SOUNDTRANSIT

Audit Report

Information Security Governance Audit

Report Number: 2020 - 04 | Report Date: July 13, 2020

DATA CLASSIFICATION: UNRESTRICTED

Executive Summary

Audit Report No.: 2020 - 03 **July 13, 2020**

WE AUDITED the current Information Security Governance (ISG) oversight process to assess the controls in place over the monitoring of information security (InfoSec) risks, compliance requirements, and remediation efforts.

AUDIT OBJECTIVES were to determine whether the agency has effective InfoSec oversight processes in place to ensure:

- InfoSec risks and compliance requirements associated with key agency functions (strategic and business) are adequately managed within acceptable levels of risk.
- Remediation efforts required to address significant risks are continuously monitored, evaluated, and communicated for effectiveness.

The audit examined the agency's oversight process and management controls in place as of March 2020.

DocuSigned by:

Patrick Johnson

D893DEC00D0B4A6...

Patrick Johnson
Director of Audit

WHAT WE FOUND?

As Sound Transit's (ST or agency) physical footprint increases, for both ST2 and ST3 projects throughout the Puget Sound region; ST's information security systems must also look to increase the needs associated with preserving critical agency information. Thus, the InfoSec division remains committed to proactively safeguarding ST's information assets, while enhancing information security practices agency-wide.

A key function of the InfoSec program includes facilitating oversight activities through the performance and reporting of an agency-wide risk management strategy – primarily focused on all ST information systems, technologies and applications.

The agency's risk management process is guided by comprehensive policies, laws, and standards, requiring a risk-based approach that leverages security or operational controls to mitigate risk. The process consists of four sequential steps that are used to systematically identify risk and establish risk-informed security priorities.

Currently, InfoSec is 'self-governed' as a sub-function of IT (i.e., under 'IT Business'), in which quarterly meetings of information security priorities are discussed internally within pertinent IT leadership. High level reporting are also made to Executive Leadership primarily through the Chief Information Officer (CIO) and disseminated to the agency's Governance Councils, as needed.

Our audit concluded that the agency's current ISG process has control deficiencies related to: (1) informal communications and reporting lines; and (2) inadequate continuous monitoring of performance actions (i.e., quality of risk treatment actions). As such, there is 'limited assurance' that management controls in place are effective in supporting ISG activities. See **Finding #1.**

Table of Contents

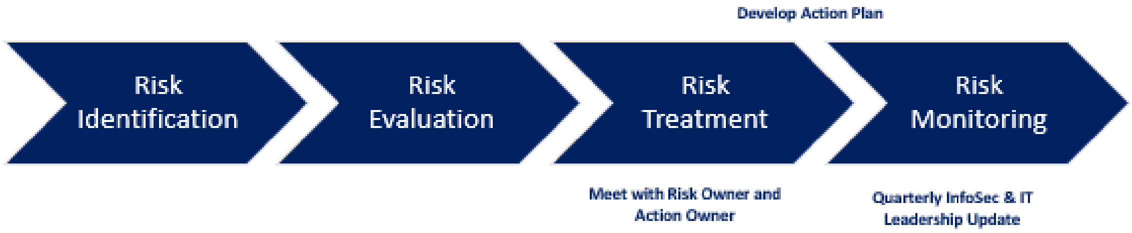
Background

As Sound Transit's (ST or agency) physical footprint increases, for both ST2 and ST3 projects throughout the Puget Sound region; ST's information security systems must also look to increase the needs associated with preserving critical agency information. Thus, the InfoSec division remains committed to proactively safeguarding ST's information assets, while enhancing information security practices agency-wide.

A key function of the InfoSec program includes facilitating 'oversight activities'[1] through the performance and reporting of an agency-wide 'risk management strategy' – primarily focused on all ST information systems, technologies or applications.[2]

The agency's InfoSec risk management process is guided by comprehensive policies, laws, and standards,[3] requiring a risk-based approach that leverages security or operational controls to mitigate risk. The process includes risk identification, risk evaluation, risk treatment, and risk monitoring wherein results are continuously assessed and updated in InfoSec's centralized risk register.[4] InfoSec also performs an 'annual risk assessment' that assesses ST's maturity and risk impacts to the agency's strategic plan.

As part of its oversight, routine 'risk reviews' between InfoSec and key stakeholders are held quarterly (at a minimum) and/or where appropriate to report information security risks. Key objectives include, among many, (1) gaining agreement on proposed remediation actions; (2) establishing appropriate timeframes for mitigation; and (3) validating the level of progress through sufficient evidence obtained (e.g., fieldwork observation and physical/documentation).



