Draft Date: 10/28/2024

Virtual Meeting

INFORMATION TECHNOLOGY (IT) EXAMINATION (E) WORKING GROUP
Thursday, October 31, 2024
3:00-4:00 p.m. ET / 2:00-3:00 p.m. CT / 1:00-2:00 p.m. MT / 12:00 p.m.-1:00 p.m. PT

ROLL CALL

Ber Vang, Chair	California	Kim Dobbs/Cynthia Amann	Missouri
Shane Mead, Vice-Chair	Kansas	Andrea Johnson	Nebraska
Blase Abreo	Alabama	Eileen Fox	New York
Mel Anderson	Arkansas	Colton Schulz	North Dakota
Ken Roulier/Michael Shanahan	Connecticut	Metty Nyangoro	Ohio
Ginny Godek	Illinois	Eli Snowbarger	Oklahoma
Jerry Ehlers	Indiana	Diana Sherman	Pennsylvania
Dmitriy Valekha	Maryland		

NAIC Support Staff: Topher Hughes/Bruce Jenson

AGENDA

1. Consider Adoption of October 10, 2024 Meeting Minutes—*Ber Vang (CA)* — Attachment A

2. Consider Adoption of Proposed Edits to Exhibit C—*Ber Vang (CA)*
   a. NAMIC Comment Letter — Attachment B
   b. Updated Draft of Guidance — Attachment C

3. Discuss Any Other Matters—*Ber Vang (CA)*

4. Adjournment

Draft: 10/11/24

Information Technology (IT) Examination (E) Working Group
Virtual Meeting
October 10, 2024

The Information Technology (IT) Examination (E) Working Group of the Examination Oversight (E) Task Force met Oct. 10, 2024. The following Working Group members participated: Ber Vang, Chair (CA); Shane Mead, Vice Chair (KS); Blase Abreo (AL); Mel Anderson (AR); Michael Shanahan (CT); Ginny Godek (IL); Jerry Ehlers (IN); Dmitriy Valekha (MD); Kim Dobbs and Cynthia Amann (MO); Colton Schulz (ND); Andrea Johnson (NE); Eileen Fox (NY); Metty Nyangoro (OH); and Eli Snowbarger (OK).

1. Discuss Current and Future Plans for Updating IT Review Guidance Based on Cybersecurity (H) Working Group Referral

Vang stated that the drafting group activities since the last meeting address the referral from the Cybersecurity (H) Working Group. The referral requested that the IT Examination (E) Working Group review the IT exam process and evaluate if there would be a benefit to making the process more cybersecurity-focused. The referral suggested several frameworks and documents that could be useful in addressing the request, including the cybersecurity performance goals (CPGs) of the Cybersecurity and Infrastructure Security Agency (CISA), the Cybersecurity Framework (CSF) 2.0 of the National Institute of Standards and Technology (NIST), or the benchmarks of the Center for Internet Security (CIS).

The drafting group determined that there could be a benefit to enhancing the cybersecurity procedures in Exhibit C. After evaluating several sources of guidance, the drafting group decided to incorporate updates based on the NIST CSF 2.0. The drafting group selected the NIST CSF 2.0 because NIST was introducing concepts not currently in the IT exam process while also being in a format similar to the current Exhibit C.

Vang explained that due to time constraints for incorporating changes into the *Financial Condition Examiners Handbook* before the end of this year, the drafting group chose to take a two-step approach to these changes. In the first step, the drafting group performed a gap analysis, and Exhibit C procedures have been modified to address critical gaps between the current Exhibit C and the NIST CSF 2.0.

In the next step, which is anticipated to extend well into 2025, the drafting group will separate procedures needed to establish the reliability of IT general controls from those needed to examine cybersecurity. Care will be taken to ensure findings concerning IT general controls can be made before the end of phase 2, while it is possible that a finding on cybersecurity matters may take place later in the exam process. It is foreseen that some current procedures from Exhibit C will also be eliminated during this process, as they will be found redundant or otherwise no longer needed. It is important that the resulting IT general controls and cybersecurity reviews remain right-sized for examination purposes.

2. Exposed Revisions to Exhibit C, Part 2

Vang explained that the drafting group had divided into two subgroups. Subgroup 1 addressed the Govern and Protect functions of CSF 2.0 while Subgroup 2 addressed Identify, Detect, Respond, and Recover.

