remotely.~~	~~Provide evidence that backup and storage requirements for critical systems, applications, data and related documents are periodically reviewed and aligned with risks and the continuity plan.~~ ~~Provide evidence that backup and storage environments are properly isolated.~~	~~Verify that critical systems, applications, data and related documents that affect business operations are periodically reviewed for alignment with the risk management model and IT service continuity plan.~~ ~~Verify that adequate policies and procedures for backup of systems, applications, data and documentation exist and consider factors including:~~ ~~1) Frequency and age of backups. Older backups can be used in the event that a newer backup copy is infected.~~ ~~2) Type of backups (e.g., disk mirroring, external media, full, incremental, air gapped, immutable, offline copy, etc.).~~ ~~3) Automated online backups.~~ ~~4) Data types (e.g., voice, optical).~~ ~~5) Creation of logs.~~

© 2026 National Association of Insurance Commissioners

Formatted Table

Risk Stmt #	Risk Statement	Ctrl #	Control Objective Identifier	Common Controls	Preliminary Information Request	Possible Test Procedures
						~~6) Critical end-user computing data (e.g., spreadsheets).~~ ~~7) Physical and logical location of data sources.~~ ~~8) Security and access rights.~~ ~~9) Encryption.~~
			D	The post-resumption review has been performed after testing or an incident and the BCP updated as a result.	Provide evidence of recent testing of backup processes or post-resumption processes to verify all components of backups were effectively restored.	Verify that sufficient restoration tests have been performed periodically to ensure that all components of backups can be effectively restored. Verify post-resumption review was performed and the BCP updated as a result.
~~DSS 05~~	~~The company's business is threatened by the impact of operational information security vulnerabilities and incidents.~~	~~DSS 05.01~~		~~Preventive, detective and corrective measures are in place (especially up-to-date security patches and virus control) across the organization to protect information systems and technology from malware (e.g., viruses, worms, spyware, spam).~~	~~Provide a copy of the company's policies and procedures over malicious software. Identify how the policy is communicated throughout the organization.~~	~~Verify that a malicious software prevention policy is established, documented and communicated throughout the organization and is included in the security policy.~~
					~~Provide an inventory of server and desktop virus protection tools, including details on the current patch level.~~	~~Select a sample of the company's servers and validate that they are updated to the current patch level.~~ ~~Verify that automated controls have been implemented to provide virus protection and that violations are appropriately communicated.~~ ~~Inquire of key staff members whether they are aware of the malicious software prevention policy and their responsibility for ensuring compliance.~~

© 2026 National Association of Insurance Commissioners

Formatted Table

Risk Stmt #	Risk Statement	Ctrl #	Control Objective Identifier	Common Controls	Preliminary Information Request	Possible Test Procedures
					~~Provide a copy of the company's virus protection tool installation and update procedures including information regarding version and patch-level used.~~	~~From a sample of user workstations, verify that a virus protection tool has been installed and includes virus definition files and the last time the definitions were updated.~~ ~~Verify that the protection software is centrally distributed (version and patch-level) using a centralized configuration and change-management process.~~ ~~Verify that information on new potential threats is regularly reviewed and evaluated and, as necessary, manually updated to the virus definition files.~~ ~~Verify that incoming email is filtered appropriately against unsolicited information.~~
				~~A vulnerability management plan is developed and implemented.~~	~~Provide a copy of the company's vulnerability management plan, including information on scanning and vulnerability remediation.~~	~~Verify that a vulnerability management plan is in place and has the following attributes:~~ ~~(1) Utilizes standardized vulnerability scanning tools.~~ ~~(2) Utilizes industry standard vulnerability scoring, such as the common vulnerability scoring system (CVSS).~~ ~~(3) Regularly scans all end-points, servers, network devices, database management systems, web applications, and internet gateways.~~ ~~(4) Includes appropriate service level agreements for remediation of discovered vulnerabilities.~~ ~~(5) Incorporates a mechanism for reporting and aging all outstanding vulnerabilities.~~

© 2026 National Association of Insurance Commissioners

Formatted Table

Risk Stmt #	Risk Statement	Ctrl #	Control Objective Identifier	Common Controls	Preliminary Information Request	Possible Test Procedures
		~~DSS 05.02~~		~~Business, risk and compliance requirements are translated into an overall IT security policy/procedure that takes into consideration the IT infrastructure and the security culture.~~	~~Provide a copy of the information security policy and IT security governance documentation, including:~~ ~~1) An external communications security policy.~~ ~~2) A firewall policy.~~ ~~3) An email security policy.~~ ~~4) An agreement to comply with IT policies.~~ ~~5) A laptop/desktop computer security policy.~~ ~~6) An Internet usage policy.~~	~~Verify that a detailed information security policy, as well as standards and procedures exist, which may address the following:~~ ~~1) Responsibilities of the board, executive management, line management, staff members and all users of the company IT infrastructure.~~ ~~2) A security compliance policy.~~ ~~3) Management risk acceptance (security noncompliance acknowledgement, including noncompliance to security policies with supporting policy exception waiver approved by senior management).~~ ~~4) An external communications security policy.~~ ~~5) A firewall policy.~~ ~~6) An email security policy.~~ ~~7) An agreement to comply with IT policies.~~ ~~8) A laptop/desktop computer security policy.~~ ~~9) An Internet usage policy.~~ ~~10) Procedures to implement, monitor, update and enforce the policies and standards.~~ ~~11) Staffing requirements.~~ ~~12) Security awareness and training.~~ ~~13) Investments in required security resources.~~ ~~14) Cyber-security.~~ ~~Verify that the IT security policy considers IT tactical plans, data classification, technology standards, security and control~~

© 2026 National Association of Insurance Commissioners

Formatted Table

Risk Stmt #	Risk Statement	Ctrl #	Control Objective Identifier	Common Controls	Preliminary Information Request	Possible Test Procedures
						~~policies, risk management and external compliance requirements.~~ ~~Verify that policy exceptions are authorized, tracked, aggregated and reviewed on a regular basis for appropriateness.~~
				~~Security policies and procedures are documented and communicated to stakeholders and users.~~	~~Provide evidence of user review and acknowledgement of the company's security policies.~~	~~Verify that personnel are required to periodically review and acknowledge the company's security policies.~~ ~~Assess the level of awareness of both the content of the security policies and the importance of compliance with policies by employees.~~
				~~Security techniques and related management procedures (e.g., firewalls, security appliances, network segmentation, intrusion detection, etc.) are used to authorize access and control information flows from and to networks.~~	~~Provide a copy of network security standards and procedures, including change-management procedures and required documentation.~~	~~Verify that a network security policy (e.g., provided services, allowed traffic, types of connections permitted) has been established and is maintained.~~ ~~Verify that procedures and guidelines for administering all critical networking components (e.g., core routers, DMZ, VPN switches) are established and updated regularly by the key administration personnel and changes to the documentation are tracked in the document history.~~
				~~Sensitive data is exchanged only over a trusted path or medium, with controls to provide authenticity of content, proof of submission, proof of receipt and non-repudiation of origin.~~	~~Provide an inventory of methods of exchanging sensitive data encryption tools used by the company.~~	~~Verify that data transmissions outside the organization require encrypted format prior to transmission.~~ ~~Verify that sensitive data processing is controlled through application controls that validate the transaction prior to transmission.~~

© 2026 National Association of Insurance Commissioners

Formatted Table

Risk Stmt #	Risk Statement	Ctrl #	Control Objective Identifier	Common Controls	Preliminary Information Request	Possible Test Procedures
		DSS 05.04–Logical Access	A	All users (internal, external and temporary) and their activity on IT systems (business application, IT environment, system operations, development and maintenance) are uniquely identifiable.	Provide a copy of the company's user access policy and procedures for adding, modifying and deleting users, including management approvals.	Verify that security practices require users and system processes to be uniquely identifiable and systems to be configured to enforce authentication before access is granted. Verify that the company's password rules are consistent with the criticality and sensitivity of the data for which they afford access.
			B	User identities are enabled via authentication mechanisms including multi-factor authentication for remote or privileged access, as appropriate based on the sensitivity of the information which may be accessed.	Provide a description of the company's authentication method for system and application access.	Verify that authentication control mechanisms are utilized for controlling logical access across all users, systems, processes and IT resources, for in-house and remotely managed users. Multi-factor authentication is required for remote access.
			C	Policies and procedures are in place ~~available~~ to classify data and protect information assets under control of the business.	Provide policies and procedures that describe the company's data classification program.	Verify the IT security policy considers IT tactical plans, data classification, technology standards, security and control policies, risk management and external compliance requirements.
			D	User access rights to systems and data are in line with defined and documented business needs. This includes access rights granted to service providers.	Provide a listing of data classification and catalogs/inventories for significant data elements.	If predetermined and preapproved roles are utilized to grant access, verify that the roles clearly delineate responsibilities based on least privileges and ensure that the establishment and modification of roles are approved by process owner management. Verify that systems, applications, and data have been classified by levels of importance and risk, complete data catalogs/inventories are maintained, and process owners have been identified and assigned.

© 2026 National Association of Insurance Commissioners

Formatted Table

Risk Stmt #	Risk Statement	Ctrl #	Control Objective Identifier	Common Controls	Preliminary Information Request	Possible Test Procedures
			E	User access rights are requested by user management, approved by system owners and implemented by the security-responsible person to grant, modify ~~limit~~ and revoke access to systems, applications and data.	Provide a listing of user access roles, including systems and applications access.	Verify that procedures exist to periodically assess and recertify individual user system and application access and authorities.
					Provide a listing of hires, transfers and terminations.	Verify that logical access rights are appropriately authorized, administered, modified and revoked.
		~~DSS 05.05 – Physical Access~~		~~Procedures are defined and implemented to grant, limit and revoke access to premises, buildings and areas, according to business needs, including during emergencies.~~	~~Provide a copy of the procedures for system and facility access.~~	~~Verify that physical access rights are appropriately authorized an administered. This may include the following:~~ ~~1) A process is in place that governs the requesting and granting of access to the computing facilities.~~ ~~2) Formal access requests are completed and authorized by management of the IT site, the records are retained, and the forms specifically identify the areas to which the individual is granted access. This may be verified by observation or review of approvals.~~ ~~3) Procedures are in place to ensure that access profiles remain current. Verify that access to IT sites (server rooms, buildings, areas or zones) is based on job function and responsibilities.~~ ~~4) A policy exists requiring visitors to be escorted at all times by a member of the IT operations group whilst on-site, and individuals who are not wearing appropriate identification are pointed out to security personnel.~~ ~~5) Access to sensitive IT sites is restricted through perimeter restrictions, such as~~

Formatted Table

Risk Stmt #	Risk Statement	Ctrl #	Control Objective Identifier	Common Controls	Preliminary Information Request	Possible Test Procedures
						~~fences/walls and security devices on interior and exterior doors.~~ ~~6) Devices record entry and sound an alarm in the event of unauthorized access. Examples of such devices include badges or key cards, keypads, closed-circuit television and biometric scanners.~~
					~~Provide a copy of the facility access logs.~~	~~Verify that there is a process to log and monitor all entry points to IT sites, registering all visitors, including contractors and vendors, to the site.~~
		DSS 05.06		~~Appropriate accounting practices and inventory management over sensitive IT assets have been established.~~	~~Provide a copy of the policy and procedures for receipt, removal and disposal of special forms (e.g., check stock and other negotiable instruments or special purpose printers).~~	~~Verify that procedures governing the receipt, removal and disposal of special forms within and out of the organization are adequate and are being followed.~~
					~~Provide a copy of the last review of the access to sensitive assets.~~	~~Verify that the access log to sensitive assets is periodically reviewed.~~ ~~Verify that procedures to gain, change and remove access to sensitive assets are adequate and are being followed.~~
			F	Procedures are in place to ensure that business requirements for the protection or removal of sensitive data, software, and hardware are met.	Provide a copy of policies, procedures, and guidelines relating to the disposal or removal of IT equipment, software, data, and storage media.	Verify that responsibility for the development and communication of policies on disposal of media are clearly defined. Verify that the policy includes guidance on when software or hardware is considered obsolete, how to address obsolescence in IT systems, and how variance to this policy would be managed.

© 2026 National Association of Insurance Commissioners

Formatted Table

Risk Stmt #	Risk Statement	Ctrl #	Control Objective Identifier	Common Controls	Preliminary Information Request	Possible Test Procedures
					Provide documentation to show that storage media disposed or transferred have been sanitized.	Verify that equipment and media containing sensitive information are sanitized prior to reuse or disposal in such a way that data marked as "deleted" or "to be disposed" cannot be retrieved (e.g., media containing highly sensitive data have been physically destroyed).
					Provide a copy of the current media inventory and the media disposal log.	Verify that disposed equipment and media containing sensitive information have been logged to maintain an audit trail. Verify there is a procedure to remove active media from the media inventory list upon disposal. Verify that the current inventory has been updated to reflect recent disposals in the log.
			G	Physical devices, software platforms, sensitive IT assets and applications within the organization are inventoried using appropriate accounting practices and inventory management.	Provide a copy of the policy and procedures detailing the inventory requirements over devices, software platforms and applications. Provide an inventory, including operating system version numbers, of server and client end-point systems, as well as network devices.	Verify that all devices, software, and applications are classified and inventoried and then tracked with metrics such as comprehensive deployment counts and versioning. Tracking should also consider the location and responsible individuals for items listed in the inventory. Verify that connected systems are supported and comply with internal policies.
					Provide a copy of the policy and procedures for receipt, removal and	Verify that procedures governing the receipt, removal and disposal of special forms within

© 2026 National Association of Insurance Commissioners

Risk Stmt #	Risk Statement	Ctrl #	Control Objective Identifier	Common Controls	Preliminary Information Request	Possible Test Procedures
					disposal of special forms (e.g., check stock and other negotiable instruments or special purpose printers).	and out of the organization are adequate and are being followed.
					Provide a copy of the last review of the access to sensitive assets.	Verify that the access log to sensitive assets is periodically reviewed. Verify that procedures to gain, change and remove access to sensitive assets are adequate and are being followed.
					Technical debt?	Technical debt?
		DSS 05.07		~~The company has an established company-wide IT security baseline and periodically tests and monitors its IT security implementation for compliance with that baseline.~~	~~Provide information regarding the process in place to log security events and how information is reviewed.~~	~~Verify that the IT security management function has been integrated within the organization's project-management initiatives to ensure that security is considered in development, design and testing requirements to minimize the risk of new or existing systems introducing security vulnerabilities.~~
				~~A vulnerability management plan is developed and implemented.~~	~~Provide a copy of the company's vulnerability management plan, including information on scanning and vulnerability remediation.~~	~~Verify that a vulnerability management plan is in place and has the following att~~ ~~(1) Utilizes standardized vulnerabilit~~ ~~scanning tools.~~ ~~(2) Utilizes industry standard vulnerability scoring, such as the common vulnerability scoring system (CVSS).~~ ~~(3) Regularly scans all end-points, servers, network devices, database management systems, web applications, and internet gateways.~~ ~~(4) Includes appropriate service level agreements for remediation of discovered vulnerabilities.~~

Formatted Table

Commented [TH7]: This is now covered in Risk 6 in Part 3

© 2026 National Association of Insurance Commissioners

Formatted Table

Risk Stmt #	Risk Statement	Ctrl #	Control Objective Identifier	Common Controls	Preliminary Information Request	Possible Test Procedures
						~~(5) Incorporates a mechanism for reporting and aging all outstanding vulnerabilities.~~
				~~The company has logging and monitoring functions enabled for early detection and/or prevention of abnormal activities (including individual user activities) that may need to be addressed.~~	~~Provide information regarding the process in place to log security events, including how such information is aggregated and correlated from multiple sources.~~ ~~Provide information regarding any network vulnerability tests and penetration tests performed during the period under examination. The information should include the findings along with the company's actions to address the findings.~~	~~Review event logs and/or reports evidencing the review of security events, including aggregated and correlated events, to ensure that network activity is being properly monitored. This should include consideration of activity generated by third-party service providers. Note that the extent of testing (and associated requests) should be focused on material events.~~ ~~Procedures performed may include consideration of the manner in which management classifies events to determine that material events are appropriately identified.~~ ~~Review the results of the vulnerability and penetration tests to identify the findings and verify that the company has addressed items with high or critical severity.~~
				~~Threat and vulnerability information received from information-sharing forums and sources (e.g., Financial Services Information Sharing and Analysis Center, CISA alerts, NIST National Vulnerability Database, etc.) is used in developing a risk profile.~~	~~Provide information regarding the process to integrate information received from information-sharing forums.~~	~~Review examples of how information received has resulted in changes to the broader security framework.~~
			H	The company has a process in place to integrate acquired entities/systems in a timely manner.	Provide information regarding the process to integrate acquired	Verify that security assessment and threat analysis was properly executed for any entities acquired. Ensure that issues

© 2026 National Association of Insurance Commissioners

Formatted Table

Risk Stmt #	Risk Statement	Ctrl #	Control Objective Identifier	Common Controls	Preliminary Information Request	Possible Test Procedures
				The process includes a security assessment and threat analysis of existing IT systems at acquired entities.	entities/systems and the timeline for doing so.	identified through this process are properly mitigated.
				~~The company has implemented integrity-checking mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes, etc.) and associated tools to monitor the integrity of information systems and hosted applications. Exceptions and incidents are logged and investigated.~~	~~Provide information regarding integrity-checking mechanisms used by the company to verify software, firmware and information integrity.~~	~~Verify that integrity-checking mechanisms are in place for critical systems and applications. For a sample of exceptions/incidents, verify that they are properly investigated and resolved.~~
				~~The company defines acceptable and unacceptable mobile code, establishes usage restrictions and implementation guidance for acceptable mobile code, and monitors use of mobile code within the information system.~~	~~Provide information regarding the process for detecting and preventing the execution of unauthorized mobile code.~~	~~Verify that a baseline of approved mobile code has been established and that detection mechanisms which block unauthorized mobile code execution are in place.~~
				~~Protections against data leaks are implemented.~~	~~Provide information regarding the data loss prevention (DLP) program designed to detect and prevent protected information from leaving the company.~~	~~Verify that a DLP program is in place that includes:~~ ~~(1) Detective and blocking technology that regularly scans network traffic for protected information and blocks the transmission and alerts security personnel.~~ ~~(2) Safeguards against the use of unauthorized or unencrypted portable media.~~ ~~(3) Safeguards against unauthorized screen capture technology.~~ ~~(4) Safeguards against unauthorized use of instant messaging.~~

© 2026 National Association of Insurance Commissioners

Risk Stmt #	Risk Statement	Ctrl #	Control Objective Identifier	Common Controls	Preliminary Information Request	Possible Test Procedures
						~~(5) Prohibits the use of unauthorized file transport applications.~~ ~~(6) Provides routine user awareness training.~~

Formatted Table

PART TWO – EVALUATION OF CONTROLS IN INFORMATION TECHNOLOGY (IT) WORK PROGRAM – MONITOR, EVALUATE, AND ASSESS (MEA)

Risk Stmt #	Risk Statement	Ctrl #	Control Objective Identifier	Common Controls	Preliminary Information Request	Possible Test Procedures
MEA 01	The company does not properly identify and address IT performance and conformance deficiencies.	MEA 01.01–MEA 01.04	A	The company has adopted and implemented a formalized monitoring framework to define the scope, methodology and process to be followed for measuring IT's solution, service delivery and contribution to the company, including tracking corrective actions to address anomalies.	Provide evidence of the policies and procedures over IT performance monitoring including key performance metrics (KPIs). Provide a listing of the reports used to monitor IT performance.	Evaluate whether the company's IT monitoring framework: 1) Is consistent with key IT processes and business goals and objectives. 2) Establishes a balanced set of performance targets that are approved by the business and other relevant stakeholders. 3) Defines benchmarks and targets to be used for comparison. 4) Requires periodic reviews of performance against targets. 5) Analyzes the cause(s) of any deviations, and initiates remedial action to address the underlying causes. Select a sample of the monitoring reports to evaluate whether the company is effectively monitoring and addressing IT performance.
MEA 02	The company does not identify and address	MEA 02.01	A	A process has been implemented to ~~continuously~~ monitor benchmark and improve the IT control	Provide a copy of internal control monitoring activities,	Review internal control monitoring activities for identification of control deficiencies, remediation, and reporting.

