INFORMATION TECHNOLOGY (IT) EXAMINATION (E) WORKING GROUP
Conference Call
Thursday, October 13, 2022
2:00 p.m. ET / 1:00 p.m. CT / 12:00 p.m. MT / 11:00 a.m. PT

ROLL CALL

Jerry Ehlers, Chair	Indiana	Kim Dobbs/Cynthia Amann	Missouri
Ber Vang, Vice-Chair	California	Colton Schulz	North Dakota
Blasé Abreo	Alabama	Justin Schrader	Nebraska
Mel Anderson	Arkansas	Eileen Fox	New York
Ken Roulier/Bill Arfanis	Connecticut	Metty Nyangoro	Ohio
Ginny Godek	Illinois	Eli Snowbarger	Oklahoma
Shane Mead	Kansas	Melissa Greiner/Matt Milford	Pennsylvania
Dmitriy Valekha	Maryland		
NAIC Staff Support: Jacob Steilen			

AGENDA

1) Adopt prior call minutes — Attachment 1

2) Discuss and expose updates proposed by the drafting group — Attachment 2

3) Discuss new addition to Exhibit C mapping document — Attachment 3

4) Other Matters

5) Adjournment

Attachment One

ITEWG Minutes from May 2nd Call

Draft: 5/2/22

Information Technology (IT) Examination (E) Working Group
Virtual Meeting
May 2, 2022

The IT Examination (E) Working Group of the Examination Oversight (E) Task Force met May 2, 2022. The following Working Group members participated: Jerry Ehlers, Chair (IN); Ber Vang, Vice Chair (CA); Blasé Abreo (AL); Mel Anderson (AR); William Arfanis and Ken Roulier (CT); Ginny Godek (IL); Dmitriy Valekha (MD); Kim Dobbs and Cynthia Amann (MO); Eileen Fox (NY); Metty Nyangoro (OH); Eli Snowbarger (OK); Melissa Greiner and Matt Milford (PA).

1. Discussed its 2022 Project List

Mr. Ehlers called the meeting to order and said that the purpose of the meeting was to discuss the 2022 Project List. Mr. Ehlers said that prior to the meeting, preliminary feedback regarding possible projects was collected from the Working Group members via an email survey. The results of that survey are captured in the 2022 Project List. Mr. Ehlers then gave a summary of the Working Group's Project List which included: 1) consideration of guidance updates within the Financial Condition Examiners Handbook (Handbook) pertaining to cloud storage environments and insurers that outsource portions of their IT activities; 2) consideration of possible guidance updates within the Handbook to add the concept of prospective risks to the IT Review; and, 3) development of general best practices for supplemental parts of an IT Review, like coordination activities across states or communication with state insurance analysts and/or contract resources (e.g., examiners, specialists, etc.).

Mr. Ehlers proposed the formation of a drafting group to address the projects and bring guidance suggestions back to the Working Group for consideration. There were no objections. Mr. Ehlers asked that individuals interested participating in the drafting group reach out to Jacob Steilen (NAIC) by May 9.

Jenny Jeffers (Jennan Enterprises, LLC) asked if contractors could be on the drafting group. Mr. Steilen said the drafting group would allow contractors due to the specialized knowledge required to accomplish these projects.

Tom Finnell (America's Health Insurance Plans—AHIP) asked how the projects would be brought back to the full working group for review. Specifically, if the full working group would review the projects individually or as a package. Mr. Steilen stated that the changes would be presented to the Working Group as a package and would be exposed for a public comment period prior to the Working Group considering any changes for adoption into the Handbook.

Bruce Jenson (NAIC) asked if the second project related to IT prospective risks is intended to help clarify whether the investigation of prospective risks related to IT systems should be documented on Exhibit V as part of the financial examination or within Exhibit C as part of the IT Review. Mr. Steilen affirmed that is the intention of the project.

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

SharePoint/NAIC Support Staff Hub/Member Meetings/E CMTE/EOTF

Attachment Two

Drafting Group Updates:
- Section 1-3
- Exhibit C

may find it more useful to corroborate the remediation of the findings as opposed to performing an independent review of the company's controls to confirm the findings' existence.