Mead provided examples of proposed changes made by Subgroup 1 to address the Govern and Protect functions of CSF 2.0. There were numerous small edits made to add emphasis to cybersecurity. One example is in APO 01.01-

© 2024 National Association of Insurance Commissioners

01.02, where the phrase “including cybersecurity” was added to the common control, and a new possible test procedure was added to review and assess the adequacy of cybersecurity staffing and/or resources. Additionally, Mead highlighted larger changes made to APO 10, BAI 03.07-03.08, BAI 10.01-10.05, and DSS 05.06. Mead also noted that Subgroup 1 proposed adding part of APO 14, based on APO 14.01 and APO 14.08-14.09, to better address data protection and retention.

Vang then addressed the changes proposed by Subgroup 2. Vang highlighted larger proposed edits to DSS 02.01, DSS 05.07, and MEA 02.01, while noting that Subgroup 2 proposed adding controls based on DSS 02.05 to better address the recovery process following an incident.

Colleen Scheele (NAMIC) asked about the addition of APO 14, concerning the data life cycle. Mead stated that the NIST CSF 2.0 had controls in it that dealt with items not previously in Exhibit C and that the Subgroup considered trying to fit the control into DSS 05.06 but believed that APO 14 better addressed the issue, as it already dealt with the data life cycle and was the more logical solution.

There were no objections to exposing the revisions for a 14-day public comment period ending Oct. 24. Vang stated that the shortened exposure period was so that revisions could be adopted before the next NAIC national meeting and included in this year’s revisions to the *Financial Condition Examiners Handbook*.

Having no further business, the IT Examination (E) Working Group adjourned.

SharePoint/NAIC Support Staff Hub/Member Meetings/E CMTE/EOTF/ITEWG Minutes 10-10-24

© 2024 National Association of Insurance Commissioners

NAMIC
NATIONAL ASSOCIATION OF MUTUAL INSURANCE COMPANIES

317.875.5250 | [F] 317.879.8408
3601 Vincennes Road, Indianapolis, Indiana 46268

202.628.1558 | [F] 202.628.1601
20 F Street N.W., Suite 510 | Washington, D.C. 20001

Deputy Commissioner Ber Vang

Information Technology (IT) Examination (E) Working Group

National Association of Insurance Commissioners

Via Email: Topher Hughes, chughes@naic,org, and Bruce Jenson, bjenson@naic.org

RE: Request for Comments on Exhibit C- Part 2

Dear Deputy Commissioner Vang,

Thank you for the opportunity to comment on the exposed revisions to Exhibit C- Part 2 of the Information Technology piece of the Financial Condition Examiner's handbook (Exposure). The National Association of Mutual Insurance Companies (NAMIC) membership reflects many of the country's largest national insurers as well as regional and local mutual insurance companies on main streets across America. NAMIC members write $391 billion in annual premiums and account for 68 percent of homeowners, 56 percent of the automobile, and 31 percent of the business insurance markets. NAMIC offers the following comments on this Exposure, organized by topics of third-party vendors and data practices.

Third-Party Vendors

The Exposure makes several changes to how insurers will be expected to interact with and monitor their third-party vendors.

In APO 10, a control was added that states:

> The company has a formal process in place whereby;
>
> 1. *An inventory is completed and maintained of the company's vendors and service providers, including information concerning their risk and their supply chain criticality.*
> 2. Risk is assessed based on the company's understanding of the third-party service providers information security program as well as by the company's ability to verify elements of the third-party service provider's security program and the data exposed to the third party, such as PII; Supply chain criticality is assessed on mission function, and availability of alternatives.

Subsequentially, a preliminary information request was added that asks insurers to "*verify an inventory of service providers is created, maintained, and includes sufficient information to rank providers based on both risk and supply chain criticality*." Possible test procedures have been edited to include:

Review the company's third-party *vendor and* 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 supply chain criticality in ranking;*
3. Whether the company*, service, or program* has appropriately determined access rights based on its risk assessment *and supply chain criticality*; and
4. Whether the company has designed appropriate controls that are consistent with the company's ~~risk assessment~~ *ranking*.

Such an above referenced inventory would be enormous and quite labor-intensive to maintain and continuously update rankings. There is a concern about adding *supply chain* to the evaluation factors for third party vendors. It is very difficult, particularly for vendor owners spread across the business, to accurately assess supply chain risk or even to understand how supply chain risk is being interpreted or defined. While we do not support introducing substantive concepts via a handbook (rather than in a legal/regulatory forum with administrative procedure and transparency of expected compliance requirements) if regulators are going to proceed with introducing such a concept perhaps consider the phrasing of a "*material adverse impact to the business, operations or security*", which is used in the NYDFS Cybersecurity Regulation.[1] It's almost impossible for anyone to accurately assess supply chain risk unless they have an investor-level understanding of each company and product. As examples, recently both Crowdstrike and SolarWinds had massive supply chain/process failures that caused huge damages to their customers. Both companies were thought to be exemplars of controls and quality prior to those catastrophic supply chain failures.