Formatted Table

	internal control deficiencies related to IT systems.			environment and control framework to meet organization objectives and cybersecurity expectations.	including control self-assessments, SOX-related control reviews, independent controls reviews by consultants/contractors (including SOC reporting if the organization provides outsourced services, penetration testing, and vulnerability scanning), and internal audits.	
					Provide a copy of the internal audit charter, mission statement and reporting relationships.	Review a copy of the internal audit charter, mission statement and reporting relationships to verify independence and objectivity of the internal audit function.
					Provide a listing of all internal audit reports, projects and reviews conducted (completed or not) during the examination period.	Review the listing of all internal audit reports, projects and reviews conducted (completed or not) during the examination period to ascertain the breadth and depth of the function.
					Provide a copy of all IT internal audit reports for the period under review.	Review all IT internal audit reports covering the examination period to ascertain the breadth and depth of the function. Verify that appropriate senior management attention was given to all significant IT findings and that issues were appropriately resolved.
					Provide a copy of the internal audit organizational chart.	Verify that the staffing of the internal audit unit is sufficient to accomplish the corporate mission.
					Provide a listing of IT specialists in the internal audit unit	Verify that the education, certifications and experience of the IT specialists in the internal

© 2026 National Association of Insurance Commissioners

					including background information such as education, certifications and experience.	audit unit enable the accomplishment of the corporate mission.
MEA 03	IT processes and IT-supported business processes are not compliant with applicable laws, regulations and other contractual requirements.	MEA 03.01–MEA 03.02	A	A ~~review~~ process has been implemented to ~~continuously~~ identify the changes in local and international laws, regulations and other external requirements that must be complied with for incorporation into the organization's IT policies, standards, procedures and methodologies.	Provide a copy of procedures to verify that legal (e.g., *Insurance Data Security Model Law* [#668]), regulatory, and contractual obligations impacting IT are reviewed.	Verify that procedures are in place to ensure that legal, regulatory, and contractual obligations impacting IT are reviewed. These regulatory compliance procedures should: 1) Identify and assess the impact of the applicable legal or regulatory requirements relevant to the IT organization. 2) Update the associated IT policies and procedures affected by the legal and regulatory requirements. 3) Include areas such as laws and regulations for electronic commerce, data flow, privacy, internal controls, financial reporting, industry-specific regulations, intellectual property copyright, and health and safety.
					Provide evidence that the company's IT policies and procedures have addressed all relevant legal, regulatory and contractual obligations.	Verify that the company's evidence documents its process to ensure that external obligations are addressed in IT policies and procedures.
		MEA 03.03–MEA 03.04	B	A procedure has been implemented to review and report compliance of IT policies, standards, procedures and methodologies with applicable legal and regulatory requirements.	Provide a copy of the position description for the chief compliance officer, including IT compliance officer if in place.	Verify that the organization has a chief compliance officer or equivalent and review a copy of the job description for this position for adequacy.
					Provide a copy of the IT organization policies, standards, regulatory	Verify that a review of the IT organization policies, standards and procedures is conducted periodically to address any non-compliance (legal and regulatory) gaps

© 2026 National Association of Insurance Commissioners

					review plan and procedures.	identified (this can be included in the risk assessment process).
					Provide a copy of compliance documentation from all financially significant third-party service providers.	Verify that policies and procedures are implemented to ensure that contract with third-party service providers requires regulator confirmation of compliance (e.g., receipt of assertions) with applicable laws, regulations and contractual commitments.

© 2026 National Association of Insurance Commissioners

Prior IT Program Steps vs. New IT Program Steps

ITGC Review

Step 1 - Gather Necessary IT Planning Information
[Exhibit C – Part One – ITPQ]
[Gather the ITGC information]

Step 2 - Review Gathered Information
[Evaluate the ITGC information]

Step 3a - Request Insurer Control Information and Complete IT Review Planning
[Customize Exhibit C Part 2 Work Program]

Step 3b - Request Insurer Control Information and Complete IT Review Planning (continued)
[ITPM]

Step 4a - Conduct IT Review Fieldwork
[Interviews]

Step 4b - Conduct IT Review Fieldwork (continued)
[Complete APO]
[Complete BAI]
[Complete DSS]
[Complete MEA]

Step 5 - Document Results of IT Review
[ITSM]

Step 6 - Assist on Financial Examination

ITGC Review

Step 1 - Information Gathering and ITGC Planning
[Exhibit C – Part One – ITPQ]
[Gather the ITGC information]
[Gather the Cyber Review information] (new)
[Evaluate the ITGC information]
[Conduct Interviews]
[Customize Exhibit C – Part Two – ITGC Work Program]
[ITGC Planning Memo]

Step 2 - Conduct ITGC Review Fieldwork
[Conduct Walkthroughs & other Interviews]
[Complete APO]
[Complete BAI]
[Complete DSS]
[Complete MEA]

Step 3 - Document Results of ITGC Review
[ITGC Summary Memo]

Cybersecurity Review

Step 4 – Prospective Cyber Risk Information Gathering and Planning
[Request any cybersecurity-related information] (new)
[Cybersecurity Planning Memo (CPM)] (new)
[Customize Exhibit C - Part Three – Cyber Risk Work Program] (based on the NIST CSF 2.0) (new)

Step 5 - Conduct Prospective Cyber Risk Assessment
[Complete Cyber Risk Work Program] (new)

Step 6 - Document Results of Cybersecurity Testing
[Cybersecurity Summary Memorandum (CSM)] (new)

Step 7 - Assist on Financial Examination

© 2026 National Association of Insurance Commissioners

PART THREE – PROSPECTIVE CYBER RISK EVALUATION OF CONTROLS WORK PROGRAM

Background

The Information Technology cybersecurity examination (IT cyber exam) repository in this section was created to assist IT examiners in identifying the most common cybersecurity risks within a typical insurance company. The intent of the repository is to provide a tool to assist IT examiners in determining cybersecurity risks that might be relevant during the cybersecurity assessment of an IT examination. The IT cybersecurity exam repository is not intended to provide an all-inclusive listing of potential risks, nor to provide a minimum baseline of which risks are required to be identified on all exams. The repository is a fluid document and, as such, will be modified and updated with relevant risks and exam procedures as deemed necessary. These risks are intended to allow flexibility and customization in identifying cybersecurity risks of the insurer and should be modified commensurate with the size and complexity of the insurer. Included with the identified risks are examples of mitigation strategies, control objectives, possible test procedures, and preliminary information requests an IT examiner may choose to customize and test each identified risk.

This work program is organized around the six functions of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0: Govern, Identify, Protect, Detect, Respond, and Recover. These functions are modeled after the NIST CSF 2.0 due to its widespread acceptance and use as a cybersecurity risk management framework. Although this work program is organized around the NIST CSF 2.0 functions, it does not incorporate every Category and Subcategory included within the framework. Rather it incorporates common cyber security risks, controls, and examination procedures that may be relevant during an insurance company examination. Govern addresses how the organization establishes and monitors cybersecurity governance, strategy, policies, roles, responsibilities, and risk management processes. Identify addresses the understanding of cybersecurity risks to organizational assets, systems, and operations. Protect addresses safeguards designed to secure systems, data, and services from cybersecurity threats. Detect addresses activities used to identify cybersecurity events and potential indicators of compromise. Respond addresses actions taken to contain, analyze, and mitigate cybersecurity incidents. Recover addresses activities performed to restore systems, services, and operations following a cybersecurity incident.

To promote a comprehensive cybersecurity assessment, IT examiners should consider evaluating at least one risk from each of the six NIST CSF 2.0 Functions: Govern, Identify,

© 2026 National Association of Insurance Commissioners

Protect, Detect, Respond, and Recover. The specific risks selected should be based on the examiner's understanding of the insurer and the cybersecurity risks most relevant to the organization.

Identified Risks

The identified risks provided within the cybersecurity risk repository are not designed to be an all-inclusive list and may not apply to all insurance companies. The IT examiner's understanding of the insurer should be used to determine which risks included in these exam repositories are applicable to the insurer. The cybersecurity risk repository is not intended to be all-inclusive, and the insurer may have additional cybersecurity risks that should be considered based on its size and complexity. The IT examiner must determine which additional risks are not included but should be examined as part of the cybersecurity review.

Mitigation Strategies

The possible mitigation strategies provided within the IT cybersecurity exam risk repository are the most common ways in which insurers mitigate the specific risks identified. These mitigation strategies are common for a typical insurance company but may not apply to each individual insurer. Each insurer has its own controls in place to mitigate the identified risks, which may or may not correspond to the mitigation strategies identified within the cybersecurity exam risk repositories. It is possible that the insurer has adequate controls in place, even if the control does not match the possible mitigation strategies listed in the cybersecurity exam risk repositories. Additionally, it is possible that a review of multiple controls would be necessary to fully mitigate the risk identified.

Control Objectives

The control objectives provided within the IT cybersecurity exam risk repository represent specific cybersecurity outcomes that support the identified controls. These control objectives are intended to provide additional context regarding the activities, processes, and practices commonly used to achieve the stated control objective. The control objectives are not designed to be an all-inclusive list of activities that may be performed by an insurer, nor are they intended to represent a minimum baseline of requirements that must be evaluated during every examination. The IT examiner should use professional judgment to determine which control objectives are relevant to the insurer under

© 2026 National Association of Insurance Commissioners

examination and may consider additional activities not included within the repository when evaluating the identified risk.

Possible Test Procedures

The possible test procedures provided within the IT cybersecurity exam risk repository are intended to illustrate common examination procedures that may be performed to evaluate the identified control objectives. These test procedures are not designed to be an all-inclusive list of actions that may be performed by an examiner, nor are they intended to represent a minimum baseline of activities that must be implemented or evaluated during every examination. The test procedures are intended to provide examples of activities an IT examiner may perform to determine whether the insurer's controls adequately address the identified risk. The IT examiner should use professional judgment to determine which test procedures are relevant to the insurer under examination and may consider additional activities not included within the repository when evaluating the identified risk.

Possible Preliminary Information Requests

The possible preliminary information requests in the cybersecurity exam risk repository are not designed to be an all-inclusive list, nor are they intended to be a list of items required to be obtained on all examinations, as some of the items may not apply to the insurer under examination. If the insurer's controls do not match the repository controls, the IT examiner should not use the possible preliminary information requests provided within the cybersecurity exam risk repository. In this case, the IT examiner needs to develop alternative requests and tests based on how the insurer mitigates the identified risk.

© 2026 National Association of Insurance Commissioners

NIST CSF 2.0 Function	Risk (Part 2 Domain, if relevant)	Mitigation Strategy (NIST CSF 2.0 Categories)	Control Objective (NIST CSF 2.0 Subcategories)	Possible Test Procedures (Adapted from NIST CSF 2.0 Implementation Examples)	Possible Preliminary Information Requests
Govern	Risk 1: The exclusion of cybersecurity risks from the company's enterprise risk management (ERM) program prevents holistic evaluation of cyber threats, resulting in unallocated / misallocated security resources and unmitigated exposures. (APO 12.02 – APO 12.05)	Control 1.1 GV.RM – Risk Management Strategy: The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions.	GV.RM-01: Risk management objectives are established and agreed to by organizational stakeholders. GV.RM-02: Risk appetite and risk tolerance statements are established, communicated, and maintained. GV.RM-03: Cybersecurity risk management activities and outcomes are included in enterprise risk management processes. GV.RM-06: A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated.	GV.RM-01.1: Verify that the company's near-term and long-term cybersecurity risk management objectives are updated as part of its annual strategic planning and when major changes occur. GV.RM-02.3: Verify that the company's organizational objectives and risk appetite are refined periodically based on known risk exposure and residual risk (e.g., a risk register). GV.RM-03.3: Verify that the company's criteria for escalating cybersecurity risks within enterprise risk management are established. GV.RM-06.1: Verify that the company's criteria for using a quantitative approach to cybersecurity risk analysis are established, and that probability and exposure formulas are specified.	GV.RM-01.1.1: Provide the cybersecurity near-term and long-term strategic plan. GV.RM-01.1.2: Provide evidence of the board of directors' formal approval of the updated cybersecurity objectives and the annual review of the cybersecurity plan. GV.RM-02.3.1: Provide the cybersecurity risk appetite statement, ERM IT risk register, and risk quantification outputs such as a heatmap or risk scoring matrix. GV.RM-03.3.1: Provide the cybersecurity risk management policy, risk scoring methodology, and ERM IT risk register. GV.RM-06.1.1: Provide documentation of the ERM IT risk register's risk likelihood and impact formula and the quantitative trigger criteria for cybersecurity risk.
Govern	Risk 2: An inadequate or unclear IT organizational structure and staffing model could result in misaligned	Control 2.1 GV.RR – Roles, Responsibilities, and Authorities: Cybersecurity roles, responsibilities, and	GV.RR-02: Roles, responsibilities, and authorities related to cybersecurity risk	GV.RR-02.1: Verify that the company's risk management roles and responsibilities are documented in policy.	GV.RR-02.1.1: Provide the company's ERM policy, cybersecurity risk management policy, and information security policy, that document the risk

© 2026 National Association of Insurance Commissioners

NIST CSF 2.0 Function	Risk (Part 2 Domain, if relevant)	Mitigation Strategy (NIST CSF 2.0 Categories)	Control Objective (NIST CSF 2.0 Subcategories)	Possible Test Procedures (Adapted from NIST CSF 2.0 Implementation Examples)	Possible Preliminary Information Requests
	and/or unassigned security responsibilities, resource gaps, and heightened vulnerability to cyber threats. (APO 01.03 – APO 01.05, APO 07)	authorities to foster accountability, performance assessment, and continuous improvement are established and communicated.	management are established, communicated, understood, and enforced. GV.RR-03: Adequate resources are allocated commensurate with the cybersecurity risk strategy, roles, responsibilities, and policies.	GV.RR-02.3: Verify that the company's cybersecurity responsibilities and performance requirements are included in personnel descriptions. GV.RR-02.5: Verify that the company's cybersecurity responsibilities are clearly articulated within operations, risk functions, and internal audit functions. GV.RR-03.3: Verify that adequate and sufficient people, process, and technical resources are provided to support the cybersecurity strategy.	management roles and responsibilities. GV.RR-02.1.2: Provide the board-level Risk Committee charter and Cybersecurity Risk Committee charter, the personnel organization chart, annual policy review and approval signoffs, and stakeholders' policy acknowledgement records. GV.RR-02.3.1: Provide position descriptions for core IT security roles (e.g., CISO, security engineers, network admins) outlining specific cybersecurity and incident response duties. GV.RR-02.5.1: Provide information security and IT operational policies detailing day-to-day execution of security controls. Identify the roles responsible for technical security configurations. GV.RR-02.5.2: Provide the board-approved internal audit charter, annual cybersecurity audit plan, and independent audit reports and remediation tracking logs for recently completed cybersecurity audits.

© 2026 National Association of Insurance Commissioners

NIST CSF 2.0 Function	Risk (Part 2 Domain, if relevant)	Mitigation Strategy (NIST CSF 2.0 Categories)	Control Objective (NIST CSF 2.0 Subcategories)	Possible Test Procedures (Adapted from NIST CSF 2.0 Implementation Examples)	Possible Preliminary Information Requests
					GV.RR-03.3.1: Provide the cybersecurity personnel organizational chart showing roles and vacancies, and the skills gap analysis and allocated training budget. GV.RR-03.3.2: Provide the cybersecurity policies, procedures, standards, and guidelines for the company's various security domains (e.g., identity and access management, asset management and lifecycle, change and configuration management, vulnerability and patch management, third-party risk management, and incident response and business continuity). GV.RR-03.3.3 Provide the cybersecurity technology architecture diagram or a listing of the company's current security stack (e.g., EDR, SIEM, IAM, firewalls, DLP).
Govern	Risk 3: The company's information security policy may be inadequate and/or outdated, which increases the risk that threat actors can exploit vulnerabilities in the company's IT environment. (DSS 05.02)	Control 3.1 GV.PO – Policy: Organizational cybersecurity policy is established, communicated, and enforced.	GV.PO-01: Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced.	GV.PO-01.1: Verify that an understandable, usable risk management policy with statements of management intent, expectations, and direction is created, disseminated, and maintained.	GV.PO-01.1.1: Provide the cybersecurity risk management policy and the supporting standards and procedures. GV.PO-01.2.1: Provide evidence that the cybersecurity risk management policy is reviewed annually and has executive management signoff.

© 2026 National Association of Insurance Commissioners

NIST CSF 2.0 Function	Risk (Part 2 Domain, if relevant)	Mitigation Strategy (NIST CSF 2.0 Categories)	Control Objective (NIST CSF 2.0 Subcategories)	Possible Test Procedures (Adapted from NIST CSF 2.0 Implementation Examples)	Possible Preliminary Information Requests
			GV.PO-02: Policy for managing cybersecurity risks is reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission.	GV.PO-01.2: Verify that the policy and supporting processes and procedures are periodically reviewed to ensure that they align with risk management strategy objectives and priorities, as well as the high-level direction of the cybersecurity policy. GV.PO-01.4: Verify that the cybersecurity risk management policy and supporting processes and procedures are communicated across the organization. GV.PO-02.4: Verify that policies are updated to reflect changes in technology (e.g., adoption of artificial intelligence) and changes to the business (e.g., acquisition of a new business, new contract requirements).	GV.PO-01.2.2: Provide the policy exception log showing approved deviations from the requirements of the company's cybersecurity risk management policies. GV.PO-01.4.1: Provide evidence of the cybersecurity risk management policy's accessibility by all staff and policy acknowledgment signoffs. GV.PO-02.4.1: Provide a consolidated inventory of recent technology and business changes, e.g., deployment of major new IT platforms, tools, or architectures, and mergers, acquisitions, divestitures, etc. during the period under review. GV.PO-02.4.2: Provide evidence of policy changes corresponding to technological and business changes. Provide evidence of the formal governance function demonstrating policy update approvals.
Govern	Risk 4: Inadequate oversight of cybersecurity risks results in unmonitored cyber threats that compromise enterprise assets and disrupt operations.	Control 4.1 GV.OV – Oversight: Results of organization-wide cybersecurity risk management activities and performance are used to inform, improve, and adjust	GV.OV-02: The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks.	GV.OV-02.1: Verify that audit findings are reviewed to confirm whether the existing cybersecurity strategy has ensured compliance with internal and external requirements.	GV.OV-02.1.1: Provide evidence of formal approval from the Chief Information Security Officer or compliance heads acknowledging audit findings.