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

5. Document Results of IT Review

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

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

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

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

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

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

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

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

6. Assist on Financial Examination

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

Commented [SJ1]: Want to give the option to have IT examiners stay involved in managing prospective IT risks. E.g. company is switching from a legacy system to a new system during the exam period, IT examiner could help with questions and risks regarding the new IT system as the exam progresses.

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

Cybersecurity Considerations

As the examiner reviews an insurer's operations, he or she may determine that the insurer has significant exposure to cybersecurity risks. The specific risk exposure for the insurer may vary based on volume, type of sensitive information (e.g. Social Security numbers, protected health information, personally identifiable health information, etc.) and the broad security environment in which the insurer is operating. The examiner should be mindful that the insurer is not required to use any particular IT security framework, nor are its IT security systems or controls required to include all of the components of any single or particular IT security framework or the examiner's work program. The examiner should broadly consider not only the volume and type of sensitive information obtained, maintained or transmitted by the insurer, but also the laws and regulations to which the insurer is subject, as well as the size and complexity of the insurer's operations and the nature and scope of its activities. All of these factors will influence the cybersecurity policies and systems and the IT security framework or frameworks that are appropriate for a particular insurer to effectively protect its sensitive information. As a result, responding to a particular insurer's risk will require judgment by the examiner in tailoring the use of existing the findings as opposed to performing an independent review of the company's controls to confirm the finding's existence.

Regulators should also consider the sensitivity of the information contained in these reports, as they request access to and document their review of the reports. Regulators should consider whether an on-site, "read only" review is appropriate, especially in situations whether the reports make specific references to identified vulnerabilities. Regulators may also wish to only document a general summary of their review as opposed to making more specific notations of their review based on the sensitivity of the information contained in the reports reviewed.

Note that in situations where management has contracted with third-parties to perform cybersecurity assessments, IT examiners can leverage the procedures performed based on the examiner's judgment. In determining the degree of reliance, the IT examiner should consider the factors noted in Handbook Section 1, Part III (F) under the subsection "SSAE 18 and Service Organization Control Reports" and Section 2, Phase 1 (C) under the subsections "Decision Whether to Utilize the Work of Auditors" and "Utilization of Company-performed Testing."

Small/Medium-Sized Company Guidance

For many small or medium-sized insurers, a number of the risks and suggested test procedures included within this work program may not be relevant. As such, the risks identified and testing to be performed should be customized to meet the needs of each individual examination. However, the work performed should allow the examination team to determine whether general reliance can be placed on a company's IT general controls. To ensure that sufficient work is performed, the customized program should continue to address each of the four primary COBIT domains, at least at a basic level. Examiners may find it useful to reference COBIT QuickStart guidance available to assist in customizing the work program for a smaller insurer. In addition, other instructions for completing an IT review for small/medium-sized companies can be found in Section 1, Part III, under "General Information Technology Review."

Additional explanations for the information included in this document and how it may be used by the examiner are as follows.

Companies who heavily outsource IT functions

Companies that heavily outsource their IT functions are not exempt from the IT examination process, nor are they exempt from risks associated with the outsourced data and functions. If company data is stolen from a third-party, the company's business operations and reputation could still be affected. In these situations, examiners should shift their focus to evaluating how the company is ensuring that the third-party hosting their data is keeping it secure (review the APO 10 procedures for more information on third-party risks). Additionally, examiners should evaluate how the company ensures that the data is appropriately backed up and is recoverable.

Commented [SJ1]: Made this a standalone paragraph based on feedback. Although the guidance is mainly aimed at small/mid size companies, there could be larger companies who also outsource the majority of their IT functions.

Risk Statement

The risk statements provided within the work program are the most common general IT control risks an examiner will likely encounter at an insurance company. This is not designed to be an all-inclusive list of common risks at a company. The information gathered from the ITPQ and other relevant sources should assist the examiner in identifying other risk statements that apply to the company.

Common Controls

The common controls provided within the work program indicate how a typical insurance company might mitigate the specific risks shown in the "Risk Statement" column, but may not apply to each individual company. Each company has its own controls in place to mitigate the identified risks, which may or may not correspond to the common control identified within the work program. Therefore, the company might have adequate controls in place, even if the control does not match the common control listed in the work program. The examiner may wish to provide the common controls to the company under examination to assist the company in developing responses, including controls used to mitigate the identified risk statements.