As previously written, APO 10 and Insurance Data Security Model Law 668 (Model 668) are generally aligned in the scope of their oversight except where APO 10 requires the entity to maintain an inventory and scoring system based on risk and supply chain criticality. It is important to note that here, compliance with Model 668 would not result in meeting the standard set forth in APO 10. Without going through the sanctioned process of amending Model 668, APO 10 replaces that model's *'appropriate measures'* with the inventory and risk/supply chain criticality ranking and is imposing completely new requirements on insurers via a handbook. In practice, 'appropriate measures' may be sufficient to cover what the Exposure is intending. NAMIC does <u>not</u> believe that any edits to this APO are necessary.

[1] 23 NYCRR 500.

Regardless of our concerns, NAMIC offers alternative edits below to the exposed language the preliminary information request and the possible test procedures that would alleviate some of the anxieties surrounding creating a ranked list of third-party vendors.

> Preliminary Information Request Edits:
>
> Verify an inventory of service providers is created, maintained, and includes sufficient information to ~~rank~~ *group or classify* providers based on risk and *material adverse impact to the business, operations or security* ~~and supply chain criticality~~.
>
> Possible Test Procedures Edits:
>
> Review the company's third-party vendor and 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* ~~and supply chain criticality~~ in ~~ranking~~ *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 supply chain criticality~~; and
> 4. Whether the company has designed appropriate controls that are consistent with the company's ~~ranking~~ *classifying or grouping*.

In APO 12, the Exposure adds language into possible test procedure:

> 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 incorporated into the risk profiles*.

As written, it implies ongoing perpetual review of third-party vendors in an incredibly vendor heavy world. This seems like an attempt to make sure that the cybersecurity personnel are involved in the broader security discussion and paying attention to various "sharing forums." While all insurers do pay attention to several industry forums, it may not be best practice, attribute specific changes to our risk assessments back to the source(s) that brought them to our attention. It is appropriate to ask about cybersecurity continuing education and broader industry awareness, but this test does not get to the point of third-party vendors' risk to ERM as finely as it could.

NAMIC suggests the below edits to APO 12's edited possible test procedure:

> 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. *This includes periodically assessing*

third party vendors which would incorporate threats or vulnerabilities into risk profiles. ~~Determine whether threats and vulnerabilities identified through information sharing forums are incorporated into the risk profiles.~~

This approach in this suggested wording is also more consistent with the language contained in Section 4 of Model 668.

Data Practices

The Exposure adds a new section, APO 14, which concerns the risk that the company does not effectively manage their data across the data life-cycle. This is not a new concern for regulators and insurers, but the way in which this Exposure frames it is different than existing guidance. The SEC looks at cybersecurity events as a potential reporting requirement in the context of *"materiality,"* which is defined as the consequence the event would have on the financial condition of the entity, specifically with concern as to whether the consequence of the event would affect the decision-making process of an investor or potential investor.[2] If the financial examiner were to focus on cybersecurity risk as a protection of financial viability, it may make sense, but that risk assessment should be focused on material financial consequence, analogous to the SEC requirement being focused on its interest in protecting innocent investors.

The current NAIC guidance on this topic exists in Model 668, Section 4, Information Security Program (Section 4). Section 4 (B) states that a licensee's information security program shall be designed to:

1. Protect the security and confidentiality of Nonpublic Information and the security of the Information System;
2. Protect against any threats or hazards to the security or integrity of Nonpublic Information and the Information System;
3. Protect against unauthorized access to or use of Nonpublic Information, and minimize the likelihood of harm to any Consumer; and
4. Define and periodically reevaluate a schedule for retention of Nonpublic Information and a mechanism for its destruction when no longer needed.

Section 4 (D) provides guidance on risk management and how the information security program should mitigate identified risk, commensurate with the size and complexity of the insurer's activities, including its use of third-party service providers. The financial exam already incorporates some of these ideas into its scope and test controls.

Another concern is the subject matter of this APO. APO 14 is connected to solvency but truly gets to the heart of privacy and security issues, which are not traditional solvency topics. To effectively manage this new topic, examiners must have sufficient knowledge about controls and technology to understand best practices as well as what insurer responses mean. The financial exam is a flexible exam, meant to meet companies where they are in both size, scope, and complexity of business practices.

[2] Security and Exchange Commission, 17 CFR Parts 229, 232, 239, 240 and 249 (2023- 16194).

Data retention may not be the largest threat to solvency in the IT space. *NAMIC suggests the Working Group not move forward with APO 14 at this time, holding back this piece of Exposure and investigating areas such as ransomware protections and practices.*

NAMIC is appreciative of the extensive work done the Working Group as it relates to insurer practices related to third party vendors. We welcome the opportunity to work with regulators and NAIC staff on the inclusion of these risks into the financial exam.