© 2026 National Association of Insurance Commissioners

NIST CSF 2.0 Function	Risk (Part 2 Domain, if relevant)	Mitigation Strategy (NIST CSF 2.0 Categories)	Control Objective (NIST CSF 2.0 Subcategories)	Possible Test Procedures (Adapted from NIST CSF 2.0 Implementation Examples)	Possible Preliminary Information Requests
	(APO 02, APO 12)	the risk management strategy.	GV.OV-03: Organizational cybersecurity risk management performance is evaluated and reviewed for adjustments needed.	GV.OV-02.3: Verify that the strategy is reviewed in light of cybersecurity incidents. GV.OV-03.2: Verify that key risk indicators (KRIs) are reviewed to identify risks the organization faces, including likelihood and potential impact.	GV.OV-02.1.2: Provide centralized issue trackers or corrective action plans for audit reports issued during the period under review. GV.OV-02.1.3: Provide evidence that audit findings have previously been added to the enterprise or IT risk register to track the impact on the broader security strategy. GV.OV-02.3.1: Provide evidence showing cybersecurity incidents being linked to updates in strategy, compliance policies, or control frameworks. GV.OV-03.2.1: Provide cybersecurity key risk indicators (KRI), dashboards, and reports showing trends, current status, and threshold levels. GV.OV-03.2.2: Provide records from risk committees or management reviews where KRIs and their risk implications were discussed.
Govern	Risk 5: Inadequate oversight of third-party and affiliate service providers, including weak access controls, unmonitored security postures, and poor supply chain risk management,	Control 5.1 GV.SC – Cybersecurity Supply Chain Risk Management: Cyber supply chain risk management processes are identified, established, managed, monitored, and	GV.SC-01: A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed	GV.SC-01.2 Verify that the cybersecurity supply chain risk management program is developed, including a plan (with milestones), policies, and procedures that guide implementation and improvement of the program, and that the policies	GV.SC-01.2.1: Provide the Cyber Supply Chain Risk Management (C-SCRM) strategy, policy, and evidence that each is shared with key organizational stakeholders (e.g., Legal, IT, business unit leadership, etc.), accompanied by active tracking

© 2026 National Association of Insurance Commissioners

NIST CSF 2.0 Function	Risk (Part 2 Domain, if relevant)	Mitigation Strategy (NIST CSF 2.0 Categories)	Control Objective (NIST CSF 2.0 Subcategories)	Possible Test Procedures (Adapted from NIST CSF 2.0 Implementation Examples)	Possible Preliminary Information Requests
	increases the likelihood of a cyber breach, data exfiltration, or system outage caused by third-party and affiliate service providers with access to critical environments or NPI. (APO 10.01 – 10.05)	improved by organizational stakeholders.	to by organizational stakeholders. GV.SC-02: Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally. GV.SC-03: Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes. GV.SC-04: Suppliers are known and prioritized by criticality. GV.SC-06: Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships.	and procedures are shared with organizational stakeholders. GV.SC-02.6: Verify that roles and responsibilities for suppliers, customers, and business partners are developed to address shared responsibilities for applicable cybersecurity risks and integrated into organizational policies and applicable third-party agreements. GV.SC-03.4: Verify that material cybersecurity risks in supply chains are escalated to senior management and addressed at the enterprise risk management level. GV.SC-04.1: Verify that criteria for supplier criticality are developed based on, for example, the sensitivity of data processed or possessed by suppliers, the degree of access to the organization's systems, and the importance of the products or services to the organization's mission. GV.SC-06.1: Verify that thorough due diligence is performed on prospective suppliers that is consistent with procurement planning and commensurate with	artifacts that document short-term and long-term implementation milestones, target completion dates, and assigned initiative owners. GV.SC-02.6.1: Provide IT security policies that govern shared risk for third parties. GV.SC-02.6.2: Provide executed third-party contracts, master service agreements, and service level agreements, complete with all addenda, including shared responsibility clauses for access control and data security. GV.SC-03.4.1: Provide the ERM materiality threshold definitions, minutes from senior management and board-level risk committee meetings that address third-party cybersecurity risk, and the ERM IT risk register and third-party risk escalation tickets. GV.SC-04.1.1: Provide the C-SCRM methodology used to define a critical affiliate or third-party service provider. GV.SC-04.1.2: Provide the finalized vendor risk tiering matrix.

© 2026 National Association of Insurance Commissioners

NIST CSF 2.0 Function	Risk (Part 2 Domain, if relevant)	Mitigation Strategy (NIST CSF 2.0 Categories)	Control Objective (NIST CSF 2.0 Subcategories)	Possible Test Procedures (Adapted from NIST CSF 2.0 Implementation Examples)	Possible Preliminary Information Requests
			GV.SC-07: The risks posed by a supplier, their products and services, and other third parties are understood, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship. GV.SC-09: Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and their performance is monitored throughout the technology product and service life cycle. GV.SC-10: Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement.	the level of risk, criticality, and complexity of each supplier relationship. GV.SC-07.3: Verify that critical suppliers are monitored to ensure that they are fulfilling their security obligations throughout the supplier relationship lifecycle using a variety of methods and techniques, such as inspections, audits, tests, or other forms of evaluation. GV.SC-07.5: Verify that unexpected supplier and supply chain-related interruptions are planned for to ensure business continuity. GV.SC-09.5: Verify that policies and procedures require checking upgrades to critical hardware for unauthorized changes. GV.SC-10.2: Verify that plans for component end-of-life maintenance support and obsolescence are defined and implemented. GV.SC-10.3: Verify that supplier access to organization resources is deactivated promptly when it is no longer needed.	GV.SC-06.1.1: Provide the C-SCRM and/or TPRM policy and the procurement vetting procedures. GV.SC-06.1.2: Provide the due diligence assessment evidence, e.g., risk questionnaires, scorecards, and third-party audit reports that are collected and analyzed. GV.SC-07.3.1: Provide the C-SCRM and/or TPRM policy and the periodic monitoring procedures for critical affiliate or third-party service providers. GV.SC-07.3.2: Provide a listing of all critical affiliate or third-party service providers and independent audits and assessments, e.g., SOC 2 Type 2 reports, SOC for Cybersecurity reports, or ISO certifications for each. GV.SC-07.5.1: Provide the formal recovery strategies (e.g., BCP/DRP and TPRM contingency sub-plans, and alternative sourcing strategies or workarounds), detailing how the company will maintain business operations in the unexpected failure of a critical affiliate or third-party service provider.

© 2026 National Association of Insurance Commissioners

NIST CSF 2.0 Function	Risk (Part 2 Domain, if relevant)	Mitigation Strategy (NIST CSF 2.0 Categories)	Control Objective (NIST CSF 2.0 Subcategories)	Possible Test Procedures (Adapted from NIST CSF 2.0 Implementation Examples)	Possible Preliminary Information Requests
				GV.SC-10.4: Verify that assets containing the organization's data are returned or properly disposed of in a timely, controlled, and safe manner.	GV.SC-07.5.2: Provide evidence of annual testing of critical affiliate or third-party service provider interruption, e.g., tabletop exercise materials, simulation scripts, and after-action reports / lesson learned logs. GV.SC-09.5.1: Provide the change management policy or hardware configuration management policy, SOPs for hardware inspection and upgrade validation, and the inventory of critical infrastructure hardware (e.g., core switches, firewalls, servers, etc.). GV.SC-10.2.1: Provide the technology lifecycle management policy (or similar), the Configuration Management Database (CMDB) or IT asset inventory that includes vendor EOL/EOS dates, and plans for decommissioning, migration, and extended support for critical assets identified as EOL/EOS. GV.SC-10.3.1: Provide the Identity and Access Management (IAM) policy, service provider offboarding SOP, consolidated register of deactivated service provider accounts showing termination date/time, the active

© 2026 National Association of Insurance Commissioners

NIST CSF 2.0 Function	Risk (Part 2 Domain, if relevant)	Mitigation Strategy (NIST CSF 2.0 Categories)	Control Objective (NIST CSF 2.0 Subcategories)	Possible Test Procedures (Adapted from NIST CSF 2.0 Implementation Examples)	Possible Preliminary Information Requests
					service provider personnel roster, and the list of all service providers whose engagements ended during the examination period. GV.SC-10.4.1: Provide the policy governing data device destruction standards, the inventory of decommissioned assets, and the third-party certificates showing that data device destruction occurred.
Identify	Risk 6: Failure to ingest, analyze, and assess cybersecurity vulnerabilities prevents early threat visibility, exposing the company to unmitigated cyber incidents and operational disruption. (DSS 05.07)	Control 6.1 ID.RA – Risk Assessment: The cybersecurity risk to the organization, assets, and individuals is understood by the organization.	ID.RA-01: Vulnerabilities in assets are identified, validated, and recorded. ID.RA-02: Cyber threat intelligence is received from information sharing forums and sources. ID.RA-06: Risk responses are chosen, prioritized, planned, tracked, and communicated. ID.RA-08: Processes for receiving, analyzing, and responding to vulnerability disclosures are established.	ID.RA-01.1: Verify that vulnerability management technologies identify unpatched and misconfigured software. ID.RA-01.2: Perform an evaluation of network and system architectures to determine whether design and implementation weaknesses are present that could impact cybersecurity. ID.RA-02.3: Review evidence showing that the organization monitors cyber threat intelligence sources for information on vulnerabilities associated with emerging technologies. ID.RA-06.1: Verify that vulnerabilities are remediated and	ID.RA-01.1.1: Provide the company's detailed technical vulnerability scans showing detected Common Vulnerabilities and Exposures (CVEs), missing software patches, configuration baseline failures (e.g., CIS Benchmark violations), and penetration test reports. ID.RA-01.2.1: Provide network and system architecture diagrams showing network topologies, network boundaries, trust zones, firewall locations, external connections, and data flows between critical systems. Provide hardening and configuration standards showing architectural baselines for network zoning, segment segregation, and system-to-system encryption protocols.

© 2026 National Association of Insurance Commissioners

NIST CSF 2.0 Function	Risk (Part 2 Domain, if relevant)	Mitigation Strategy (NIST CSF 2.0 Categories)	Control Objective (NIST CSF 2.0 Subcategories)	Possible Test Procedures (Adapted from NIST CSF 2.0 Implementation Examples)	Possible Preliminary Information Requests
				tracked to closure based on risk priority. ID.RA-06.3: Verify that the company tracks the progress of risk response implementation through artifacts such as plan of action and milestone documents, the risk register, or risk detail reports. ID.RA-06.4: Trace documented risk assessment findings to corresponding change management tickets, budget allocations, or formal executive risk-acceptance signoffs to verify that risk findings directly drive response decisions. ID.RA-08.2: Confirm the execution of procedures for processing, analyzing, and responding to cybersecurity threats, vulnerabilities, or incident disclosures from suppliers, customers, partners, and government cybersecurity organizations.	ID.RA-02.3.1: Provide information regarding the process to integrate information received from information-sharing forums, e.g., CISA, ISAC, etc. ID.RA-06.1.1: Provide evidence the company remediated vulnerability scan and penetration test findings. ID.RA-06.3.1: Provide plans of action and milestones (POA&M) or similar evidence showing granular timelines and verified testing results for remediated vulnerabilities. ID.RA-06.4.1: Provide a list of change management tickets and formal executive risk-acceptance signoffs documenting the specific technical controls or resources purchased to correct the identified vulnerabilities. ID.RA-08.2.1: Provide action plans or remediation tickets tied to specific threat, vulnerability, or incident disclosure reports.
Identify	Risk 7: An inadequate, ineffective, or stale cyber incident response plan could result in delayed breach containment and prolonged service outage.	Control 7.1 ID.IM – Improvement: Improvements to organizational cybersecurity risk management processes, procedures and activities are	ID.IM-04: Incident response plans and other cybersecurity plans that affect operations are established, communicated,	ID.IM-04.1: Evaluate the organization's contingency plans (e.g., incident response, business continuity, disaster recovery) to determine whether they adequately support response and recovery	ID.IM-04.1.1: Provide the cybersecurity incident response plan and evidence of annual or more frequent testing.

© 2026 National Association of Insurance Commissioners

NIST CSF 2.0 Function	Risk (Part 2 Domain, if relevant)	Mitigation Strategy (NIST CSF 2.0 Categories)	Control Objective (NIST CSF 2.0 Subcategories)	Possible Test Procedures (Adapted from NIST CSF 2.0 Implementation Examples)	Possible Preliminary Information Requests
	(DSS 02.01)	identified across all CSF Functions.	maintained, and improved.	from adverse events that could disrupt operations, expose confidential information, or otherwise endanger organizational viability. ID.IM-04.5: Verify that all cybersecurity plans are reviewed and updated annually or when significant improvements are identified.	ID.IM-04.5.1: Provide evidence that the cybersecurity incident response plan is updated at least annually and that updates are approved by management.
Protect	Risk 8: Inadequate security baseline and configuration management of IT assets increases the vulnerability to intrusions, undetected malicious cyber activities, data breaches, and compromised system integrity. (BAI 04.01 – BAI 04.02)	Control 8.1 PR.PS – Platform Security: The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are managed consistent with the organization's risk strategy to protect their confidentiality, integrity, and availability.	PR.PS-01: Configuration management practices are established and applied. PR.PS-02: Software is maintained, replaced, and removed commensurate with risk. PR.PS-04: Log records are generated and made available for continuous monitoring. PR.PS-05: Installation and execution of unauthorized software are prevented.	PR.PS-01.1: Verify that hardened baselines are established, tested, deployed, and maintained to enforce cybersecurity policies and ensure only essential capabilities are enabled (i.e., principle of least functionality). PR.PS-01.3: Assess monitoring processes to confirm that implemented software is routinely checked for deviations from approved baselines. PR.PS-02.1: Select a sample of the organization's servers and workstations to verify that routine and emergency patching is performed within the timeframes specified in the vulnerability management plan.	PR.PS-01.1.1: Provide a copy of the organization's policies and procedures regarding platform hardening and configuration monitoring standards. PR.PS-01.3.1: Provide evidence of implemented automated file integrity monitoring (FIM) system, a configuration management database (CMDB), or a vulnerability/compliance scanner. PR.PS-02.1.1: Provide a copy of the policies governing the required patch windows and timeframes for both emergency and standard scenarios and the procedures regarding the patching process for workstations, servers, and other IT assets.

© 2026 National Association of Insurance Commissioners

NIST CSF 2.0 Function	Risk (Part 2 Domain, if relevant)	Mitigation Strategy (NIST CSF 2.0 Categories)	Control Objective (NIST CSF 2.0 Subcategories)	Possible Test Procedures (Adapted from NIST CSF 2.0 Implementation Examples)	Possible Preliminary Information Requests
				PR.PS-02.3: Confirm that EOL software and service versions are replaced with supported and maintained versions. PR.PS-04.1: Verify that operating systems, applications, and services (including cloud-based services) are configured to generate log records. PR.PS-04.2: Confirm that security tools send notifications to the company's logging infrastructure systems and services (i.e., SIEM, etc.) PR.PS-05.4: Verify that platforms are configured to allow installation of only organization-approved software.	PR.PS-02.1.2: Provide the system-generated reports from the company's patching toolset (e.g., WSUS or SCCM/MECM), for servers and workstations, showing asset IDs, patch names/KB numbers, installation status, and execution timestamps. PR.PS-02.3.1: Provide the company's policies and procedures for replacing EOL software and mitigating strategies to protect software past its end of life if there's a valid reason it can't be updated. PR.PS-02.3.2: Provide the formal administrative policy governing patch management or asset lifecycle management and a CMDB system-generated export listing all servers, workstations, network devices, databases, and installed software versions. PR.PS-02.3.3: Provide the most recent full infrastructure and application vulnerability scan reports, including any associated remediation tracking dashboards. PR.PS-04.1.1: Provide the formal administrative policy governing log

© 2026 National Association of Insurance Commissioners

NIST CSF 2.0 Function	Risk (Part 2 Domain, if relevant)	Mitigation Strategy (NIST CSF 2.0 Categories)	Control Objective (NIST CSF 2.0 Subcategories)	Possible Test Procedures (Adapted from NIST CSF 2.0 Implementation Examples)	Possible Preliminary Information Requests
					management, and the system-generated baseline configuration screenshots or scripts showing actively enabled logging settings on system assets. PR.PS-04.2.1: Provide information regarding the process in place to log security events and how information is reviewed. PR.PS-04.2.2: Provide the system-generated forwarding configurations from the security tools' administrative consoles, showing that log and notification exporting is actively enabled. PR.PS-05.4.1: Provide system-generated configuration screenshots or policy export files showing the enforcement rules (e.g., block rules, whitelists, code-signing requirements) applied to endpoints, servers, and mobile devices. PR.PS-05.4.2: Provide a system-generated log or dashboard export from the EDR, SIEM, or Mobile Device Management system showing historical alerts for blocked, unauthorized software execution attempts.

© 2026 National Association of Insurance Commissioners

NIST CSF 2.0 Function	Risk (Part 2 Domain, if relevant)	Mitigation Strategy (NIST CSF 2.0 Categories)	Control Objective (NIST CSF 2.0 Subcategories)	Possible Test Procedures (Adapted from NIST CSF 2.0 Implementation Examples)	Possible Preliminary Information Requests
Protect	Risk 9: Inadequate safeguards over data loss prevention, confidentiality, integrity, and availability compromise enterprise assets and disrupt operations. (DSS 05.01, DSS 05.02, APO 14.08 – APO 14.09)	Control 9.1 PR.IR – Technology Infrastructure Resilience: Security architectures are managed with the organization's risk strategy to protect asset confidentiality, integrity, availability, and organizational resilience.	PR.IR-01: Networks and environments are protected from unauthorized logical access and usage.	PR.IR-01.2: Verify that organization networks are logically segmented from external networks and that only necessary communications are permitted to enter the organization's environment. PR.IR-01.3: Confirm that zero trust architectures are implemented to restrict network access to the minimum necessary for each resource. PR.IR-01.4: Verify that endpoint cyber-health checks are performed prior to granting access to production resources.	PR.IR-01.2.1: Provide a copy of network security standards and procedures, including firewall and segmentation configurations. PR.IR-01.2.2: Provide a system-wide map or topology, showing all hardware platforms and network connections, indicating all internal and external access points. PR.IR-01.3.1: Provide a copy of the company's network architecture and segmentation diagrams. PR.IR-01.3.2: Provide configuration exports or screenshots from the central management consoles of the organization's Zero Trust Network Access, Secure Access Service Edge, or identity providers, showing that default-deny structures are active. PR.IR-01.3.3: Provide documentation showing that network access to critical systems and resources is restricted to authorized users, devices, services, and communications based on business need and least-privilege principles. PR.IR-01.4.1: Provide system-generated configuration settings or

© 2026 National Association of Insurance Commissioners

NIST CSF 2.0 Function	Risk (Part 2 Domain, if relevant)	Mitigation Strategy (NIST CSF 2.0 Categories)	Control Objective (NIST CSF 2.0 Subcategories)	Possible Test Procedures (Adapted from NIST CSF 2.0 Implementation Examples)	Possible Preliminary Information Requests
					screenshots from the Unified Endpoint Management or Mobile Device Management system showing the required health baseline (e.g., EDR/Antivirus, enabled disk encryption, minimum OS patch levels, firewall state, etc.). PR.IR-01.4.2: Provide active policy configurations or screenshots from the Identity Provider or Zero Trust Network Access platform showing that production resource access is conditional upon a compliant or healthy device status flag.
		Control 9.2 PR.DS – Data Security: Data are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-01: The confidentiality, integrity, and availability of data-at-rest are protected. PR.DS-02: The confidentiality, integrity, and availability of data-in-transit are protected.	PR.DS-01.1: Verify that encryption, digital signatures, and cryptographic hashes are used to protect the confidentiality and integrity of stored data across files, databases, virtual machine disk images, container images, and other resources. PR.DS-01.2: Confirm that full disk encryption is implemented on user endpoints to protect stored data. PR.DS-01.4: Verify that the use of removable media is restricted to prevent unauthorized data exfiltration.	PR.DS-01.1.1: Provide screenshots of encryption settings for databases (e.g., Transparent Data Encryption , AWS S3 Default Encryption, Azure Storage Encryption, etc.). PR.DS-01.1.2: Provide BitLocker / dm-crypt settings, cloud managed-disk encryption policies, or hypervisor-level storage encryption parameters. PR.DS-01.1.3: Provide cryptographic audit trails from a Key Management Service (KMS) showing active encryption keys. PR.DS-01.1.4: Provide information on encryption key rotation records.