EXHIBIT C
IT REVIEW STANDARD SUMMARY MEMORANDUM

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

Salutation

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

Background and Scope

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

Summary of Control Environment

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

Work Performed

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

Summary / Detail of Findings (Including Cybersecurity Related Findings)

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

Findings

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

Commented [SJ1]: Added a datapoint to this chart to 1) put more emphasis on our 2021 guidance addition on mitigating factors and 2) it would support our current objective by helping examiners classify resolved risks from ones that are prospective in nature.

Prospective IT Risks

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

Commented [SJ2]: Per drafting group request - added this new section which can be used to list prospective IT risks. Clarified these should be directly applicable to the insurer so avoid overly vague and general risks such as "cybersecurity risk" or "ransomware" which are omnipresent and applicable to all companies.

Conclusion/Results of IT General Control Review

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

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

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

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

Meeting with Examiner-In-Charge and Other Financial Examiners

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

Assistance on the Financial Examination

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

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

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

Attachment Three

Mapping Document addition

DRAFT

Potential Considerations for Mapping to SOC 2 TSC Security & Availablity

Exhibit C #	*SOC 2 TSC #*	*SOC 2 TSC*
APO 01, DSS 01	CC1.1	COSO Principle 1: The entity demonstrates a commitment to **integrity and ethical** values.
APO 01	CC1.2	COSO Principle 2: The board of directors demonstrates **independence** from management and exercises oversight of the development and performance of internal control.
APO 01	CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, **reporting lines, and appropriate authorities** and responsibilities in the pursuit of objectives.
APO 01, DSS 01	CC1.4	COSO Principle 4: The entity demonstrates a commitment to **attract, develop, and retain** competent individuals in alignment with objectives.
MEA 01	CC1.5	COSO Principle 5: The entity holds individuals **accountable** for their internal control responsibilities in the pursuit of objectives.
	CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, **quality information** to support the functioning of internal control.
APO 02, 04, DSS 02	CC2.2	COSO Principle 14: The entity **internally communicates** information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
APO -9, DSS 01	CC2.3	COSO Principle 15: The entity **communicates with external parties** regarding matters affecting the functioning of internal control.
APO 10, 12, MEA 03	CC3.1	COSO Principle 6: The entity specifies **objectives** with sufficient clarity to enable the identification and **assessment of risks** relating to objectives.
APO 10, 12, DSS 01	CC3.2	COSO Principle 7: The entity **identifies risks** to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.
APO 10, 12	CC3.3	COSO Principle 8: The entity considers the potential for **fraud** in assessing risks to the achievement of objectives.
APO 10, 12, DSS 01	CC3.4	COSO Principle 9: The entity identifies and assesses **changes** that could significantly impact the system of internal control.
DSS 01	CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
DSS 01, MEA 02	CC4.2	COSO Principle 17: The entity evaluates and **communicates internal control deficiencies** in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.
BAI all	CC5.1	COSO Principle 10: The entity **selects** and develops **control activities** that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
BAI all	CC5.2	COSO Principle 11: The entity also selects and develops **general control activities over technology** to support the achievement of objectives.
BAI all	CC5.3	COSO Principle 12: The entity **deploys** control activities through policies that establish what is expected and in procedures that put policies into action.
APO 03	CC6.1	The entity implements **logical access security software, infrastructure**, and architectures over protected information assets to protect them from security events to meet the entity's objectives.
	CC6.2	**Prior to issuing** system credentials and granting system access, the entity registers and **authorizes new** internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are **removed** when user access is no longer authorized.
	CC6.3	The entity **authorizes, modifies, or removes access** to data, software, functions, and other **protected information assets** based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of **least privilege and segregation of duties**, to meet the entity’s objectives.