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

Risk Stmt #	Risk Statement	Ctrl #	Common Controls	Preliminary Information Request	Possible Test Procedures
APO 01	IT organizational structure is inadequate to support business objectives.	APO 01.01 – APO 01.02	The company's IT management organizational structure, with clearly defined roles and responsibilities, supports business objectives and IT priorities (including cybersecurity) and enables efficient decision-making.	Provide the IT organization chart showing job title and names of IT executives and managers and reporting lines to CEO and the BOD. Provide ~~resume/biographical information from~~job descriptions for key IT positions, including cybersecurity,~~executives~~ 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 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. Review IT governance committees to determine whether business is adequately represented to facilitate IT priorities in supporting business objectives.
		APO 01.03-APO 01.04	The company has established and communicated IT standards to ensure consistency and to drive	Provide IT policies and procedures, including security, HR policies and IT training program documentation, including	Assess policies and procedures to ensure currency and completeness. Determine whether IT security is embedded in HR policies for all employees.

Commented [BJ1]: Edit recommended by KS

1

Risk Stmt #	Risk Statement	Ctrl #	Common Controls	Preliminary Information Request	Possible Test Procedures
			compliance across the organization.	for specialized roles such as cybersecurity professionals.	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 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	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

Commented [BJ2]: Edit recommended by KS

Risk Stmt #	Risk Statement	Ctrl #	Common Controls	Preliminary Information Request	Possible Test Procedures
					understanding of systems, including input from stakeholders. 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	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 obsolete and poorly aligned	APO 04.02	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 04.05	The company has a technology advisory board (or equivalent)	Provide a copy of the membership, agendas and minutes of the meetings	Review membership, agendas and minutes of the technology advisory board to verify that they are providing information on emerging

Risk Stmt #	Risk Statement	Ctrl #	Common Controls	Preliminary Information Request	Possible Test Procedures
	with business objectives.		that identifies emerging technologies and/or other IT innovations.	of the technology advisory board.	technologies and other IT innovations, as well as evaluating and monitoring the results of proof of concept initiatives.
APO 06	The IT budget is not representative of the organization's goals and business needs, and IT expenses are not properly allocated.	APO 06.01 - APO 06.05	The IT budget is developed based on strategic plan initiatives.	Provide evidence that the IT budget is based on supporting the strategic plan.	Review budget documentation to verify consistency with the IT strategic plan. 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.
			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 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	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,	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.

4

Risk Stmt #	Risk Statement	Ctrl #	Common Controls	Preliminary Information Request	Possible Test Procedures
			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. 4) Ensure that regular reviews of SLAs and supporting contracts are performed to ensure that formalized IT services are being provided.		Ensure that SLAs are reviewed and revised when needed.
APO 10	Third-party service provider risks are not properly assessed, addressed, and mitigated.	APO 10.01 - APO 10.05	The company has a formal process in place to manage service providers. The company creates formal agreements with the service provider to identify roles and responsibilities, expected deliverables, performance standards and credentials.	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 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

Risk Stmt #	Risk Statement	Ctrl #	Common Controls	Preliminary Information Request	Possible Test Procedures
			Contracts conform to business standards in accordance with legal, ~~and~~ regulatory and/or statutory requirements. Nondisclosure agreements, escrow accounts and conformance with security requirements are included as considered necessary.		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.
			Reviews are performed on outside service providers 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 controls. Consider the impact of any exceptions identified.
			The company has a formal process in place whereby: 1) An inventory ~~is completed and maintained~~ of the company's vendors and service providers is completed and maintained~~,~~ and	Verify an inventory of vendors and service providers is created and maintained, and includes sufficient information to ~~rank~~ group and classify providers based on both risk and ~~supply chain criticality~~ material adverse impact to the business, operations, or	Review the company's third-party vendor and 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 ~~supply chain criticality~~ material adverse impact in ~~ranking~~ classifying or grouping; 3~~2~~) Whether the company, service, or program has appropriately determined access rights based on its risk assessment and supply chain

Commented [BJ9]: Edits recommended by KS

Commented [TH10]: Per the NAMIC letter

Risk Stmt #	Risk Statement	Ctrl #	Common Controls	Preliminary Information Request	Possible Test Procedures
			includes ~~including~~ information concerning their risk and their ~~supply chain criticality~~ material adverse impact to the business, operations, or security. 2) ~~1)~~ Risk is assessed based on the company's understanding of the third-party service providers information security program as well as by the company's ability to verify elements of the third-party service provider's security program and the data exposed to the third party, such as PFI, PHI, and PII; ~~1)~~ ~~Supply chain criticality~~ Material adverse impact to the business, operations, or security is assessed based on mission function, and availability of	security. Provide a summary of the company's third-party service provider management process.	criticality; and 43) Whether the company has designed appropriate controls that are consistent with the company's ~~risk assessment.ranking~~ classifying or grouping.