© 2026 National Association of Insurance Commissioners

NIST CSF 2.0 Function	Risk (Part 2 Domain, if relevant)	Mitigation Strategy (NIST CSF 2.0 Categories)	Control Objective (NIST CSF 2.0 Subcategories)	Possible Test Procedures (Adapted from NIST CSF 2.0 Implementation Examples)	Possible Preliminary Information Requests
				PR.DS-01.5: Confirm that removable media containing unencrypted sensitive information is physically secured in controlled locations such as locked offices or file cabinets. PR.DS-02.1: Verify that encryption, digital signatures, and cryptographic hashes are used to protect the confidentiality and integrity of network communications. PR.DS-02.2: Confirm that outbound emails and other communications containing sensitive data are automatically encrypted or blocked based on data classification. PR.DS-02.3: Verify that access to personal email, file sharing, file storage services, and other personal communications applications is blocked on organizational systems and networks. PR.DS-02.4: Confirm that sensitive production data (such as customer records) are not reused in development, testing, or other non-production environments.	PR.DS-01.2.1: Provide information on full disk encryption that is required and implemented on user endpoints. PR.DS-01.4.1: Provide information on technical restrictions applied to the usage of portable devices that contain protected information. PR.DS-01.5.1: Provide asset inventory lists identifying removable media and their assigned storage locations. PR.DS-02.1.1: Provide information on TLS/SSL configurations on customer-facing portals, API gateways, and internal applications. PR.DS-02.1.2: Provide VPN configuration documentation showing encrypted tunnels such as IPsec or SSL VPN. PR.DS-02.2.1: Provide information regarding the data loss prevention (DLP) program designed to detect and prevent protected information from leaving the company. PR.DS-02.2.2: Provide information regarding DLP tools used to prevent or

© 2026 National Association of Insurance Commissioners

NIST CSF 2.0 Function	Risk (Part 2 Domain, if relevant)	Mitigation Strategy (NIST CSF 2.0 Categories)	Control Objective (NIST CSF 2.0 Subcategories)	Possible Test Procedures (Adapted from NIST CSF 2.0 Implementation Examples)	Possible Preliminary Information Requests
					encrypt protected information from being sent via email. PR.DS-02.3.1: Provide information regarding DLP tools, URL/web filters, etc. used to prevent protected information from being sent via personal email, file sharing sites, file storage services, or unsanctioned non-enterprise AI. PR.DS-02.4.1: Provide information on how the company prevents the use of sensitive data from being used in development, testing, and other non-production environments.
Detect	Risk 10: The absence of continuous security monitoring and defined alert baselines hinders the timely detection of anomalies and indicators of compromise, resulting in delayed threat visibility, prolonged adversary persistence, and undetected data exfiltration. (DSS 01.03, DSS 05.07)	Control 10.1 DE.CM – Continuous Monitoring: Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events.	DE.CM-01: Networks and network services are monitored to find potentially adverse events. DE.CM-03: Personnel activity and technology usage are monitored to find potentially adverse events. DE.CM-09: Computing hardware and software, runtime environments, and their data are monitored to find	DE.CM-01.1: Verify that the company monitors network services for adverse events. DE.CM-01.2: Verify that the company monitors wired and wireless networks for connections from unauthorized endpoints. DE.CM-03.1: Verify that the company uses behavior analytics software to detect anomalous user activity to mitigate insider threats. DE.CM-03.2: Verify that the company monitors logs from logical access control systems to find	DE.CM-01.1.1: Provide network monitoring policies defining roles, responsibilities, and escalation paths. DE.CM-01.1.2: Provide screenshots or historical reports from security operations centers (SOC). DE.CM-01.1.3: Provide a list of security incidents that occurred during the period under review. DE.CM-01.1.4: Provide evidence of the company's security incident tracking process.

© 2026 National Association of Insurance Commissioners

NIST CSF 2.0 Function	Risk (Part 2 Domain, if relevant)	Mitigation Strategy (NIST CSF 2.0 Categories)	Control Objective (NIST CSF 2.0 Subcategories)	Possible Test Procedures (Adapted from NIST CSF 2.0 Implementation Examples)	Possible Preliminary Information Requests
			potentially adverse events.	unusual access patterns and failed access attempts. DE.CM-09.1: Verify that the company monitors email, web, file sharing, collaboration services, and other common attack vectors to detect malware, phishing, data leaks and exfiltration, and other adverse events. DE.CM-09.2: Verify that the company monitors authentication attempts to identify attacks against credentials and unauthorized credential reuse. DE.CM-09.5: Verify that the company uses technologies with a presence on endpoints to detect cyber health issues (e.g., missing patches, malware infections, unauthorized software) and redirects the endpoints to a remediation environment before access is authorized.	DE.CM-01.2.1: Provide a system-generated log extract or dashboard capture from the SIEM or network security console, showing an alert for the historical detection of an actual or simulated rogue device. DE.CM-01.2.2: Provide results from scanning tools checking for rogue wireless access points. DE.CM-03.1.1: Provide written security policies defining acceptable user behavior and insider threat guidelines. DE.CM-03.1.2: Provide software inventory list showing the active user behavior analytics (UBA) or user and entity behavior analytics (UEBA) platform license. DE.CM-03.2.1: Provide triage records or ticket histories demonstrating that generated alerts are actively reviewed and investigated. DE.CM-09.1.1: Provide settings and rule bases from secure email gateways (e.g., Microsoft Defender for Office 365 or Proofpoint) showing active inspection for malware, phishing, and URL rewriting.

© 2026 National Association of Insurance Commissioners

NIST CSF 2.0 Function	Risk (Part 2 Domain, if relevant)	Mitigation Strategy (NIST CSF 2.0 Categories)	Control Objective (NIST CSF 2.0 Subcategories)	Possible Test Procedures (Adapted from NIST CSF 2.0 Implementation Examples)	Possible Preliminary Information Requests
					DE.CM-09.1.2: Provide a sample of historical alerts, tickets, or incident response logs triggered by email phishing attempts, blocked malicious websites, or DLP violations over the last 3 to 6 months. DE.CM-09.2.1: Provide monthly or quarterly metrics reporting on blocked login attempts, locked accounts, and credential reuse detections. DE.CM-09.2.2: Provide SIEM alert rules on access attacks such as credential stuffing, brute force attacks, or password spraying. DE.CM-09.5.1: Provide evidence of continuous, runtime endpoint detection of health compliance, via EDR/XDR agent, etc.
Detect	Risk 11: The company's failure to timely detect and analyze abnormal activities and indicators of compromise results in delayed threat visibility and escalating operational cyber incidents. (DSS 05.07)	Control 11.1 DE.AE – Adverse Event Analysis: Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents.	DE.AE-02: Potentially adverse events are analyzed to better understand associated activities. DE.AE-04: The estimated impact and scope of adverse events are understood.	DE.AE-02.1: Verify that the company uses security information and event management (SIEM) or other tools to continuously monitor log events for known malicious and suspicious activity. DE.AE-02.2: Verify that the company utilizes up-to-date cyber threat intelligence in log analysis tools to improve detection accuracy	DE.AE-02.1.1: Provide a list of all servers, firewalls, and applications sending log events to a SIEM or other monitoring tool. DE.AE-02.1.2: Provide system availability reports for the SIEM or other monitoring tools, showing that logging is ongoing without interruption.

© 2026 National Association of Insurance Commissioners

NIST CSF 2.0 Function	Risk (Part 2 Domain, if relevant)	Mitigation Strategy (NIST CSF 2.0 Categories)	Control Objective (NIST CSF 2.0 Subcategories)	Possible Test Procedures (Adapted from NIST CSF 2.0 Implementation Examples)	Possible Preliminary Information Requests
				and characterize threat actors, their methods, and indicators of compromise. DE.AE-02.4: Verify that the company uses log analysis tools to generate reports on their findings. DE.AE-04.1: Verify that the company uses SIEMs or other tools to estimate impact and scope of events, and review and refine the estimates. DE.AE-04.2: Verify that the company creates their own estimates of impact and scope of events.	DE.AE-02.2.1: Provide information regarding the process in place to log security events, including how such information is aggregated and correlated from multiple sources. DE.AE-02.2.2: Provide evidence of active subscriptions, current contracts, or valid API tokens linked to threat intelligence providers. DE.AE-02.4.1: Provide the name of the tool being used for log event analysis and reporting. DE.AE-02.4.2: Provide ticketing system entries, meeting notes, or signoffs showing staff read and acted on the reports from log analysis tools (e.g., Splunk, Microsoft Sentinel, ELK, CrowdStrike Falcon, etc.). DE.AE-04.1.1: Provide configuration screenshots or query exports from the central SIEM console, showing how the system correlates events with asset telemetry. DE.AE-04.2.1: Provide documents showing comparisons of past internal estimates against actual results as evidence of an ongoing internal evaluation process.

© 2026 National Association of Insurance Commissioners

NIST CSF 2.0 Function	Risk (Part 2 Domain, if relevant)	Mitigation Strategy (NIST CSF 2.0 Categories)	Control Objective (NIST CSF 2.0 Subcategories)	Possible Test Procedures (Adapted from NIST CSF 2.0 Implementation Examples)	Possible Preliminary Information Requests
					DE.AE-04.2.2: Provide signoff sheets, meeting minutes, or email trails where internal management and stakeholders discussed and approved the internal estimates.
Respond	Risk 12: Inadequate or ineffective response to user requests and incidents delays containment of security threats, resulting in cyber-attacks, prolonged unauthorized system access, and data breaches. (DSS 02.01)	Control 12.1 RS.MA – Incident Management: Responses to detected cybersecurity incidents are managed.	RS.MA-01: The incident response plan is executed in coordination with relevant third parties once an incident is declared.	RS.MA-01.2: Verify that the company can successfully request incident response assistance from its incident response outsourcer in accordance with established plans or when internal thresholds are met.	RS.MA-01.2.1: Provide contractual service level agreements and the escalation section of the incident response plan detailing predefined thresholds, authorized personnel, and designated hotlines or portals required to initiate contact. RS.MA-01.2.2: Provide rule definitions in SIEM or SOAR tools showing automated ticketing flags.
		Control 12.2 RS.CO – Incident Response Reporting and Communication: Response activities are coordinated with internal and external stakeholders as required by laws, regulations, or policies.	RS.CO-02: Internal and external stakeholders are notified of incidents. RS.CO-03: Information is shared with designated internal and external stakeholders.	RS.CO-02.3: Verify that the company notifies law enforcement agencies and regulatory bodies of incidents based on criteria in the incident response plan and management approval. RS.CO-03.1: Verify that the company securely shares information consistent with response plans and information sharing agreements. RS.CO-03.6: Verify that the company coordinates crisis communication methods between	RS.CO-02.3.1: Provide documented approvals from the Chief Information Security Officer (CISO), General Counsel, or CEO authorizing the external disclosure. RS.CO-02.3.2: Provide copies of formal letters, emails, or portal submissions sent to regulatory entities. RS.CO-02.3.3: Provide copies of reports filed with local, state, or federal law enforcement (such as an FBI IC3 complaint or local police report).

© 2026 National Association of Insurance Commissioners

NIST CSF 2.0 Function	Risk (Part 2 Domain, if relevant)	Mitigation Strategy (NIST CSF 2.0 Categories)	Control Objective (NIST CSF 2.0 Subcategories)	Possible Test Procedures (Adapted from NIST CSF 2.0 Implementation Examples)	Possible Preliminary Information Requests
				the organization and its critical third parties and affiliate service providers.	RS.CO-03.1.1: Provide after-action reports from past security incidents that show how information sharing followed the established agreements and policies. RS.CO-03.6.1: Provide crisis communication plans. RS.CO-03.6.2: Provide after-action reports from joint crisis simulations. RS.CO-03.6.3: Provide samples of past incident alerts sent to third parties.
		Control 12.3 RS.MI – Incident Mitigation: Activities are performed to prevent expansion of an event and mitigate its effects.	RS.MI-01: Incidents are contained.	RS.MI-01.1: Verify that the company's Cybersecurity technologies (e.g., antivirus software) and cybersecurity features of other technologies (e.g., operating systems, network infrastructure devices) automatically perform containment actions. RS.MI-01.2: Verify that the company allows incident responders to manually select and perform containment actions. RS.MI-01.3: Verify that the company allows a third party (e.g., internet	RS.MI-01.1.1: Provide incident response playbooks detailing expected automated triggers and responses. RS.MI-01.1.2: Provide network device access control list (ACL) or firewall rules for auto-blocking. RS.MI-01.2.1: Provide procedure playbooks addressing containment strategies and intervention steps. RS.MI-01.3.1: Provide contracts, service level agreements (SLAs), and policies addressing containment

© 2026 National Association of Insurance Commissioners

NIST CSF 2.0 Function	Risk (Part 2 Domain, if relevant)	Mitigation Strategy (NIST CSF 2.0 Categories)	Control Objective (NIST CSF 2.0 Subcategories)	Possible Test Procedures (Adapted from NIST CSF 2.0 Implementation Examples)	Possible Preliminary Information Requests
				service provider, managed security service provider) to perform containment actions on behalf of the organization.	authority of third parties tasked with breach response responsibilities.
Respond	Risk 13: Failure to effectively identify, log, and classify user security requests and system alerts hinders early threat detection, resulting in undetected malicious network activity, escalating cyber incidents, and unmitigated system compromises. (DSS 02.01)	Control 13.1 RS.AN – Incident Analysis: Investigations are conducted to ensure effective response and support forensics and recovery activities.	RS.AN-03: Analysis is performed to establish what has taken place during an incident and the root cause of the incident. RS.AN-06: Actions performed during an investigation are recorded.	RS.AN-03.1: Verify that the company determines the sequence of events that occurred during the incident and which assets and resources were involved in each event. RS.AN-03.2: Verify that the company attempts to determine what vulnerabilities, threats, and threat actors were directly or indirectly involved in the incident. RS.AN-03.3: Verify that the company analyzes the incident to find the underlying, systemic root causes. RS.AN-06.1: Verify that the company requires each incident responder and others (e.g., system administrators, cybersecurity engineers) who perform incident response tasks to record their actions and make the record immutable.	RS.AN-03.1.1: Provide a formal incident investigation report including a detailed reconstruction timeline. RS.AN-03.2.1: Provide the post-incident review reports including threat intelligence analysis. RS.AN-03.2.2: Provide reports from hired forensic specialists or external security consultants. RS.AN-03.3.1: Provide information regarding lessons learned from current and previous incident response activities and how they are incorporated into the organization's response activities. RS.AN-03.3.2: Provide root cause analysis (RCA) documentation. RS.AN-06.1.1: Provide written procedures and standard operating procedures (SOPs) that mandate immutable recordkeeping and define the controls enforcing it.

© 2026 National Association of Insurance Commissioners

EXHIBIT C, PART THREE

CYBERSECURITY REVIEW STANDARD SUMMARY MEMORANDUM

A summary memorandum should be developed by the IT examiner to communicate the results of the Cybersecurity review to the examiner-in-charge, financial analyst, or other regulatory stakeholders. Some of the topics the IT examiner may want to consider incorporating into the summary memorandum are included in the illustration below, along with a brief description of information that could be discussed relating to each topic. This document should provide sufficient detail of the results of the Cybersecurity review for use during the financial condition examination.

Salutation

This section should be in any format the state deems appropriate for its purposes. At a minimum, all states that are placing reliance on the ITGC review should be included in the distribution of this memo.

Background and Scope

This section should include an introductory paragraph identifying the following: companies under examination (domiciliary state and type may be helpful), the exam as-of date and time period under examination, where the work was performed, when the work was performed, who performed the work, and the scope/topic of the work performed, highlighting the risk-based intent of the work. This section should be identical to the equivalent section in the Cybersecurity Planning Memorandum.

Summary of Control Environment

This section should provide a summary description of the Cybersecurity environment, which refers to the entire holistic defense ecosystem used to protect the organization's information systems, digital assets, and data from cyber threats to ensure the confidentiality, integrity, and availability of digital information. It should include, as key components, identification of data and information assets, technologies and tools, processes and administrative policies, people and culture, and physical security. This section should also include discussion of any breaches identified since the previous exam.

Work Performed

This section of the memo should provide an overview of the work performed to evaluate Cybersecurity controls throughout the prospective cyber risk review process based on the NIST CSF 2.0 framework, as well as the reliance placed on internal or external sources (e.g., Model Audit Rule documentation/testing, Sarbanes-Oxley documentation, external audit work, self-assessments, third-party assessments, etc.). If the results of other sources are utilized to populate Exhibit C, Part 3 procedures, then include a review of the work in this section. This review could include an assessment of the source, scope, and robustness of the third-party work being utilized.

Summary / Detail of Findings

This section should provide a summary description of the findings that were identified while performing the prospective cyber risk review. These findings may include: areas that affect the company's current operations; areas that will be relevant for future examinations; or areas of recommendation for the company to consider. The IT examiner should document the recommendation and impact of the finding on financial analysis and provide reference to the supporting detail located in the completed Exhibit C, Part Three (or similar document). The IT examiner should consider mitigating factors in their assessment of the impact that findings may have (additional testing may be required to assess the effectiveness of the mitigating factors). Findings that are sufficiently mitigated by other factors may be found to have a minimal ongoing impact or risk to the insurer. Findings that have not been sufficiently mitigated, or findings that

© 2026 National Association of Insurance Commissioners

require tracking and future follow-up information, may be passed to the Summary Review Memorandum (Exhibit AA, SRM) and/or communicated to the analyst depending on significance and duration of impact. The following elements may be used in assessing findings, mitigating factors, and the overall impact on the exam: Cyber Review Findings, Prospective Impact on Insurer, Mitigating Factors, Supporting Detail Reference, Recommendation for company, and Recommended Ongoing Monitoring (if applicable).