	CC6.4	The entity **restricts physical access** to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.
	CC6.5	The entity **discontinues** logical and physical protections **over physical assets** only after the **ability to read or recover data and software** from those assets has been diminished and is no longer required to meet the entity's objectives.
	CC6.6	The entity implements logical access security measures to protect against threats from sources **outside** its system boundaries.
	CC6.7	The entity restricts the **transmission, movement, and removal** of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.
	CC6.8	The entity implements controls to prevent or detect and act upon the **introduction of unauthorized or malicious software** to meet the entity's objectives.
	CC7.1	To meet its objectives, the entity uses **detection and monitoring procedures** to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.
	CC7.2	The entity monitors system components and the operation of those components for **anomalies** that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; **anomalies are analyzed** to determine whether they represent security events.
DSS 02	CC7.3	The entity **evaluates** security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (**security incidents**) and, if so, takes actions to prevent or address such failures.
DSS 02	CC7.4	The entity responds to identified security incidents by executing a **defined incident response program** to understand, contain, remediate, and communicate security incidents, as appropriate.
DSS 02	CC7.5	The entity identifies, develops, and implements **activities to recover** from identified security incidents.
	CC8.1	The entity **authorizes**, designs, develops or acquires, configures, documents, tests, approves, and implements **changes** to infrastructure, data, software, and procedures to meet its objectives.
	CC9.1	The entity identifies, selects, and develops **risk mitigation activities** for risks arising from potential business disruptions.
DSS 01	CC9.2	The entity assesses and manages risks associated with **vendors and business partners**.
DSS 01, DSS 03, DSS 04	A1.1	The entity **maintains, monitors, and evaluates current processing capacity** and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.
DSS 01, DSS 03, DSS 04	A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors **environmental protections, software, data back-up processes, and recovery infrastructure** to meet its objectives.
DSS 01, DSS 03, DSS 04	A1.3	The entity **tests recovery plan procedures** supporting system recovery to meet its objectives.

DRAFT

Exhibit C Risk Stmt #	Exhibit C Risk Statement	Potential Considerations for Mapping to SOC 2 TSC Security & Availablity
APO 01	IT organizational structure is inadequate to support business objectives.	CC1.1-CC1.4
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.	CC2.1 - CC2.2
APO 03	Enterprise goals may not be met because the data and systems architecture is poorly defined, and/or fragmented.	CC6.1
APO 04	Company operations may lack efficiency and competitive advantage because system technology is obsolete and poorly aligned with business objectives.	CC2.2
APO 06	The IT budget is not representative of the organization's goals and business needs and IT expenses are not properly allocated.	
APO 09	IT-enabled services and internal service levels are not managed to ensure that IT services align with enterprise needs and expectations.	CC2.3
APO 10	Third party service provider risks are not properly assessed and addressed during the procurement process.	CC3.1-CC3.4
APO 12	IT-related enterprise risks have not been integrated into the overall enterprise risk management (ERM) program.	CC3.1-CC3.4
BAI 01	IT projects may fail to meet business objectives/Enterprise Risk Management goals or run over budget in the absence of an effective program and project management methodology.	CC5.1, CC 5.2, CC5.3
BAI 02	Projects are initiated with out proper authorization or analysis.	CC5.1, CC 5.2, CC5.3
BAI 03	Project deliverables fail to meet business objectives due to inadequate design and/or ineffective oversight of implementation.	CC5.1, CC 5.2, CC5.3
BAI 04	Systems fail to meet current and future business needs due to inadequate planning for capacity, performance and availability.	CC5.1, CC 5.2, CC5.3
BAI 06 & 07	Systems lack of proper change management threatens system stability or integrity.	CC5.1, CC 5.2, CC5.3
BAI 08	Systems cannot be properly managed and optimized due to inadequate documentation and training.	CC5.1, CC 5.2, CC5.3
BAI 10	Lack of configuration management threatens system stability, integrity, and recovery.	CC5.1, CC 5.2, CC5.3
DSS 01	The quality, timeliness and availability of business data is reduced due to an ineffective data management process.	A1.1-A1.3
	The operation of outsourced IT services is not managed to maintain the protection of enterprise information and reliability of service delivery.	CC1.1, CC1.4, CC2.3, CC3.2, CC3.4, **CC9.2**
	Lack of infrastructure monitoring may result in the inability to detect or recognize security incidents.	CC4.1, CC 4.2
DSS 02	Inadequate physical and environmental controls may result in unauthorized access and inadequate protection of data.	
DSS 03	The company has an ineffective problem management process, which reduces system availability, service levels, customer satisfaction and increases operating costs.	A1.1-A1.3
DSS 04	Inadequate continuity management may result in the inability to ensure critical business functions.	A1.1-A1.3