Commented [TH11]: Per NAMIC letter

Commented [TH12]: Per NAMIC letter

Commented [BJ3]: Edits recommended by KS

Commented [TH4]: Changed from supply chain criticality to material adverse impact to the business, operations, or security per NAMIC letter.

Commented [BJ5]: Edit recommended by KS

Commented [TH6]: Per NAMIC

Risk Stmt #	Risk Statement	Ctrl #	Common Controls	Preliminary Information Request	Possible Test Procedures
			alternatives. 3) ~~2)~~ 2) Based on the company's risk ~~and supply chain criticality~~ and material adverse impact to the business, operations, or security, the company ~~ranks~~groups and classifies vendors and uses a vendor's ranking to determine depth and frequency of review procedures performed related to ongoing vendor relationships; 4) ~~3)~~ 3) The company determines appropriate access rights, based on the risk assessment and company needs; 5) 6) ~~4)~~ The company designs specific mitigation strategies ,including network monitoring specific to third-party service		

Commented [TH7]: Per NAMIC letter

Commented [HT8]: per NAMIC letter

Risk Stmt #	Risk Statement	Ctrl #	Common Controls	Preliminary Information Request	Possible Test Procedures
			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	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.
			An IT risk profile is actively maintained describing known risks and risk attributes and of related resources, capabilities and current control activites.	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 incorporated into the risk profile.
			Continual communication on 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 as a result of IT-

Risk Stmt #	Risk Statement	Ctrl #	Common Controls	Preliminary Information Request	Possible Test Procedures
					related exposures and opportunities.
APO 14	The company does not effectively manage ~~their~~its data across the data life-cycle.	APO 14.01	The company defines and communicates ~~their~~its data management strategy, and roles and responsibilities.	Provide a copy of the data management strategy, policy, 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	The company has established data protection policies and procedures in place to support data confidentiality, integrity, and availability.	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.
			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 ~~their~~its data archival and retention policies.

Commented [BJ13]: Edits recommended by KS

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

Risk Stmt #	Risk Statement	Ctrl #	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 project-management methodology.	BAI 01.01–BAI 01.05, BAI 01.07–BAI 01.10, BAI 01.12, BAI 01.14	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. 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	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

Risk Stmt #	Risk Statement	Ctrl #	Common Controls	Preliminary Information Request	Possible Test Procedures
					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, timeliness and reasonableness of the cost justification and related project approval.
		BAI 02.04	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	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	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

Risk Stmt #	Risk Statement	Ctrl #	Common Controls	Preliminary Information Request	Possible Test Procedures
			agreed-on criteria.		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.
		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	Business and IT solution components and information repositories 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	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	Validate that IT procurement procedures address the services needed by the business, while also meeting security requirements.

Risk Stmt #	Risk Statement	Ctrl #	Common Controls	Preliminary Information Request	Possible Test Procedures
			integration of hardware and infrastructural software to protect resources and ensure availability and integrity. Acquired application software is configured to meet business processing requirements.	acquisition strategy, hardware, software and services, etc.	
		BAI 03.06	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 evidence and documentation of the QA function.	Review the software QA practices relative to program and system development to ensure related processes align with the organization's QA practices. 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	Integrated test plans and practices are commensurate with the enterprise environment and strategic technology plans. ~~The company has established a test environment that is representative of the production environment and takes into consideration security,~~	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, ~~surrounding the usage of~~for ~~the test~~ pre-production environments.	Validate that integration test plans and practices enable the creation of suitable testing and simulation environments. Validate that the ~~test~~ pre-production environments adequately support~~s~~ the application requirements and mirror~~s~~ 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.