Conclusion/Results of Cybersecurity Review

This section should document the conclusion/results of the Cybersecurity review, summarizing the risks above into one or more aggregated risks, as appropriate, with risk assessment level and trend identified (as specified in Exhibit AA Branded Risk Assessment). The IT examiner, potentially in consultation with the EIC, should consider the impact of the findings on the insurer in totality (probability and severity of financial impact) and specify monitoring or other work by the financial analyst to analyze the identified risks until the next exam. Monitoring suggestions should include specific reports, items, or information the analyst can request as well as what terminology or information to look for in those reports. This language should be used by the EIC in the Summary Review Memorandum (Exhibit AA) in the appropriate Branded Risk(s).

Completed Exhibit C, Part Three (or Similar Document) and Supporting Documentation

A completed Cyber Risk Work Program should be included or referenced here and provided to the EIC if exam procedure steps are not used. Detailed findings should be noted within the work program and referenced in the “Summary / Detail of Findings” section above.

© 2026 National Association of Insurance Commissioners

III. GENERAL EXAMINATION CONSIDERATIONS

This section covers procedures and considerations that are important when conducting financial condition examinations. The discussion here is divided as follows:

A. General Information Technology (IT) Review
B. Materiality
C. Examination Sampling
D. Business Continuity
E. Using the Work of a Specialist
F. Outsourcing of Critical Functions
G. Use of Independent Contractors on Multi-State Examinations
H. Considerations for Insurers in Run-Off
I. Considerations for Potentially Troubled Insurance Companies
J. Comments and Grievance Procedures Regarding Compliance with Examination Standards

A. General Information Technology Review

The examination of information technology (IT) utilized by an insurer has become an increasingly important part of the examination process as companies have placed a greater reliance on IT systems to run their business. IT general controls (ITGCs) are policies and procedures that help ensure proper operation of computer systems, including controls over network operations, software acquisition and maintenance, and access security. ITGCs provide a foundation necessary to ensure the completeness, integrity and availability of IT systems and data and comprise the environment from which application controls are designed, implemented, and operated. An effective ITGC ~~general control~~ environment can, therefore, provide financial examiners with greater assurance regarding the overall reliability of a company's IT systems and the reports generated from those systems. In addition, this allows the opportunity to test and rely on automated application controls during Phase 3 of the exam.

The general IT review also includes a prospective assessment of the insurer's cybersecurity risks. To distinguish the objectives and timing of this work, the IT review process separates the assessment of ITGC reliability from the prospective cybersecurity risk assessment. The ITGC reliability assessment (steps 1 through 3) is based on COBIT 2019 and should be completed before the end of Phase 2 so the financial examination team has a timely conclusion regarding ITGC reliability. The prospective cybersecurity risk assessment (steps 4 through 6) is based on elements of COBIT 2019 and the NIST Cybersecurity Framework (CSF) 2.0 and may continue during later phases of the examination. Step 7 should be completed by the end of Phase 5.

~~As such, a formalized process to complete a general IT review has been developed to assist the IT examiner in completing this important section of the financial condition examination. In a risk-focused examination, steps 1–5 of the general IT review process should be performed prior to the completion of planning the overall financial condition examination. Step 6 of the IT review process should be performed in conjunction with the remaining portion of the overall examination.~~ The following steps document the process to be followed in completing the general IT review:

1. ~~Gather Necessary IT Planning Information~~Information Gathering and ITGC Planning

   The first step in performing a general IT review is to gather the information necessary to plan the IT review of the insurer. At this time, the examiner-in-charge (EIC) and the IT examiner should work together to request that the insurer complete the Information Technology Planning Questionnaire (ITPQ), included in Exhibit C – Part One, to assist in the planning process. Information relevant to the prospective cybersecurity risk assessment should also be gathered during this step when readily available so that it may be leveraged during later steps and duplicative requests may be avoided. In addition, other relevant information to obtain

in planning the IT review might include prior examination workpapers, work on IT systems performed by internal/external auditors or consultants, and information maintained by the insurance department's financial analysts. The reports and results from third-party cyber self-assessment tools may also be utilized for an IT review. Note that if companies do not use these tools, the IT examiner can continue with the normal IT review process. There are a variety of cyber self-assessment tools that companies may opt to use depending on their business type. Examples of cyber assessment tools that have been developed include, but are not limited to, tools developed by, or to facilitate compliance with the following: the Financial Services Sector Coordinating Council (FSSCC), the Health Information Technology for Economic and Clinical Health Act (HITECH), and the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Based on ~~a~~ consideration of the assessment tool's scope, date of preparation, and quality of information presented (including whether or not the information has been validated by an independent third party), the state insurance regulator may determine the information contained within the assessment ~~that~~ can be extensively leveraged during the IT review. Depending on the assessment of the IT examiner, the results of the cyber self-assessment tool may be used to:

- Populate Exhibit C with risk statements and controls to be tested.
- Reduce the extent of testing within Exhibit C if the state insurance regulator determines that the self-assessment has already been sufficiently validated.

After the information for planning the IT review has been gathered, including the ITPQ, the IT examiner should review the information obtained to assist in planning and determining the scope of the ITGC risks to be reviewed. Some factors to consider as part of this process include:

- The complexity of the insurer's information systems and IT risk mitigation strategies;
- The extent to which reliance will be placed on those risk mitigation strategies in the financial examination;
- The length of time the existing system has been in place and any significant changes to the system;
- The types of subsystems being used and how data is shared among systems;
- The hardware and software being used and whether the software was internally or externally developed;
- The extent to which the insurer outsources its IT functions;
- Past issues the insurer may have had with its systems;
- Answers provided from the insurer via the ITPQ;
- Documentation available from other sources, including external and internal auditors;
- The insurer's participation in electronic business and electronic data interchange;
- The amount of reliance placed on the work of third parties;
- The type, volume, and external availability of sensitive information that is processed and/or stored by the company and;
- Changes to the company's controls and/or processes to ensure compliance with applicable federal and state security statutes, consumer privacy law, ~~state data security model laws~~ or the General Data Protection Regulation (GDPR), if applicable, or other relevant data protection requirements.

The IT examiner should consider which risks included on the Evaluation of Controls in Information Technology (IT) Work Program (Exhibit C – Part Two) are applicable to the insurer under examination and determine if there are additional general IT risks that should be reviewed for this insurer. Additionally, based on the review of internal and external audit work, the IT examiner may determine that sufficient testing has been performed to fully address specific risks or areas of concern. In this case, the IT examiner may document in the IT planning memo their comfort with, and planned reliance on, the specific internal and/or external audit work included in the file. Additionally, the IT examiner need not include these specific risks or areas of concern in the IT work program.

After the initial planning information has been gathered and reviewed, the Evaluation of Controls in Information Technology (IT) Work Program (Exhibit C – Part Two) to be utilized in the review should be created. As part of this process, the IT examiner should customize the standard work program to include only the general IT risks that are of concern for the insurer under examination. In addition to providing a list of risks in the work program, the IT examiner may wish to provide a list of common controls that indicate how a typical insurer may mitigate these risks to assist the insurer in developing its response. Finally, the IT examiner may consider prompting the insurer to include information supporting the IT controls in place to mitigate risks by including an information request in the work program distributed to the insurer. The IT examiner ~~review team~~ should coordinate with the appropriate staff at the insurer to request a response. The insurer's response should indicate ~~their~~its controls in place to mitigate the risks identified in the work program. The IT examiner should review the company responses, considering the adequacy of the controls identified, and request evidence to test the effectiveness of the insurer's mitigating controls. The IT examiner may consider some of the examination procedures listed in the Evaluation of Controls in Information Technology (IT) Work Program (Exhibit C – Part Two~~), and~~) and complete the planning of the IT review.

Formatted: Strikethrough

Following this planning, more targeted information aligned with and specific to the scope of the current financial examination should be requested. This can include interviews with company staff, as needed. These interviews should serve as an opportunity to substantiate and clarify information provided by the insurer in the ITPQ or Exhibit C – Part Two~~2~~.

After the work program has been finalized, the IT examiner should document the plan to complete the IT review. The plan should document the staffing to be used to complete the review, the scope of work to be performed, and a proposed budget to complete the review. The plan should be subject to the review and approval of the EIC and additional examination supervisors, as considered appropriate by the state. This plan may be documented through the use of an IT review planning memo, or other workpaper that documents the approval of the EIC.

2. ~~Review Information Gathered~~Conduct ITGC Review Fieldwork

The IT examiner should schedule examination fieldwork, with the initial fieldwork to include additional interviews with key IT staff, as necessary, and walkthroughs. ~~interviews with key IT staff, if additional interviews are needed, and walkthroughs~~ These interviews should serve as an opportunity to substantiate and clarify some of the information provided by the insurer in Exhibit C – Part Two. The IT examiner may also gain additional information relating to key activities, risks, and risk mitigation strategies for the financial examination. As such, the IT examiner may want to invite the examiner-in-charge and/or other financial examination staff to participate in the interview process. Some of the potential candidates ~~for~~to interview include the Chief Information Officer, Chief Technology Officer, Chief Security Officer, System Architect, Chief System Engineer, and any other individuals responsible for maintaining, updating and testing the insurer's business continuity and disaster recovery plans. Example agenda items for IT interviews, subject to the areas of expertise for the interviewee, include but are not limited to:

- IT s~~S~~trategic ~~pP~~planning;
- IT g~~G~~overnance;
- Leadership development and succession planning;
- Organizational structure;
- Risk management;
- Development and maintenance of policies;
- ~~Budgeting;~~
- Security;
- E-Business;
- Business continuity and disaster recovery;

- Acquisitions and integration;
- Architecture, development and implementation of major programs;
- Outsourced IT functions
- External environment, and
- Any other items necessary to evaluate the insurer's ~~general IT controls~~ITGCs.

After the IT examiner ~~review team~~ has completed the interviews, the team should begin to test the general controls identified by the insurer. This work should be completed with the assistance of the insurer's IT staff and should utilize the existing work of others, if deemed appropriate. As noted in ~~s~~Step 1 above, if the IT examiner has determined that reliance will be placed on all or some of the work performed by CPAs or the company's internal audit function (if deemed independent) to fully address a specific risk or area of concern, the IT examiner would not be required to include those specific risks or areas of concern on the work program. However, if the IT examiner determines that the work performed by the third ~~-~~party only partially addresses a risk, ~~but~~and additional work would be required to fully address that risk, the IT examiner should include the relevant third-party documentation in the file and map or link it to the respective risk in the work program.

While it is expected that audit work (external/internal) would be the most common type of work relied on by the exam team, work performed by other regulatory agencies and/or cybersecurity experts may also be leveraged to reduce the independent work performed during an exam. Regardless of the work being reviewed, state insurance regulators should specifically consider the scope of work, the independence, and qualifications of the entity (or person) performing the work, the timing of the work performed, and the findings included in any report received. State insurance regulators should also review supporting workpapers to determine whether the work performed adequately addresses the risks under consideration. Qualifications should be evaluated based on the training, experience and education of personnel performing the work ~~(see Section 1-2 Letter E for more information on the use of specialists)~~. Based on the state insurance regulators' review of the third-party work, state insurance regulators may be able to use the work to enhance the risk assessment, interview, and scoping process performed during the IT review. While the IT examiner is responsible for performing his/her own independent risk assessment, third-party work that directly addresses an identified risk may be relied upon in a similar manner to external/internal audit work. In this case, the IT examiner should briefly document his/her understanding of the third-party testing performed and any conclusions reached from the testing procedures. To the extent that findings are noted in the report obtained, state insurance regulators may find it more useful to ~~corroborate~~validate the remediation of the findings as opposed to performing an independent review of the company's controls to confirm the findings' existence.

After considering the utilization of existing work, testing of ~~general IT controls~~ITGCs and other procedures should be performed in order to gain an appropriate level of understanding of the insurer's IT environment and the effectiveness of ~~general IT controls~~ITGCs in place. As noted above, the IT examiner may consider performing examination procedures listed in the Evaluation of Controls in Information Technology (IT) Work Program (Exhibit C – Part Two) or any other procedures necessary to conclude upon the effectiveness of the company's ~~general controls~~ITGCs in mitigating the risks identified. All testing should be documented appropriately to ensure that the work may be referenced within the financial examination workpapers, as necessary.

~~After the information for planning the IT review has been gathered, including the ITPQ, the IT examiner should review the information obtained to assist in planning and determining the scope of the general IT risks to be reviewed. Some factors to consider as part of this process include:~~

Formatted: Strikethrough

Formatted: Strikethrough

- ~~The complexity of the insurer's information systems and IT risk mitigation strategies;~~
- ~~The extent to which reliance will be placed on those risk-mitigation strategies in the financial examination;~~
- ~~The length of time the existing system has been in place and any significant changes to the system;~~
- ~~The types of subsystems being used and how data is shared among systems;~~
- ~~The hardware and software being used and whether the software was internally or externally developed;~~
- ~~The extent to which the insurer outsources its IT functions;~~
- ~~Past issues the insurer may have had with its systems;~~
- ~~Answers provided from the insurer via the ITPQ;~~
- ~~Documentation available from other sources, including external and internal auditors;~~
- ~~The insurer's participation in electronic business and electronic data interchange;~~
- ~~The amount of reliance placed on the work of third parties;~~
- ~~The type, volume, and external availability of sensitive information that is processed and/or stored by the company and;~~
- ~~Changes to the company's controls and/or processes to ensure compliance with the General Data Protection Regulation (GDPR), if applicable, or other relevant data protection requirements.~~

~~The IT examiner should consider which risks included on the Evaluation of Controls in Information Technology (IT) Work Program (Exhibit C – Part Two) are applicable to the insurer under examination and determine if there are additional general IT risks that should be reviewed for this insurer. Additionally, based on the review of internal and external audit work, the IT examiner may determine that sufficient testing has been performed to fully address specific risks or areas of concern. In this case, the IT examiner may document in the IT planning memo their comfort with, and planned reliance on, the specific internal and/or external audit work included in the file. Additionally, the IT examiner need not include these specific risks or areas of concern in the IT work program.~~

3. ~~Request Insurer Control Information and Complete IT Review Planning~~Document Results of ITGC Review

At the conclusion of the ITGC review fieldwork (at or prior to the conclusion of planning of the financial examination process), the IT examiner should have a completed ITGC work program supported by documentation and testing as a deliverable. In addition, a summary of findings regarding the insurer's IT environment and ~~general IT controls~~ITGCs should be prepared at this time. These findings should be documented through the use of an ITGC review summary ~~report~~~~memo~~, memorandum (ITSM), which should include a description of recommendations to the company and/or how the findings may impact the financial examiner's reliance on ITGCs~~general IT controls~~ and approach to application control testing in Phase 3. The ~~review~~ITSM ~~summary memo~~ may also include a summary of the insurer's IT operations~~;~~ and detail ~~on~~of the IT review work performed. Based on the impact of the findings, the IT examiner should determine whether the ITGC environment is ~~generally~~ effective. An ~~generally~~ effective environment would indicate that IT risks have been sufficiently mitigated and findings are not pervasive enough to limit the ability to allow for testing of application controls in Phase 3.

From the IT examiner's perspective, controls over IT systems are considered ~~generally~~ effective when they maintain the integrity of information ~~and the security of the data that such systems process~~ and when they include effective ~~general IT controls~~ITGCs. Typically, at the end of the ITGC review, the ITGC environment would be considered generally effective, unless specific adverse findings summarized in the ITSM~~IT review summary memo~~ indicate otherwise. Professional judgement and skepticism should be exercised when making this determination. Often, even when issues are identified, the IT examiner may be able to determine that the finding is isolated to a specific system or point in time and, therefore, would not impact the overall reliability of the ITGC environment. In this case, the IT examiner should document in the ITSM ~~summary memo~~ which key activities or specific applications may be impacted by IT review findings and how.

Formatted: Strikethrough

Formatted: Strikethrough

Formatted: Strikethrough

Formatted: Strikethrough

Formatted: Strikethrough

Formatted: Strikethrough

Formatted: Strikethrough

In some instances, the overall ITGC environment may be deemed ineffective. In reaching this conclusion, the IT examiner should consider whether the findings outlined in the IT summary report:

- Are pervasive throughout the ITGC environment.
- Significantly impact the systems used in calculating and reporting financial results or the accuracy of information used in reaching major strategic decisions.
- Indicate deficiencies relating to management involvement and oversight of the IT strategy and direction.
- Are not alleviated by other mitigating factors or compensating controls.

If the ITGC environment is not deemed generally effective, the financial examiner may perform additional testing in later phases of the exam before relying on system generated reports or application controls in place of the insurer. The additional testing procedures should be designed to prove that the application control or system report is complete and correct despite the generally ineffective ITGC environment. Whether the ITGC environment is deemed generally effective ultimately depends on the IT examiner's professional judgment. To determine the impact of the ITGC review findings on the remainder of the examination, the IT examiner should next consider if the nature of the findings affects the quality of information produced by the company's applications and systems. For instance, a finding that the company has inadequate continuity management controls may be significant. However, such a finding would be unlikely to affect information produced by the company's IT systems. The IT examiner should assess ITGCs with regard to their effect on applications and data that become part of the financial statements or are used in making strategic business decisions.

The IT examiner may also consider performing additional procedures to determine the extent of the impact of specific findings. For instance, the company may have deficient user access controls. If the IT examiner is able to determine that in the period under examination, the key systems to the exam were not accessed inappropriately, the impact of the examination's findings may not substantively affect the examination in later phases of the exam beyond the reporting of the finding. Given the complexity of evaluating the impact of individual findings and/or findings in the aggregate, communication of the results and mitigating factors in the ITSM~~IT review summary memo~~ is important.

Formatted: Strikethrough

The IT examiner is cautioned against defaulting to the conclusion that the overall ITGC environment is ineffective, as such a conclusion could have a significant impact on the approach taken by the financial examiner on the remainder of the examination. For instance, in Phase 3, the financial examiner would be required to test manual or compensating controls for an identified risk if application controls cannot be relied upon and, therefore, may not be able to reach strong controls reliance. This may lead to additional detail testing in Phase 5 to fully address the identified risk. Additionally, the financial examiner would be required to test the accuracy and completeness of system generated reports, prior to those reports being utilized in addressing the identified risk in Phase 5.

The IT review process outlined up to this point, along with the corresponding documentation of results, may be performed on each examination, regardless of insurer size and complexity. These documents should also be appropriately presented and discussed with the examiner-in-charge to help facilitate a general understanding of the IT systems in place at the insurer and the impact that any findings may have on the ongoing exam.

As appropriate, significant ITGC findings should also be communicated to the insurer through management letter comments.

~~After the initial planning information has been gathered and reviewed, the Evaluation of Controls in Information Technology (IT) Work Program (Exhibit C – Part Two) to be utilized in the review should be created. As part of this process, the IT examiner should customize the standard work program to include only the general IT risks that are of concern for the insurer under examination. In addition to providing a list of risks in the work program, the IT examiner may wish to provide a list of common controls that indicate how a typical insurer may mitigate these risks to assist the insurer in developing its response. Finally, the IT examiner may consider prompting the insurer to include information supporting the IT controls in place to mitigate risks by including an information request in the work program distributed to the insurer. The IT review team should coordinate with the appropriate staff at the insurer to request a response. The insurer's response should indicate their controls in place to mitigate the risks identified in the work program. The IT examiner should review the company responses, considering the adequacy of the controls identified, and request evidence to test the effectiveness of the insurer's mitigating controls. The IT examiner may consider some of the examination procedures listed in the Evaluation of Controls in Information Technology (IT) Work Program (Exhibit C – Part Two), and complete the planning of the IT review.~~

~~After the work program has been finalized, the IT examiner should document the plan to complete the IT review. The plan should document the staffing to be used to complete the review, the scope of work to be performed and a proposed budget to complete the review. The plan should be subject to the review and approval of the EIC and additional examination supervisors, as considered appropriate by the state. This plan may be documented through the use of an IT review planning memo, or other workpaper that documents the approval of the EIC.~~

4. ~~Conduct IT Review Fieldwork~~Prospective Cyber Risk Information Gathering and Planning

The first step in the prospective cybersecurity risk assessment is to gather and review the information necessary to plan the cybersecurity review of the insurer. Any additional cybersecurity-related information will be requested during this step. For some examinations, all information required might have already been collected during ~~s~~Step 1. Previous work for ITGC reliability determination and third-party work (e.g., internal audit work, external audit work, self-assessments, third-party assessments, penetration tests, security reviews, etc.) may be leveraged to the extent possible.

After the information for planning the cybersecurity review has been gathered, the IT examiner should review the information obtained to assist in planning and determining the scope of the prospective cybersecurity risks to be reviewed. The IT examiner's understanding of the insurer should be used to determine which risks included in Exhibit C – Part Three are applicable to the insurer under examination. The IT examiner may consider additional risks that have not been included within Exhibit C – Part Three.

After the cybersecurity planning information has been gathered and reviewed, the Prospective Cyber Risk Evaluation of Controls Work Program (Exhibit C – Part Three) ~~should be~~ utilized in the review should be created. As part of this process, the IT examiner should customize the work program to include only the prospective cybersecurity risks that are of concern for the insurer under examination. This information should be used to develop a risk-focused testing plan based on elements of COBIT 2019 and the NIST CSF 2.0 framework by customizing the Prospective Cyber Risk Evaluation of Controls Work Program (Exhibit C – Part Three). The scope of the assessment should be carefully tailored to the examination and according to the insurer's nature, size, complexity, and risk profile as well as consideration of the materiality of potential risks.

The possible controls, preliminary information requests, and test procedures included with Exhibit C – Part Three are not designed to be an all-inclusive list and may not apply to every insurer. If the insurer's controls do not correspond to those identified within Exhibit C – Part Three, the IT examiner should not use the

possible preliminary information requests and test procedures provided with the exhibit. In this case, the IT examiner should develop alternative requests and procedures based on how the insurer mitigates the identified risk.

At the end of this step, the cyber risk assessment planning documentation should be completed in preparation for fieldwork. The plan should document the scope of work to be performed, risks selected for review, and the extent to which reliance will be placed on previously completed work. This plan may be documented through the use of a Cybersecurity Planning Memorandum, or other workpaper that documents the approval of the EIC.

~~The IT examiner should schedule examination fieldwork, with the initial fieldwork to include conducting interviews of key IT staff. These interviews should serve as an opportunity to substantiate and clarify some of the information provided by the insurer in Exhibit C – Part Two. The IT examiner may also gain additional information relating to key activities, risks, and risk mitigation strategies for the financial examination. As such, the IT examiner may want to invite the examiner-in-charge and/or other financial examination staff to participate in the interview process. Some of the potential candidates for interview include the Chief Information Officer, Chief Technology Officer, Chief Security Officer, System Architect, Chief System Engineer, and any other individuals responsible for maintaining, updating and testing the insurer's business continuity and disaster recovery plans. Example agenda items for IT interviews, subject to the areas of expertise for the interviewee, include but are not limited to:~~

- ~~IT Strategic Planning;~~
- ~~IT Governance;~~
- ~~Leadership development and succession planning;~~
- ~~Organizational structure;~~
- ~~Risk management;~~
- ~~Development and maintenance of policies;~~
- ~~Budgeting;~~
- ~~Security;~~
- ~~E-Business;~~
- ~~Business continuity;~~
- ~~Acquisitions and integration;~~
- ~~Architecture, development and implementation of major programs;~~
- ~~External environment, and~~
- ~~Any other items necessary to evaluate the insurer's general IT controls.~~

~~After the IT review team has completed the interviews, the team should begin to test the general controls identified by the insurer. This work should be completed with the assistance of the insurer's IT staff and should utilize the existing work of others, if deemed appropriate. As noted in step 2 above, if the IT examiner has determined that reliance will be placed on all or some of the work performed by CPAs or the company's internal audit function (if deemed independent) to fully address a specific risk or area of concern, the IT examiner would not be required to include those specific risks or areas of concern on the work program. However, if the IT examiner determines that the work performed by the third-party only partially addresses a risk, but additional work would be required to fully address that risk, the IT examiner should include the relevant third-party documentation in the file and map or link it to the respective risk in the work program.~~

~~While it is expected that audit work (external/internal) would be the most common type of work relied on by the exam team, work performed by other regulatory agencies and/or cybersecurity experts may also be leveraged to reduce the independent work performed during an exam. Regardless of the work being reviewed, state insurance regulators should specifically consider the scope of work, the independence, and~~

~~qualifications of the entity (or person) performing the work, the timing of the work performed, and the findings included in any report received. Qualifications should be evaluated based on the training, experience and education of personnel performing the work (see Section 1-2 Letter E for more information on the use of specialists). Based on the state insurance regulators' review of the third-party work, state insurance regulators may be able to use the work to enhance the risk assessment, interview, and scoping process performed during the IT review. While the IT examiner is responsible for performing his/her own independent risk assessment, third-party work that directly addresses an identified risk may be relied upon in a similar manner to external/internal audit work. In this case, the IT examiner should briefly document his/her understanding of the third-party testing performed and any conclusions reached from the testing procedures. To the extent that findings are noted in the report obtained, state insurance regulators may find it more useful to corroborate the remediation of the findings as opposed to performing an independent review of the company's controls to confirm the findings' existence.~~

~~After considering the utilization of existing work, testing of general IT controls and other procedures should be performed in order to gain an appropriate level of understanding of the insurer's IT environment and the effectiveness of general IT controls in place. As noted above, the IT examiner may consider performing examination procedures listed in the Evaluation of Controls in Information Technology (IT) Work Program (Exhibit C – Part Two) or any other procedures necessary to conclude upon the effectiveness of the company's general controls in mitigating the risks identified. All testing should be documented appropriately to ensure that the work may be referenced within the financial examination workpapers, as necessary.~~

5. ~~Document Results of IT Review~~Conduct Prospective Cyber Risk Assessment

The IT examiner should perform procedures necessary to evaluate the insurer's prospective cybersecurity risks. Fieldwork performed during this step should focus on the risks and controls included within the customized Prospective Cyber Risk Evaluation of Controls Work Program (Exhibit C – Part Three). The IT examiner should utilize the existing work of others, if deemed appropriate.

After considering the utilization of existing work, testing of cybersecurity controls and other procedures should be performed in order to gain an appropriate level of understanding of the insurer's cybersecurity environment and the effectiveness of controls in place to mitigate prospective cybersecurity risks. The IT examiner may consider performing examination procedures included within the Prospective Cyber Risk Evaluation of Controls Work Program (Exhibit C – Part Three) and, where appropriate, additional procedures tailored to the insurer's specific cybersecurity risks and controls.

This work should apply elements of COBIT 2019 and the NIST CSF 2.0 framework to evaluate the insurer's forward-looking cybersecurity posture using professional judgment. Testing should be conducted for controls specifically related to cybersecurity risk and should be used to help assess the effectiveness of the insurer's Govern, Identify, Protect, Detect, Respond, and Recover capabilities.

The prospective cyber risk assessment should be completed prior to the conclusion of Phase 5 and should result in an assessment of prospective cyber risk exposure being provided to the financial examination team and financial analyst in accordance with the current prospective risk assessment guidance outlined in Exhibit V of the Financial Condition Examiners Handbook.

~~At the conclusion of the IT review fieldwork (at or prior to the conclusion of planning of the financial examination process), the IT examiner should have a completed IT controls work program supported by documentation and testing as a deliverable. In addition, a summary of findings regarding the insurer's IT environment and general IT controls should be prepared at this time. The findings may be considered prospective in nature (resulting in recommendations to the company or communication to the exam team)~~

~~or current in nature (which may have an impact on the financial exam). These findings should be documented through the use of an IT summary report (or similar document), which should include a description of recommendations to the company and/or how the findings may impact the examiner's reliance on general IT controls and approach to application control testing in Phase 3. Findings that are prospective in nature can be passed to the exam team for inclusion in the testing of prospective risks performed on Exhibit V. The IT summary report may also include a summary of the insurer's IT operations, and detail on the IT review work performed. Based on the impact of the findings, the IT examiner should determine whether the ITGC environment is generally effective. A generally effective environment would indicate that IT risks have been sufficiently mitigated and findings are not pervasive enough to limit the ability to allow for testing of application controls in Phase 3.~~

~~From the IT examiner's perspective, controls over IT systems are considered generally effective when they maintain the integrity of information and the security of the data that such systems process and when they include effective general IT controls and application controls. Typically, at the end of the IT review, the ITGC environment would be considered generally effective, unless specific adverse findings summarized in the IT summary memorandum indicate otherwise. Professional judgement and skepticism should be exercised when making this determination. Often, even when issues are identified, the IT examiner may be able to determine that the finding is isolated to a specific system or point in time and, therefore, would not impact the overall reliability of the ITGC environment. In this case, the IT examiner should document in the IT summary memo which key activities or specific applications may be impacted by IT review findings and how.~~

~~In some instances, the overall ITGC environment may be deemed ineffective. In reaching this conclusion, the IT examiner should consider whether the findings outlined in the IT summary report:~~

- ~~Are pervasive throughout the ITGC environment.~~
- ~~Significantly impact the systems used in calculating and reporting financial results or the accuracy of information used in reaching major strategic decisions.~~
- ~~Indicate deficiencies relating to management involvement and oversight of the IT strategy and direction.~~
- ~~Are not alleviated by other mitigating factors or compensating controls.~~

~~If the ITGC environment is not deemed generally effective, the examiner may perform additional testing in later phases of the exam before relying on system generated reports or application controls in place of the insurer. The additional testing procedures should be designed to prove that the application control or system report is complete and correct despite the generally ineffective ITGC environment. Whether the ITGC environment is deemed generally effective ultimately depends on the IT examiner's professional judgment. To determine the impact of the IT review findings on the remainder of the examination, the examiner should next consider if the nature of the findings affects the quality of information produced by the company's applications and systems. For instance, a finding that the company has inadequate continuity management controls may be significant. However, such a finding would be unlikely to affect information produced by the company's IT systems. The IT examiner should assess ITGCs with regard to their effect on applications and data that become part of the financial statements or are used in making strategic business decisions.~~

~~The examiner may also consider performing additional procedures to determine the extent of the impact of specific findings. For instance, the company may have deficient user access controls. If the examiner is able to determine that in the period under examination, the key systems to the exam were not accessed inappropriately, the impact of the examination's findings may not substantively affect the examination in later phases of the exam beyond the reporting of the finding. Given the complexity of evaluating the impact of individual findings and/or findings in the aggregate, communication of the results and mitigating factors in the IT Summary Conclusion Memorandum is important.~~

~~The IT examiner is cautioned against defaulting to the conclusion that the overall ITGC environment is ineffective, as such a conclusion could have a significant impact on the approach taken by the financial examiner on the remainder of the examination. For instance, in Phase 3, the examiner would be required to test manual or compensating controls for an identified risk if application controls cannot be relied upon and, therefore, may not be able to reach strong controls reliance. This may lead to additional detail testing in Phase 5 to fully address the identified risk. Additionally, the examiner would be required to test the accuracy and completeness of system generated reports, prior to those reports being utilized in addressing the identified risk in Phase 5.~~

~~The IT review process outlined up to this point, along with the corresponding documentation of results, may be performed on each examination, regardless of insurer size. These documents should also be appropriately presented and discussed with the examiner-in-charge to help facilitate a general understanding of the IT systems in place at the insurer and the impact that any findings may have on the ongoing exam.~~

6. ~~Assist in Financial Examination~~Document Results of Cybersecurity Assessment

At the conclusion of the prospective cybersecurity risk assessment, the IT examiner should have a completed Prospective Cyber Risk Evaluation of Controls Work Program (Exhibit C – Part Three) supported by documentation and testing as a deliverable. In addition, a summary of findings regarding the insurer's cybersecurity environment and prospective cybersecurity risks should be prepared at this time. These findings should be documented through the use of a Cybersecurity Review Summary Memorandum (CRSM), which should include a description of recommendations to the company and how the findings may impact the insurer's prospective cybersecurity risk profile. The CRSM should also include a summary of the insurer's cybersecurity environment and ~~detail~~details on the cybersecurity work performed.

After considering the insurer's inherent exposure to prospective cybersecurity risks (e.g., nature of operations or sensitivity to data), as well as the controls and mitigating strategies in place, the IT examiner should determine the insurer's Cybersecurity risk assessment level and trend. In making this determination, the IT examiner should consider the guidance contained within the Summary Review Memorandum (Exhibit AA), the impact of the identified findings, and any mitigating factors present. The IT examiner should not default to a particular risk assessment level or trend, but should reach a conclusion based on the specific facts and circumstances of the insurer under examination. The IT examiner should consider the impact of the findings in totality and identify any monitoring or follow-up activities that may be relevant until the next examination.

The IT examiner should assist the financial examination team in translating significant cybersecurity findings and recommendations into the Summary Review Memorandum (Exhibit AA) and other appropriate examination communications. Findings that require continued monitoring or future follow-up may also be communicated to the financial analyst, as appropriate. Management letter comments should be developed, as appropriate, to communicate significant cybersecurity findings and recommendations to the insurer.

7. Assist in Financial Examination

Following the completion of the IT review the IT examiners involved in the IT review should remain available to assist in the completion of the financial portion of the examination. Such assistance could include data mapping, ~~ACL~~ data analytics testing, clarification of work performed during the IT review, assistance in completing the examination report and/or management letter, and additional assistance in identifying and testing IT prospective risks and IT application controls to mitigate risks identified by the financial examination team.

Although the identification and assessment of risk mitigation strategies is the responsibility of the examination team as a whole, the IT examiners may have additional insight and experience that may be beneficial in identifying and testing IT controls associated with particular insurer applications and IT prospective risks. This could include adding IT prospective risks (including emerging technology risks and their potential impact) to Exhibit V. The involvement of IT examiners in this area of the examination may be especially beneficial when examining companies with internal controls that may allow the examination team to reduce substantive testing. IT examiners can also be used to consult on Exhibit V IT prospective risks to which their expertise may be pertinent.

Cybersecurity Considerations

As the IT examiner reviews an insurer's operations, he or she may determine that the insurer has significant exposure to cybersecurity risks. The specific risk exposure for the insurer may vary based on volume, type of sensitive information or nonpublic information. ~~(e.g.,nonpublic information, including personally identifiable information, personal financial information, protected health information, and nonpublic personal information, etc.). Social Security numbers, protected health information, personally identifiable health information, etc.)~~ and the broad security environment in which the insurer is operating. The IT examiner should be mindful that the insurer is not required to use any particular IT security framework, nor are its IT security systems or controls required to include all of the components of any single or particular IT security framework or the IT examiner's work program. The examiner should broadly consider not only the volume and type of sensitive information obtained, maintained, or transmitted by the insurer, but also the laws and regulations to which the insurer is subject, as well as the size and complexity of the insurer's operations and the nature and scope of its activities. All of these factors will influence the cybersecurity policies and systems and the IT security framework or frameworks that are appropriate for a particular insurer to effectively protect its sensitive information. As a result, responding to a particular insurer's risk will require judgment by the IT examiner in tailoring the use of existing Handbook guidance. When performing this assessment, the IT examiner should use Exhibit C – Part Three as a resource in identifying relevant cybersecurity risks. The IT examiner should evaluate at least one risk from each NIST CSF 2.0 Function within Exhibit C – Part Three. IT examiners should review the insurer's risk mitigation strategies and/or controls that identify cybersecurity risks to protect against and detect cybersecurity incidents and respond to and recover from cybersecurity incidents when they do occur.

When assessing the level of an insurer's cybersecurity controls/processes, the IT examiner should take into account the distinction between the roles of the insurer's board of directors and its senior management. The IT examiner should recognize that, while it is the role of the board to understand and oversee the insurer's cybersecurity policies, systems, and controls, it is the role of its senior management to implement the insurer's cybersecurity policies and to ensure the performance and outcomes of the insurer's risk mitigation strategies and controls are appropriate. ~~Strategies and controls should identify, protect against, and detect cybersecurity incidents, as well as allow the insurer to respond/recover from such incidents.~~ Each of the primary information security functions ~~are~~ is described below:

- Govern - The Govern function guides an organization on how to prioritize and achieve the outcomes of the other five functions and ensures cybersecurity aligns with the insurer's mission and stakeholder expectations, making it a critical part of the broader enterprise risk management strategy. Govern focuses on understanding the business context, building a cybersecurity strategy, managing supply chain risks, defining organizational roles and policies, and providing oversight.

- Identify - The identification of cybersecurity risks is important in helping the organization understand the best way to deploy its limited resources. Internal risk assessment is crucial for organizations to understand constantly evolving risks. Participation in information networks, though not required, is likely to enhance understanding of risks. In a robust control environment, insurers devote resources to a risk assessment process that includes some amount of management/board involvement, appropriate to the distinct roles of

© 2026 National Association of Insurance Commissioners

the board and senior management, as well as a sufficient level of technical expertise to ensure that issues are well understood and responded to appropriately.

- Protect - Protection is an important element in the overall strategy for any risk and cybersecurity is no exception. A robust risk mitigation strategy may include a combination of strong policies, system and network access controls, and data security protection (e.g., encryption of~~-~~ data ~~-~~at ~~-~~rest, in use, in transit, and in storage~~ are protected, etc.~~), as appropriate to the broad security environment in which the insurer is operating, including the volume and type of sensitive information obtained, maintained, or transmitted by the insurer, the security laws and regulations to which it is subject, its size and complexity, and the nature and scope of its activities. When applicable, controls should directly address risks presented by third ~~-~~party access to the insurer's network, systems and data (including access by vendors, agents, brokers, third-party administrators [TPAs] and managing general agents [MGAs]). Training is also an important part of the insurer's response to cybersecurity risks, as many incidents occur due to improper execution of controls, rather than the lack of controls. Control effectiveness is limited if employees are not provided adequate training to understand the objectives and importance of their assigned responsibilities.

- Detect - Insurers should also have a strong set of detective controls that enable timely identification and mitigation of threats to the organization. These may include anti~~-~~virus and anti~~-~~malware software as well as network monitoring and intrusion detection related processes and controls. Organizations may perform vulnerability scans and penetration tests to ensure that weaknesses in the protective/detective controls are identified and addressed.

- Respond and Recover - A review of the insurer's incident response plan is an important consideration in the overall assessment of an insurer's cybersecurity~~ at an insurer~~. The response to a cybersecurity incident may leverage concepts from the insurer's broader disaster recovery plan but may also require unique considerations since recovering from a cybersecurity incident requires a different response than recovering from an environmental incident (e.g., fire, earthquake, tornado, etc.). The examiner should note, however, that network threats and incidents are not rare events like environmental incidents. It is also important that people with assigned responsibilities within the disaster recovery plan have the necessary background/training to perform the assigned duties. Insurers should include in their plan who they are required to contact in the event of a security incident (regulators, affected parties, etc.) and how public relations will be managed to limit the impact of the incident on the organization's reputation. Importantly, response plans should be tested to ensure that the organization is ready to deploy the plan in the event of an actual incident.