Commented [TH14]: This control is duplicated in BAI 07.04

Risk Stmt #	Risk Statement	Ctrl #	Common Controls	Preliminary Information Request	Possible Test Procedures
			~~workloads and data quality.~~ The company has secure pre-production development environments to maintain security throughout the software development life-cycle.		
		BAI 03.08	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 due to inadequate planning for capacity, cybersecurity events, performance and availability.	BAI 04.01	The company has established a planning and review process for continuous performance and capacity monitoring of IT resources. Management ensures that contingency plan procedures are in place to properly address availability,	Provide a copy of the policies and procedures regarding performance and capacity management.	Review policies and procedures and interview key staff members involved in the development of the performance and capacity plan to verify that the appropriate 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),

Risk Stmt #	Risk Statement	Ctrl #	Common Controls	Preliminary Information Request	Possible Test Procedures
			~~capacit~~capacity, cybersecurity events, ~~y~~ and performance of individual IT resources.		verify compliance with the contingency plan procedures and verify that they were effective.
		BAI 04.02	Solutions and services that are critical in the availability and capacity management process are evaluated as part of business impact analysis procedures. 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 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.
				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.
		BAI 04.03	Capacity and performance plans are updated and reviewed by management periodically, and define current and forecasted performance, and are	Obtain capacity and performance plans, including modeling techniques that define current and forecasted performance, capacity and throughput of the IT	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.

Risk Stmt #	Risk Statement	Ctrl #	Common Controls	Preliminary Information Request	Possible Test Procedures
			used for service trend analysis.	resources. Obtain evidence of periodic update and review by management.	
		BAI 04.04	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.

Risk Stmt #	Risk Statement	Ctrl #	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	The company has a process in place to record, authorize, manage, monitor and implement requests for 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 procedures require 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	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	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	The company has a defined process to ensure data is converted accurately and	Provide procedures detailing system and data conversion.	Verify that the conversion procedures ensure that data is converted accurately and completely and can be recovered.

18

Risk Stmt #	Risk Statement	Ctrl #	Common Controls	Preliminary Information Request	Possible Test Procedures
			completely.	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	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	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).
		BAI 07.06	The company has controls in place to ensure that changes are	Provide evidence of controls that ensure production release in	Review the company's implementation process. Select a sample of completed projects and

Risk Stmt #	Risk Statement	Ctrl #	Common Controls	Preliminary Information Request	Possible Test Procedures
			released into production in accordance with the implementation plan.	accordance with the implementation plan	verify that changes were released into production in accordance with the implementation plan.
		BAI 07.08	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	The company has procedures in place over configuration management, which includes establishing and monitoring baselines for every system and service, in addition to	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.

Risk Stmt #	Risk Statement	Ctrl #	Common Controls	Preliminary Information Request	Possible Test Procedures
			the logging of any changes.		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.
			Installed software is periodically compared to the policy for software usage to determine compliance with software licensing agreements or to identify 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.

Commented [BJ15]: Edit recommended by KS

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

Risk Stmt #	Risk Statement	Ctrl #	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-management process.	DSS 01.01	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.
			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.
			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.
			The scheduling and completion of jobs is organized into a sequence, maximizing	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	Verify that procedures include points of contact

Risk Stmt #	Risk Statement	Ctrl #	Common Controls	Preliminary Information Request	Possible Test Procedures
			throughput and utilization to meet business requirements.	documentation showing contact information and codes for job failures.	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 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	DSS 01.04–DSS 01.05	The data center contains proper physical and environmental controls to protect the equipment, data and personnel	Provide information regarding the physical and environmental controls in place at the company's data center	Tour the data center, inspect documents and interview the appropriate personnel to verify that physical security and environmental controls are in place and monitored.

Risk Stmt #	Risk Statement	Ctrl #	Common Controls	Preliminary Information Request	Possible Test Procedures
	unauthorized access and inadequate protection of data.		located within.	and other sensitive IT sites.	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 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

Risk Stmt #	Risk Statement	Ctrl #	Common Controls	Preliminary Information Request	Possible Test Procedures
					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. 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

25

Risk Stmt #	Risk Statement	Ctrl #	Common Controls	Preliminary Information Request	Possible Test Procedures
					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. IT sites and server rooms are kept clean and in safe condition.
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 ~~a computer emergency response team (CERT) exists~~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 ~~CERT~~ 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	Select a sample of incidents to verify that the security incident management process includes:

Risk Stmt #	Risk Statement	Ctrl #	Common Controls	Preliminary Information Request	Possible Test Procedures
				period under review.	1) Event detection and containment. 2) Correlation of events and evaluation of threat/incident. 3) Resolution of threat, or creation and escalation of an appropriate work order. 4) Criteria for initiating the organization's ~~CERT~~ 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	Provide a copy of the	Review and confirm whether the company's

Risk Stmt #	Risk Statement	Ctrl #	Common Controls	Preliminary Information Request	Possible Test Procedures
			established procedures for performing a 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.).	company's computer forensic investigation procedures.	procedures follow a process of identifying, 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	The company has a service function to record, classify and prioritize requests and incidents (e.g., service	Provide a copy of the policy and procedures for the service function.	Verify that the processes and tools are in place to register incidents, status and actions for resolution. Review the standards for communication of

Risk Stmt #	Risk Statement	Ctrl #	Common Controls	Preliminary Information Request	Possible Test Procedures
			desks).		incidents and verify that they were complied with.
				Provide a listing of open and closed user reported incident records.	Review a sample of open and closed customer incidents to verify compliance with the process and service commitments. For the sample selected, verify that all resolved incidents are described in detail, including a detailed log of all steps taken to resolve the incident.
				Provide documentation on the workflow used to handle incidents	Review procedures for reporting significant incidents to management. Verify with management that significant incidents 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 incident response plan have been fulfilled prior to proceeding with recovery • Proper communication to internal/external stakeholders prior to and following 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

29

Risk Stmt #	Risk Statement	Ctrl #	Common Controls	Preliminary Information Request	Possible Test Procedures
					If applicable, select from a sample of recent security incidents to verify documented processes related to recovery were appropriately followed. Otherwise, request documentation regarding recent testing of recovery processes.
		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, service levels and customer satisfaction.	DSS 03.01	The company maintains problem-management policies and procedures, including escalation triggers, with adequate audit trails and analysis to identify, report and classify incidents by category, impact, urgency and priority.	Provide a copy of the policy and procedures used to identify, classify and track incidents.	Verify that adequate processes supported by appropriate tools are in place to identify and monitor incidents. For TPA problem management, review SLAs, SSAE 18, contracts, etc.
		DSS 03.02	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	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	Select a sample of tickets for appropriate prioritization, identification of root cause, timely completion, documentation of actions taken and any necessary approvals.

Risk Stmt #	Risk Statement	Ctrl #	Common Controls	Preliminary Information Request	Possible Test Procedures
			determining the root cause of all reported problems.	problem was reported, date the problem was closed and, if open, current priority.	
				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.
		DSS 03.03–DSS 03.04	Problem disposition procedures are in place to address 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	Change management is integrated with problem management to ensure effective management of problems and to enable improvements.	Provide a copy of the company's incident management policy.	Review the policy to verify that the problem-management process is integrated with the change-management process to ensure that incidents are addressed. Select a sample of problem tickets to verify that there was an associated change ticket.
DSS 04	Inadequate continuity management may result in the inability to ensure critical business functions.	DSS 04.01–DSS 04.02, DSS 04.05	The company has a defined and documented framework that provides: 1) A consistent company-wide process for IT continuity management. 2) A planning process that creates the rules and structures to document, test and execute the IT disaster recovery and	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 IT	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

Risk Stmt #	Risk Statement	Ctrl #	Common Controls	Preliminary Information Request	Possible Test Procedures
			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. Change control procedures are in place to ensure that the IT continuity plan is kept up-to-date and continually reflects actual business requirements.	continuity plan. Provide the procedures and evidence for testing and periodic plan updates.	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. 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

Risk Stmt #	Risk Statement	Ctrl #	Common Controls	Preliminary Information Request	Possible Test Procedures
					are stored on- and off-site.
		DSS 04.04	The company tests the IT business continuity and disaster recovery plans on a regular basis to ensure that IT systems can be effectively recovered. The company has policies in place to ensure that test results and deficiencies are communicated to management and the plan is updated as required.	Provide evidence of management's review of continuity recovery test results. Provide evidence of continuity test deficiency resolutions.	Verify that IT continuity tests are scheduled and completed on a regular basis and after 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	All critical backup media, documentation and other IT resources necessary for IT recovery and continuity plans are stored off-site in a secure location.	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.	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.
				Provide an inventory of	Inquire and verify that an inventory of backups

Risk Stmt #	Risk Statement	Ctrl #	Common Controls	Preliminary Information Request	Possible Test Procedures
				backups and media and evidence that the company periodically validates the inventory.	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.
			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	Provide evidence that	Verify that critical systems, applications, data

Risk Stmt #	Risk Statement	Ctrl #	Common Controls	Preliminary Information Request	Possible Test Procedures
			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.	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.	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. 6) Critical end-user computing data (e.g., spreadsheets). 7) Physical and logical location of data sources. 8) Security and access rights. 9) Encryption.
			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	DSS 05.01	Preventive, detective and corrective measures are in place (especially up-to-date security patches	Provide a copy of the company's policies and procedures over malicious software.	Verify that a malicious software prevention policy is established, documented and communicated throughout the organization and is included in the security policy.

Risk Stmt #	Risk Statement	Ctrl #	Common Controls	Preliminary Information Request	Possible Test Procedures
	operational information security vulnerabilities and incidents.		and virus control) across the organization to protect information systems and technology from malware (e.g., viruses, worms, spyware, spam).	Identify how the policy is communicated throughout the organization.	
				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.
				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	Provide a copy of the company's vulnerability	Verify that a vulnerability management plan is in place and has the following attributes:

Risk Stmt #	Risk Statement	Ctrl #	Common Controls	Preliminary Information Request	Possible Test Procedures
			developed and implemented.	management plan, including information on ~~recent~~ scanning ~~activities~~ and vulnerability remediation.	(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, ~~and~~ 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.
		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.