  When significant incidents do occur, it is important that the insurer performs a thorough post-remediation analysis and restores services that were affected as a result of the incident in accordance with the response plan. ~~Examination teams~~ The IT examiner may consider reviewing incident reports to consider how the organization has learned and adapted when security protocols are breached.

Depending on the insurer's operations, there may be unique risks that the IT examiner identifies for further review. For instance, some insurers may leverage controls at service providers to provide assurance over cybersecurity risks. While this may be appropriate, insurers should be able to confirm that the service provider has appropriate risk mitigation~~s~~ strategies and controls in place and that appropriate protections are built into their service agreement (e.g.,~~-~~ indemnification clauses, right to audit, technology errors and omissions insurance coverage, etc.) to address the risks presented to the insurer.

Although uncommon, if the IT examiner determines that the insurer has significant exposure to cybersecurity risk, the IT examiner may consider incorporating the use of a cybersecurity expert to assist in performing cybersecurity

procedures. The specific risk exposure assessment for the insurer should be based on the IT examiner's judgment and may consider the insurer's line of business, the size and complexity of operations, known cybersecurity incidents; risks presented by third-party access to the insurer's network systems and data, recent mergers and acquisitions, concerns about the controls in place to protect against, detect, respond and recover from cybersecurity incidents, or any other significant risk factors related to cybersecurity. Note that the decision to use additional expertise to address cybersecurity concerns should be based on the accumulation of circumstances and not necessarily due to any one situation discussed above.

The following insights may assist regulators and/or cybersecurity experts as they assess the strength of the insurer's security program and therefore the risk that cybersecurity events present to the insurer. These insights are for informational purposes and are not intended to be requirements for insurers. Companies may be assessed by their individual risk profile and the organization's risk strategy.

Events, Incidents and Breaches

As regulators engage insurers in discussion regarding past cybersecurity events, it may be useful to understand the difference between various types of events. A "cybersecurity event" can be defined as an event resulting in unauthorized access to, disruption or misuse of an information system or information stored on such an information system. Insurance companies may also use terms such as incidents and breaches or may distinguish between successful and unsuccessful events as they discuss their cybersecurity program. Regardless, regulators should gain an understanding of how the insurer defines its events and incidents. Insurers should consider both unsuccessful cybersecurity events and successful cybersecurity events (incidents), as appropriate. For instance, while an unsuccessful event may only access the company's network without accessing sensitive information, it may still represent an event that the insurer should consider, correlate with other activity, and learn from to ensure security practices are enhanced, as appropriate. Timely, effective incident response is extremely critical in minimizing the impact of a cybersecurity incident.

Integration of Cybersecurity Risk into Enterprise Risk Management

As noted before, an insurer's board and/or senior management often play a significant role overseeing a cybersecurity program. As an insurer's cybersecurity risk increases, examination teams may want to scrutinize the integration of cybersecurity risk into the insurer's Enterprise Risk Management. This may include consideration of the level of information provided to the board and/or senior management and the appropriateness of the insurer's risk identification and assessment process. It may be appropriate for board and/or senior management to receive summary level information, but there should be a designated person with cybersecurity expertise that is responsible for developing the insurer's response to mitigate cybersecurity risks. This person should be deemed the insurer's cybersecurity risk owner and should receive information that is tailored to the insurer's specific cyber risk exposures. For instance, use of third-party service providers, integration of acquired companies, legacy systems, etc. may all represent unique exposures that require specific consideration as mitigation strategies are developed.

Information Security Program

Note: The guidance that follows should only be used in states that have enacted the NAIC *Insurance Data Security Model Law* (#668). Moreover, in performing work during an exam in relation to the Model #668, it is important the examiners first obtain an understanding and leverage the work performed by other units in the department, including, but not limited to, market conduct-related work.

Specific requirements related to an insurance company's information security program are included in Model #668. States that have passed the law may have an enhanced ability to encourage remediation of control issues in relation to issues identified during the exam. To the extent a state has adopted Model #668 and it is in effect at the time of

the examination, IT examiners may consider tailoring the IT review to include consideration of the items below. As evidenced below, implementation of each control identified for consideration shall be done based on the insurer's individual risk assessment:

Section 4-C of Model #668 details the requirements for performing a risk assessment. As part of a risk assessment, the licensee shall perform the following:

1. Designate one or more employees, an affiliate or an outside vendor designated to act on behalf of the licensee who is responsible for the Information Security Program.

2. Identify reasonably foreseeable internal or external threats that could result in unauthorized access, transmission, disclosure, misuse, alteration or destruction of nonpublic information, including the security of information systems and nonpublic information that are accessible to, or held by, third-party service providers.

3. Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the nonpublic information.

4. Assess the sufficiency of policies, procedures, information systems and other safeguards in place to manage these threats, including consideration of threats in each relevant area of the licensee's operations, including:

    a. Employee training and management.

    b. Information systems, including network and software design, as well as information classification, governance, processing, storage, transmission, and disposal.

    c. Detecting, preventing and responding to attacks, intrusions or other systems failures.

5. Implement information safeguards to manage the threats identified in its ongoing assessment, and no less than annually, assess the effectiveness of the safeguards' key controls, systems and procedures.

Based on this risk assessment, Section 4-D requires the licensee to execute the following:

1. Design its Information Security Program to mitigate the identified risks, commensurate with the size and complexity of the licensee's activities, including its use of third-party service providers, and the sensitivity of the nonpublic information used by the licensee or in the licensee's possession, custody or control.

2. Determine which security measures listed below are appropriate and implement such security measures.

    a. Place access controls on information systems, including controls to authenticate and permit access only to authorized individuals to protect against the unauthorized acquisition of nonpublic information.

    b. Identify and manage the data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes in accordance with their relative importance to business objectives and the organization's risk strategy.

    c. Restrict access at physical locations containing nonpublic information only to authorized individuals.

© 2026 National Association of Insurance Commissioners

d. Protect by encryption or other appropriate means all nonpublic information while being transmitted over an external network and all nonpublic information stored on a laptop computer or other portable computing or storage device or media.
e. Adopt secure development practices for in-house developed applications utilized by the licensee and procedures for evaluating, assessing, or testing the security of externally developed applications utilized by the licensee.

f. Modify the information system in accordance with the licensee's Information Security Program.

g. Utilize effective controls, which may include multifactor authentication procedures for any individual accessing nonpublic information.

h. Regularly test and monitor systems and procedures to detect actual and attempted attacks on, or intrusions into, information systems.

i. Include audit trails within the Information Security Program designed to detect and respond to cybersecurity events and designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the licensee.

j. Implement measures to protect against destruction, loss, or damage of nonpublic information due to environmental hazards, such as fire and water damage or other catastrophes or technological failures.

k. Develop, implement, and maintain procedures for the secure disposal of nonpublic information in any format.

3. Include cybersecurity risks in the licensee's ERM process.

4. Stay informed regarding emerging threats or vulnerabilities and utilize reasonable security measures when sharing information relative to the character of the sharing and the type of information shared.

5. Provide its personnel with cybersecurity awareness training that is updated as necessary to reflect risks identified by the licensee in the risk assessment.

Review ~~section~~ Section 3 of ~~the~~ Model #668 for legal definitions of relevant and commonly used terms. For purposes of the exam process, licensees include, but are not limited to, insurance companies. Model #668 also covers the topics of board of directors oversight, third-party service providers, program adjustments, incident response plan, and the annual certification to the commissioner of the domiciliary state. Review Model #668 language for further insights on the topics above.

Evaluating Employee Training / Security Awareness Programs

Employees often represent the front line of any strong security program. However, without proper training, employees may also represent vulnerability in the company's defense program. Therefore, strong security awareness training can help in mitigating the risk presented by phishing e-mails and other social engineering attacks. Strong security awareness training may be characterized by:

- Use of ~~real world~~real-world examples to help users be able to identify phishing e-mails;
- Use of phishing emails sent to the user community by the insurers internal security specialists or security vendor to measure effectiveness of user training;
- A clear protocol that provides employees help in identifying and reporting phishing e-mails; and

- Elements of ~~a~~ training that are tailored to the employee's specific roles, responsibilities, and access rights.

Since cybersecurity threats are constantly evolving, it is important to have a strong and up-to-date training regimen. Additionally, in a strong cybersecurity program trainings should be performed on a consistent and periodic (e.g., annually) basis to ensure the information reaching the employees is commensurate with the modern-day threats facing the company. As regulators evaluate the appropriateness of the program, they should consider whether the training is mandatory for all employees and whether it includes procedures and instructions for employees to follow in the event that the employee has a good faith, fact-based belief that a breach or cybersecurity event may have occurred.

Vulnerability Management

In the most robust information security programs, companies understand that not all vulnerabilities can be eliminated, typically due to business needs or time and resources. However, companies should have an understanding and should inventory their identified vulnerabilities as well as have a plan to ensure vulnerabilities that can't be eliminated are mitigated as much as possible. For instance, if the insurer is unable to confirm that a third-party service provider is able to secure their own access to the company's information system, the company should ensure they monitor the service provider's access to determine if improper activity occurs on the company's network. As many vulnerabilities originate with a company's patching practice, it is important that regulators obtain an understanding of the company's patch management. Research suggests that in any given year, the majority of breaches have a root in a Common Vulnerability and Exposure (CVE) that often has been known and identified for several years. An insurer should maintain a strong practice of patch management, or at least a practice of understanding and mitigating existing vulnerabilities as an important part of a robust security program. For vulnerabilities discovered between exam periods, the NAIC maintains a "Cybersecurity Vulnerability Response Plan" document on the Information Technology (IT) Examination (E) Working Group web page with company questions and follow-up procedures to learn more about the extent of the vulnerability, how that information can be used going forward, and possible actions to be taken, if warranted (e.g., targeted exam procedures, additional interim procedures, etc.).

Ransomware

Ransomware is one of the more common manifestations of a cybersecurity risk. Ransomware attacks pose a significant risk to confidentiality and availability of company data. It is difficult to predict when and where a ransomware attack will strike, so it is important for a company to maintain strong cyber hygiene habits to stay ready for ransomware attacks. At a minimum, insurers with good cyber hygiene do the following:

- Patch their systems/networks regularly, in a timely manner, and in accordance with application updates.
- Require strong passwords, and, where appropriate, multi-factor authentication.
- Have information security awareness training, including email filtering and anti-phishing training for employees, with periodic phishing test campaigns.
- Monitor and react to suspicious activity on their network.
- Have system backups that are stored in an air-gapped, immutable environment that is inaccessible from the internet; this backup can be quickly deployed in the event the production environment is infected. Companies should test backup deployment regularly.
- Have firewalls, or other mechanisms within the network, so someone with unauthorized access cannot move laterally.
- Limit user access rights to the minimum necessary to perform their job.
- Have and test a robust incident response plan.

Company Acquisitions

Finally, in situations where a company has recently acquired/integrated another company, the IT examiner should also pay special attention to the procedures performed in integrating company systems. This is often when

companies are most vulnerable to cybersecurity threats as controls are often in flux and mistakes in integration may create vulnerabilities that are not easily identified or remedied.

Exhibit C – Part Three is a Cybersecurity Risk Repository, which can be used to help ensure the examination appropriately addresses identified cybersecurity risks. The IT examiner should also consider overlap with security assessment and threat analysis procedures included within Exhibit C – Part Two, as applicable, when evaluating risks associated with recently acquired or integrated entities. ~~Exhibit C, Part Two (Instruction Note 3) includes specific mention of risk statements and sections of the exhibit that can be applied to ensure the examination has an appropriate response to identified cybersecurity risks.~~

Note that the findings identified through the review of the company's cybersecurity control environment should be communicated to the financial examiner via the CRSM~~IT Summary Memo~~.

Uniformity of Data for Timely and Efficient Transfer

Legacy systems with uncommon and difficult-to-access data structures should be flagged for further investigation as part of the IT review. Companies with multiple IT platforms, multiple cloud storage providers, or that rely on ~~managing general agents (MGAs)~~MGAs or ~~third-party administrators (TPAs)~~TPAs may be at a higher risk, especially if their data is stored in a commingled environment. The ability to migrate and transfer data may be relevant in a number of scenarios, including switching service providers, merging with or acquiring another company, company insolvency necessitating the transfer of policyholder data to the guaranty fund, etc. If the data is found to be in a format that is not conducive with timely and efficient data transfer, the IT examination team is encouraged to notify the insurer to discuss data migration and the possible need for a more uniform data standard (e.g., NAIC Uniform Data Standards [UDS] for property/casualty ~~(~~[P/C]~~)~~ companies). The IT examination team may also review contracts with third-party data storage providers for clauses on data transfer rights. The solvency outlook of the company may be considered when discussing if data migration to a more uniform format is necessary. See DSS 01.01 in Exhibit C for common controls~~;~~, information requests~~;~~, and possible procedures regarding the quality, timeliness, and availability of data. In summary, the data should be stored in a format that allows it to be accessed, utilized, and efficiently transferred, if necessary.

Note: While NAIC UDS apply specifically to P/C companies, all companies should have the ability to export claims data through a defined format that would allow the data to be received and utilized by a third-party guaranty fund, if necessary. See the *NAIC Uniform Data Standard Operations Manual* for more information. This manual is maintained by the National Conference of Insurance Guaranty Funds (NCIGF). The following sections would be most applicable to examiners:

- A Record Extended Table Appendix: IX
- B Record Extended Table Appendix: XIX
- G Record Extended Table Appendix: LVIII
- F Record Extended Table Appendix: LIV
- I Record Extended Table Appendix: LXV
- Coverage Codes: 15-1
- Transaction Codes: 14-1
- Other Code Tables: 16-1

Customization for Small Companies

When conducting an IT review of a small company or a company with a non-complex IT environment, it is acceptable to limit the extent of test procedures performed. However, the examination must adhere to the seven~~six~~-step process outlined above. This includes obtaining the ITPQ responses from the insurer, completing a basic work program, ~~and~~ preparing a summary memo concluding on the results of the IT review and its impact on the rest of the examination, and preparing a CRSM.

Formatted: Not Strikethrough

The most significant area to be customized for small insurers is the IT work program. Regardless of size or complexity, some level of testing is required to be performed to verify the design and operating effectiveness of the insurer's IT environment; however, the presentation of such work may vary. ~~It is recommended that~~ IT examiners should consider performing some level of review for ~~IT general controls~~ ITGCs~~-~~ in place within each domain of the COBI~~i~~T Framework and each function of the NIST CSF 2.0 Framework. This may be shown using a customized version of Exhibit C – Part Two, where a limited number of controls applicable to the insurer are populated and reviewed. In limited circumstances, as described below, IT examiners may bypass the utilization of Exhibit C – Part Two:

1. If the CPAs or the company's internal audit function (if deemed independent) ~~have~~ has performed a review of ITGCs that sufficiently cover risks within each of the ~~COBiT~~ COBIT domains, the IT examiner may rely on such work without mapping or linking the work to a separate work program. However, the IT examiner must document their comfort with and planned reliance on the work performed.

2. When the IT environment is simplistic and the insurer utilizes purchased software programs from well-known vendors, IT examiners may choose to summarize, in memo format, the procedures performed for each domain of the ~~COBiT~~ COBIT Framework. However, before determining that it is appropriate to bypass the utilization of Exhibit C, IT examiners should consider whether the company has made significant modifications to the software being used, as modifications may impact the software's reliability. In situations where significant modifications have been made and continue to be made, IT examiners should utilize Exhibit C – Part Two to document an understanding of controls ~~consideration of risks~~ relating to change management.

B. Materiality

The examiners should consider materiality ~~before~~ during planning ~~and~~ , while conducting examination procedures, and when evaluating the ~~results of those procedures~~impact of findings on the financial examination.~~-~~ Materiality is defined as the dollar amount above which the examiner's perspective of the company's financial position will be influenced. It is determined at two levels during the initial planning stage: (1) an overall level as it relates to the annual statement taken as a whole; and (2) an individual balance (annual statement line item) level.

----------Detail Eliminated for Spacing Purposes----------

VII. SPECIAL CONSIDERATIONS FOR RISK RETENTION GROUPS

This section covers procedures and considerations that are important when conducting financial condition examinations of risk retention groups. The discussion here is divided as follows:

A. Background
B. Examination Coordination
C. Risk-Focused Examination Considerations
    1. Corporate Governance Assessment
    2. Conducting Interviews
    3. Consideration of Information Technology (IT) Risks
    4. Identification and Testing of Controls

A. Background

----------Detail Eliminated for Spacing Purposes----------

B. Examination Coordination

----------Detail Eliminated for Spacing Purposes----------

C. Risk-Focused Examination Considerations

Although RRGs are unique in both size and reporting, they are still required to be subjected to the risk-focused surveillance process. There are some areas that will require modification to the risk-focused examination process; however, in general, the examination of an RRG should be very comparable to that of a standard insurer.

For an examination of an RRG, examiners should gain an understanding of the company, as required in Phase 1. Based upon that understanding, the examiner should identify the key functional activities of the RRG. Within Phase 1, the examiners are expected to assess the corporate governance of an insurer, as well as conduct management interviews. This must be completed for all insurers, including RRGs; however, there may be some unique considerations with regard to these procedures as discussed below.

After the key functional activities have been identified as part of Phase 2 procedures, the examiner would identify and document the inherent risks of the RRG. The examiners should then utilize professional judgment to assess the inherent risk by determining the likelihood of occurrence and magnitude of impact to obtain the overall inherent risk assessment for each identified risk.

Phase 3 requires the examiner to identify and evaluate controls in place to mitigate inherent risks. As with small insurers, many RRGs will not have extensive documentation surrounding internal controls. Examiner considerations in regard to identification and testing of controls for RRGs is discussed below.

The remainder of the RRG exam (Phases 4–7) should follow the general guidance for risk-focused exams as outlined in Section 2 of this Handbook.

----------Detail Eliminated for Spacing Purposes----------

3. Consideration of Information Technology (IT) Risks

    Consideration should be given to the information technology used by all insurers, including RRGs. Section 1 of this Handbook describes a seven-step General IT Review process. Auditors should utilize this process, along with the Exhibit C – Part Two Evaluation of Controls in Technology work program and the Exhibit C – Part Three Prospective Cyber Risk Evaluation of Controls Work Program, on all examinations. For RRGs that do not maintain any significant automated accounting functions, it may not be practical to conduct an in-

depth review of the IT function; however, as the Exhibit C work program allows for extensive customization to meet the needs of each IT review, it should be modified and used regardless of the depth of review. The modifications to Exhibit C would eliminate any IT risks that are not of concern for the RRG under examination. This could substantially reduce the extent of the IT review; however, examiners do need to keep in mind that each section of ~~COBiT~~ COBIT should be reviewed, in general, and findings from the IT review impacting reliance that can be placed on the IT function must be identified.