Commented [HT16]: per suggestion of MO due to duplication with DSS 05.07

Risk Stmt #	Risk Statement	Ctrl #	Common Controls	Preliminary Information Request	Possible Test Procedures
					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 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.

Risk Stmt #	Risk Statement	Ctrl #	Common Controls	Preliminary Information Request	Possible Test Procedures
			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.
		DSS 05.04–Logical Access	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.
			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.
			Policies and procedures are 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.
			User access rights to	Provide a listing of data	If predetermined and preapproved roles are

Risk Stmt #	Risk Statement	Ctrl #	Common Controls	Preliminary Information Request	Possible Test Procedures
			systems and data are in line with defined and documented business needs. This includes access rights granted to service providers.	classification and catalogs/inventories for significant data elements.	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 ~~if~~ process owners have been identified and assigned.
			User access rights are requested by user management, approved by system owners and implemented by the security-responsible person to grant, 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 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

Risk Stmt #	Risk Statement	Ctrl #	Common Controls	Preliminary Information Request	Possible Test Procedures
					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 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, key pads, 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

Risk Stmt #	Risk Statement	Ctrl #	Common Controls	Preliminary Information Request	Possible Test Procedures
					and are being followed.
			Procedures are in place to ensure that business requirements for protection or removal of sensitive data, ~~and~~ software, and hardware are met ~~upon disposal or transfer of data and hardware (endpoints, mobile devices, network devices, servers, portable media and hard drives)~~.	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.
				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.
			Physical devices, software platforms and applications within the organization are inventoried.	Provide a copy of the policy and procedures detailing the inventory requirements over devices, software platforms and applications. Provide an inventory,	Verify that all devices, software and applications are classified and inventoried and then tracked with such metrics 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

Risk Stmt #	Risk Statement	Ctrl #	Common Controls	Preliminary Information Request	Possible Test Procedures
				including operating system version numbers, of server and client end-point systems, as well as network devices.	and comply with internal policies.
		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.
			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 ~~or~~ 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	Provide information regarding the process to	Review examples of how information received has resulted in changes to the broader security

Risk Stmt #	Risk Statement	Ctrl #	Common Controls	Preliminary Information Request	Possible Test Procedures
			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.	integrate information received from information-sharing forums.	framework.
			The company has a process in place to integrate acquired entities/systems in a timely manner. The process includes a security assessment and threat analysis of existing IT systems at acquired entities.	Provide information regarding the process to integrate acquired entities/systems and timeline for doing so.	Verify that security assessment and threat analysis was properly executed for any entities acquired. Ensure that issues 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.

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

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

Risk Stmt #	Risk Statement	Ctrl #	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	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 anomolies.	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.

Risk Stmt #	Risk Statement	Ctrl #	Common Controls	Preliminary Information Request	Possible Test Procedures
					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 internal control deficiencies related to IT systems.	MEA 02.01	A process has been implemented to continuously monitor benchmark and improve the IT control environment and control framework to meet organization objectives and cybersecurity expectations.	Provide a copy of internal control monitoring activities 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 audit.	Review internal control monitoring activities for identification of control deficiencies, remediation and reporting.
				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

Risk Stmt #	Risk Statement	Ctrl #	Common Controls	Preliminary Information Request	Possible Test Procedures
					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 including background information such as education, certifications and experience.	Verify that the education, certifications and experience of the IT specialists in the internal 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 review process has been implemented to identify on a continuous basis the changes in local and international laws, regulations and other external requirements that must be complied with for incorporation into the organization's IT polices, 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 ~~their~~ its process to ensure that external obligations are addressed in IT policies and procedures.
		MEA 03.03–	A procedure has been	Provide a copy of the	Verify that the organization has a chief

Commented [BJ17]: Edit recommended by KS

Risk Stmt #	Risk Statement	Ctrl #	Common Controls	Preliminary Information Request	Possible Test Procedures
		MEA 03.04	implemented to review and report compliance of IT policies, standards, procedures and methodologies with applicable legal and regulatory requirements.	position description for the chief compliance officer, including IT compliance officer if in place.	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 review plan and procedures.	Verify that a review of the IT organization policies, standards and procedures is conducted periodically to address any non-compliance (legal and regulatory) gaps 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 require regulator confirmation of compliance (e.g., receipt of assertions) with applicable laws, regulations and contractual commitments.