----------Detail Eliminated for Spacing Purposes----------

SECTION 2 – RISK-FOCUSED EXAMINATION PROCESS

© 2026 National Association of Insurance Commissioners

PHASE 1 – UNDERSTAND THE COMPANY AND IDENTIFY KEY FUNCTIONAL ACTIVITIES TO BE REVIEWED

In Phase 1 of a risk-focused examination, key activities will be confirmed or identified using background information gathered on the company from various sources. Some of this information will already have been available in the department prior to the initial planning ~~meeting, or~~meeting or can be obtained from the company's internal audit department or external auditors. A Phase 1 goal is to gather any additional or current information necessary to begin a risk-focused examination. Sources of information may include organizational charts, filings required by sections 302 and 404 of the Sarbanes-Oxley Act of 2002 (where applicable), interviews with senior management, or other publicly available information.

To ensure the appropriate risk-focused examination scope, it is important to identify the key functional activities (i.e., business activities) of the company. Information gathered by understanding the company, the company's corporate governance structure, and assessing the company's audit function will form the basis for determining key activities.

----------Detail Eliminated for Spacing Purposes----------

Step 4: Consideration of Information Technology Risks

The examiner-in-charge should also become familiar with the general controls surrounding the company's IT environment. Due to technological advancement (e.g., Internet, Intranet and e-commerce), internal control risks could be more pervasive within the IT environment than in other areas within the company. IT requires more technology insight to understand how it impacts the company's operations. Properly assessing IT risk requires appropriate IT training, experience, and technological insight. The examiner-in-charge may want to consider consulting with a specialist who has experience in reviewing IT general controls (ITGC).

In conducting examinations of insurers that are part of a holding company group, it is important to note that ITGCs ~~general controls~~ may occur at the holding company level. The exam team should seek to coordinate the identification and assessment of prospective risk in accordance with the exam coordination framework and lead state approach outlined in Section 1 of this Handbook. Where possible, in a coordinated examination, the lead state's work on the IT examination ~~general controls~~ should be utilized to prevent duplication of effort and to leverage examination efficiencies.

Section 1, Part III, A – General Information Technology Review outlines the process in which an IT control environment should be reviewed. Exhibit C -~~,~~ Part Two and Exhibit C – Part Three (also located in this Handbook) ~~is one~~are tools the IT examiner ~~can~~ should utilize while conducting the IT review. During the IT review, the IT examiner will identify risks that are relevant to the company based on their understanding of the company.

Once risks have been identified, the examiner will request control information from the company and test the appropriate controls within the IT environment. In the event an IT specialist is utilized, communication with the examiner-in-charge is critical throughout the review of ITGCs ~~general controls~~, especially when it comes to communicating findings of the review and the impact on the financial examination. As explained in Section 1, Part III, A – General Information Technology Review, the IT specialist should determine whether the ITGCs ~~general controls~~ environment is effective or ineffective. It is important for the examiner to review and understand the conclusion reached by the IT specialist in order to determine the extent of testing that may be required in later phases of the exam. If necessary, the IT specialist may need to assist in completing the work for the financial examination, such as identifying and testing IT application controls.

Consideration and review of the IT environment may be customized based on the size and complexity of the insurer under examination. For additional detail, refer to Section 1, Part III – General Examination Considerations.

© 2026 National Association of Insurance Commissioners

EXHIBIT C

EVALUATION OF CONTROLS IN INFORMATION TECHNOLOGY (IT)

The evaluation of controls in information technology (IT) is a critical element of the examination process. Determining the complexity of a company's IT environment and the extent of work that must be performed to evaluate both the IT general controls (ITGCs) in place and the company's exposure to cybersecurity risks is not always easy. Guidance on how to conduct an IT review is included within the General Information Technology Review guidance provided within Section 1, Part III of this Handbook. The tools included in this exhibit have been developed to assist the examiner in gaining an understanding of and evaluating the effectiveness of the company's ~~general~~ ITGCs ~~controls~~ and cybersecurity risk management practices in mitigating common IT and cybersecurity risks, as outlined within the General Information Technology Review guidance.

There are three~~wo~~ main sections to this exhibit. Part One, the Information Technology Planning Questionnaire (ITPQ), is a tool designed to assist the examiner in planning the extent of IT control work that might be necessary on an examination. The ITPQ provides the insurance department with a high-level overview of the company's information technology environment. It is used to plan the scope and extent of IT control work to be performed and assist the examiner in determining which sections or risks included in the Evaluation of Controls in Information Technology (IT) Work Program (Part Two of this exhibit) and the Prospective Cyber Risk Evaluation of Controls Work Program (Part Three of this exhibit) should be prepared for the examination. To achieve maximum benefit, the ITPQ should be completed in advance of even normal examination planning, so that the examiner can begin planning what work the examiner will complete within Parts Two and Three.

Part Two of the exhibit is the Evaluation of Controls in Information Technology (IT) Work Program. The IT Work Program has been created to assist the examiner in identifying general IT risks, and to provide example controls and potential test procedures to assist the examiner in evaluating how well the company mitigates its general IT risks. Part Two of the exhibit ~~replaces the Information Systems Questionnaire that has been included in previous editions of this Handbook, and~~ should be used as the primary tool to evaluate a company's ~~general~~ ITGCs ~~controls~~. For more information on how the two parts of the exhibit should be used during the examination, please refer to narrative guidance included in the General Information Technology Review caption in Section 1, Part III of this Handbook.

Part Three of the exhibit is a Cybersecurity Risk Repository. The Risk Repository has been developed to provide common cybersecurity risks, mitigation strategies, control objectives, possible test procedures, and preliminary information requests that may be used to assist the examiner in evaluating how the insurer mitigates identified cybersecurity risks. The Risk Repository is not intended to provide an all-inclusive listing of potential risks, nor is it intended to establish a minimum baseline of risks required to be included in every examination. For more information on this topic, please refer to Cybersecurity Considerations included in General Information Technology Review caption in Section 1, Part III of this Handbook.

----------Detail Eliminated for Spacing Purposes----------

PART TWO – EVALUATION OF CONTROLS IN INFORMATION TECHNOLOGY (IT) WORK PROGRAM

This work program has been created to assist examiners in completing a review of the general controls of a company's information technology (IT) in accordance with the risk-focused examination process. Detailed~~Detail~~ instructions for completing this program can be found in Section 1, Part III, under "General Information Technology Review." Due to the inherently high degree of change in IT~~ information technology~~, the period under review for this work program should generally range from the latest 12 to 24 months of the overall financial condition examination time period~~. The period under review~~ and should generally encompass the last year of the examination period and the period of time up to, and including, the actual examination fieldwork.

This work program assists the examiner in identifying the most common risks that are often inherent within the ~~general~~ IT general controls (ITGCs) of a typical insurance company. Included with the risk statements are examples of common controls, information requests and test procedures that may assist the examiner in determining how the company mitigates each risk.

This work program is categorized into four sections: Align, Plan and Organize (APO); Build, Acquire and Implement (BAI); Deliver, Service and Support (DSS); and Monitor, Evaluate and Assess (MEA). These sections are modeled after the COBIT Framework, due to its wide acceptance and use in the IT community. Although these sections are modeled after the COBIT Framework, they do not incorporate all of the control objectives of COBIT; rather, they incorporate only the most common control objectives that might need to be reviewed in an insurance company examination. APO addresses strategies and tactics and integrates IT into the overall business needs and objectives of the company. BAI addresses the identification, acquisition and implementation of those IT strategies and tactics identified within the APO section. DSS addresses the actual delivery of IT services identified in the BAI section. MEA assesses whether the IT processes from all sections are functioning adequately. The COBIT 2019~~5~~ Framework includes a fifth domain, Evaluate, Direct and Monitor (EDM) that assesses the overall governance of the IT environment. This domain was not incorporated in Exhibit C~~, Part 2~~ – Part Two, as the concepts presented throughout this domain are considered in other areas of the exam, including the review of corporate governance.

In certain situations, additional language has been added drawing on content within other IT frameworks (e.g., the National Institute of Standards and Technology [NIST], etc.) or ~~drawing on~~ content provided by state insurance regulators.

This work program is meant to be customized to include only the general IT risks that are of concern for the company under examination. As a result, the work program will vary from company to company, as the content will depend on the size and complexity of each company's IT environment. After the risks of concern have been identified, the examiner should consider making common control examples and information requests available to the company to assist the company in explaining how it mitigates each risk. A separate work program template, intended to be sent to the company, is maintained on ~~StateNet~~ NAIC Connect and includes a column for "Company Controls Identified," where the company will be able to document ~~their~~ its specific controls for the risks identified by the examiner. This template is designed to assist the examiner in identifying the risk statements, common controls and test procedures, based on the knowledge gained from the examiner's review of the company's response within the Information Technology Planning Questionnaire (ITPQ) and other information gathered as part of the "General Information Technology Review" guidance within Section 1, Part III (A). The IT ~~review team~~examiner should coordinate with the appropriate staff at the company to request this response. After the response is received, the examiner should perform testing as necessary to ~~corroborate~~ validate the company's risk-mitigation strategies.

~~Third~~ Third-Party Work

To assist in the identification and review of unique risks, examiners should obtain all available reports generated as a result of third-party work to ensure that the examiner has access to relevant findings from other entities. Examiners should understand work performed by other entities in auditing/reviewing the insurer's IT systems (e.g. independent third ~~-~~parties~~, federal regulators, etc.~~) and consider whether the work performed by other entities contains sufficient testing such that reliance can be placed on their work and whether the findings have been suitably addressed, as appropriate.

----------Detail Eliminated for Spacing Purposes----------

Possible Test Procedures

After gaining an understanding of the controls in place to mitigate the relevant risks, the examiner should test the effectiveness of the company's controls. Examples of possible test procedures are included in this work program. The test procedures provided are not designed to be an all-inclusive list and might not apply to all insurance companies that are under examination. In some circumstances, the examiner will need to develop additional test procedures or modify existing procedures beyond what is included within the work program. As mentioned above, for some possible test procedures, the examiner will need to request additional detailed information to perform testing. In addition, it is not expected that all possible test procedures will be utilized for all companies under examination.

INSTRUCTION NOTE 1: After the examiner has identified controls over the company's IT environment, based on the company's responses to the ITPQ and other information provided to the examiner, the examiner may determine that these controls over the company's IT environment should be tested for operating effectiveness. Section 1, Part III of this Handbook provides specific guidance on sampling for tests of controls and should be utilized by the examiner when testing the company's identified controls. In some cases, the examiner may be asked to assist in the financial examination, as outlined in the "General Information Technology Review" in Section 1, Part III of this Handbook. If it is determined that some of this work includes substantive testing, the examiner should utilize the substantive sampling guidance provided in Section 1, Part III of this Handbook.

INSTRUCTION NOTE 2: The following issues are addressed in Part One (ITPQ) and Part Two (Evaluation of Controls in IT Work Program). If the ITPQ is utilized and subsequently it is determined that all sections and risks included in the IT work program should be addressed, the responses received in the ITPQ should be considered when requesting information on the corresponding sections of the IT work program listed below.

Information Technology Planning Questionnaire (ITPQ)	Evaluation of Controls in Information Technology (IT) Work Program
2b	APO 01.01-01.02, MEA 02
2c	APO 02
2d	APO 02, APO 04
3e	APO 09
3f	APO 10
4a – 4d	MEA 02
5b	DSS 05.01 – 05.04

© 2026 National Association of Insurance Commissioners

7a	APO 03
7b	DSS 03.05, BAI 02.04, BAI 03.05, BAI 06
8b – 8d	BAI 03.02, BAI 04.02, DSS 04
9a-9c	DSS 04.04, DSS 04.07, DSS 05.01, APO 03, APO 04

~~**INSTRUCTION NOTE 3:** Examiners may determine that cybersecurity risks are significant for the insurer under examination. This may be based on responses provided to the ITPQ, results of planning and examiner's judgment. To ensure that the examination procedures performed include an adequate response to the insurer's cybersecurity risk, which can affect multiple facets of the IT environment, examiners may consider performing procedures in relation to risk statements APO 1, APO 10, APO 12, DSS 02 and DSS 05. Note these risk statements and associated procedures may or may not explicitly mention the threat of cybersecurity in the language presented, but examiners should customize the procedures provided to respond to this risk as appropriate. DSS 04 covers the protections of system backups in the event of a ransomware attack. Examiners may determine that additional risks are relevant when considering cybersecurity and ransomware exposure, and they should tailor their work program based on information available on the exam. Additional considerations for cybersecurity concerns are located in Section 1-III (A) of the Examination Handbook guidance, entitled "General Information Technology Review."~~

INSTRUCTION NOTE ~~34~~: Examiners should consider the overall accessibility and transferability of the company's claims and policyholder data. Holistically, the exam team should determine whether the company would be able to transfer its data efficiently and effectively to another location should that need occur (e.g., when switching service providers, in the event of an audit or receivership, etc.). Companies that rely heavily on legacy systems, MGAs, multiple cloud platforms, TPAs; or that commingle claims data may be at a higher risk. Risk statements APO 03, APO 04, APO 14, DSS 01, DSS 04, and DSS 05 can be referenced for procedures surrounding data quality, infrastructure, security, and portability.

© 2026 National Association of Insurance Commissioners

EXHIBIT C

ITGC REVIEW ~~STANDARD~~ SUMMARY MEMORANDUM

A summary memorandum should be developed by the IT examiner to communicate the results of the IT general control (ITGC) review to the examiner-in-charge, or any other users. Some of the topics the IT examiner may want to consider incorporating into the summary memorandum are included in the illustration below, along with a brief description of information that could be discussed relating to each topic. This document should provide sufficient detail of the results of the IT review for use during the financial condition examination.

Salutation

This section should be in any format the state deems appropriate for its purposes. At a minimum, all states that are placing reliance on the IT review should be included in the distribution of this memo.

Background and Scope

This section should include an introductory paragraph identifying the following: companies under examination (domiciliary state and type may be helpful), the exam as-of date and time period under examination, where the work was performed, when the work was performed, who performed the work, and the scope/topic of the work performed.

Summary of Control Environment

This section should provide a summary description of the IT environment and the ~~general IT controls~~ITGCs assessed during the IT review. This section should also provide a general description of the insurer's overall processes and controls, including access controls, in place to protect sensitive information. This section should also include discussion of any breaches identified during the period under exam.

Work Performed

This section of the memo should provide an overview of the work performed to evaluate ~~general~~ ITGCs ~~controls~~ throughout the IT review process, as well as the reliance placed on external sources (e.g., Model Audit Rule documentation/testing, Sarbanes-Oxley documentation, external audit work, etc.). If the results of external audit, third-party work, and/or cyber self-assessment tools are utilized to populate Exhibit C procedures, include a review of the external work in this section. This review could include an assessment of the source, scope, and robustness of the third-party work being utilized.

Summary / Detail of Findings ~~(Including Cybersecurity Related Findings)~~

This section should provide a summary description of the findings that were identified while performing the IT review. These findings may include~~:~~ areas that affect the company's current operations~~;~~, areas that will be relevant for future examinations~~;~~, or areas of recommendation for the company to consider. The IT examiner should document the recommendation and impact of the finding on the financial examination and provide reference to the supporting detail located in the completed Exhibit C, Part Two (or similar document). The IT examiner should consider mitigating factors in their assessment of the impact that findings will have on the exam (additional testing may be required to assess the effectiveness of the mitigating factors). Findings that are sufficiently mitigated by other factors may be found to have a minimal ongoing impact for examination purposes. Findings that have not been sufficiently mitigated, or findings that require tracking and future follow-up information, may be passed to the Summary Review Memorandum (SRM) and/or communicated to the analyst depending on significance and length of impact. Cybersecurity related findings identified collaterally during completion of Exhibit C – Part Two should be reported in the Cybersecurity Review Summary Memorandum during completion of Exhibit C – Part Three.

The following elements ~~table(s) or similar format~~ may be used in assessing findings, mitigating factors, and the overall impact on the exam: IT Review Finding, Recommendation for Company, Mitigating Factors, Impact on Financial Examination, Supporting Detail Reference, Recommended Ongoing Monitoring (if applicable).

~~**Findings**~~

~~IT Review Finding~~	~~Recommendation for Company~~	~~Mitigating Factors~~	~~Impact on Financial Examination~~	~~Supporting Detail Reference~~	~~Recommended Ongoing Monitoring (if applicable)~~
					~~(e.g., if the company does not have a disaster recovery plan but is currently creating one, include this information in the SRM and pass to analyst).~~

IT Prospective Risks

This section should identify significant IT prospective Risks that were not fully addressed during the IT review and that the financial examiners should consider performing further review/investigation during the remaining phases of the examination. IT prospective risks in this section should be material in nature and should have an explicit connection to the company's risk profile. The description of the IT prospective risks should include the impact on the company's risk profile. IT prospective risks identified in this section may be documented and reviewed further in the Exhibit V.

Conclusion/Results of IT General Control Review

This section should document the conclusion/results of the ITGC review. Based on the impact of the findings, the IT examiner should determine whether the ITGC environment is effective and would, therefore, indicate that IT risks have been sufficiently mitigated to allow for reliance on ~~general~~ ITGCs ~~controls~~ and testing of application controls in Phase 3. If the ITGC environment is not effective, the examiner would be required to perform additional testing in later phases of the exam before relying on system-generated reports or controls in place at the insurer. The IT examiner should consider the impact of the findings on the exam in totality and consider the following when concluding between a generally effective or ineffective ITGC environment. In some instances, the overall ITGC environment may be deemed ineffective. In reaching this conclusion, the IT examiner should consider whether the findings outlined in the IT summary report:

- Are pervasive throughout the ITGC environment.
- Significantly impact the systems used in calculating and reporting financial results or the accuracy of information used in reaching major strategic decisions.

© 2026 National Association of Insurance Commissioners

- Indicate deficiencies relating to management involvement and oversight of the IT strategy and direction.
- Are not alleviated by other mitigating factors.

If the impact of a finding is isolated to a point in time or a less significant system, the IT examiner may still determine a generally effective ITGC environment while listing the particular system(s) as an exception. The IT examiner should document the possible implications on the exam with the goal of helping the exam team adjust their testing approach around the affected area. For additional guidance regarding the conclusion of the ITGC review refer to Section 1, Part III, A – General Information Technology Review.

Note: The IT Examiner should provide a conclusion on the effectiveness of the ITGCs using the terminology prescribed by the Handbook (effective or ineffective). Using alternate language may leave the Financial Examiner in an unclear position on whether ITGC's can be relied upon and may lead to inefficiencies later in the examination process.

Meeting with Examiner-In-Charge and Other Financial Examiners

This section should document the date and time of the meeting with the EIC and other examiners (e.g., examiners from other states participating in the financial examination) that was conducted to discuss the findings and results of the IT review.

Assistance on the Financial Examination

This section should identify the remaining areas of the financial examination in which the IT examiner~~review team~~ ~~will~~ may be asked to provide assistance. This may include identifying and testing application controls in conjunction with Phase 3 of the risk-focused examination, performing data mapping or ~~ACL testing~~data analytics, and/or assisting with drafting the examination report and/or management letter. This could also include assisting with the evaluation of IT prospective risks and any ongoing monitoring required for IT examination findings.

Completed Exhibit C, Part Two (or Similar Document) and Supporting Documentation

A completed IT Review Work Program should be referenced here and provided to the EIC. Detail findings should be noted within the work program and referenced in the "Detail of Findings" section above.

© 2026 National Association of Insurance Commissioners