Source: AD prepared (Retrieved from: InfoSec Risk Management Manual [dated 08/27/19]; and process walkthroughs).[5]

Currently, the division is 'self-governed' as a sub-function of IT (i.e., under 'IT Business') wherein quarterly meetings of information security priorities are discussed internally within pertinent IT leadership and stakeholders. High level reporting are also made to Executive

[1] Policy 1100 (dated, 01/17/17) established the agency's Information Security Management System (ISMS) [or head of InfoSec] to administer and oversee the: (1) Communication of the agency's risk management strategy for InfoSec; (2) Provision of clear InfoSec guidance to staff and contractors; and (3) report on the performance of InfoSec risk posture.

[2] Distribution or risks are comprised of: (1) Unacceptable – High risks requiring the implementation of additional controls to immediately mitigate the risk; (2) Undesirable – Moderate risks requiring for the planning of additional controls; and (3) acceptable – Low risks requiring the acceptance and/or 'carry further' of mitigation actions if they can be achieved with little to no cost. Risks and related 'action status' are classified as 'treated' (i.e., monitoring & completed) and 'untreated' (i.e., not started and in-progress) risk exposures. Risk ratings are derived directly from the rating criteria set for other risk management functions within the agency, such as Safety (e.g. Agency Safety and Security Management Plan [dated, Aug. 2018]).

[3] Refer to 'scope & methodology section' for more details.

[4] Risks identified from the varying risk management approaches (e.g., annual risk assessment, risk candidate lists, etc.) are recorded in the Information Security Risk Register in order to be evaluated, treated, monitored, and reported on.

[5] Refer to 'findings and recommendations' for more details.

Leadership primarily through the Chief Information Officer (CIO) and disseminated to the agency's Governance Councils or other committees[6], as needed.

Moreover, InfoSec Program is regularly subjected to independent reviews to determine if the agency's information systems and security conforms to industry standards (i.e., ISO 27000 series controls); and facilitates scheduled compliance audits driven by regulatory and contractual requirements (e.g., DOL and PCI reviews).

Audit Objectives

To determine whether Sound Transit has an effective Information Security (InfoSec) oversight processes in place to ensure:

1. InfoSec risks and compliance requirements associated with key agency functions (strategic and business) are adequately managed within acceptable levels of risk.
2. Remediation efforts required to address significant risks are continuously monitored, evaluated, and communicated for effectiveness.

Scope and Methodology

We conducted this audit in accordance with the International Standards for the Professional Practice of Internal Auditing and Generally Accepted Government Auditing Standards (GAGAS). Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained, and reported upon below provides a reasonable basis for our findings and conclusions based on our audit objectives.

Over the course of the audit, we gained an understanding of the InfoSec oversight process at the agency and department/division level through data analysis, observation, documentation reviews, and personnel interviews. We identified risks in the processes and assessed management controls in place to mitigate those risks. Based on our assessment of management control effectiveness, we focused on controls over the agency's oversight process to manage information security risks/compliance requirements and the communication of its effectiveness as of March 31, 2020.

The audit reviewed reports, policies and processes for the period of performance as of March 31, 2020. Based on our audit objectives above, we examined the following:

Objective 1:

To determine whether the agency has an effective oversight process in place to ensure InfoSec risks and compliance requirements associated with key agency functions (strategic and business) are adequately managed within acceptable levels of risk, we performed the following procedures:

a. Conducted comprehensive examinations of agency policies/informational assets[7];

[6] In summer 2019, three Governance Councils were formed in line with the agency's strategic plan and Design for Growth initiative, replacing the existing Executive Leadership structure, formerly known as the "ELT." Occasionally, InfoSec may report to the Technology Investment Committee (TIC) [supersedes Technology Governance Team] for IT-led/managed projects outside routine activities.

[7] Reviewed agency documents to include: **Policies** – Policy 1100 Information Security; InfoSec Risk Management Manual (Ver. 2, 08/27/19); InfoSec Management System (ISMS) Charter (Ver. 1.1, 08/19/19); Risk Council Charter ST Information

external/internal agency assessments; and related laws and standards (e.g., ISO 27001/27002 InfoSec Framework, Payment Card Industry [PCI] Data Security Standard, and OCIO Policy 141.10l) to gain a sufficient understanding of the audit environment.

b. Conducted over 15 interviews; and process walkthroughs to determine if controls were working effectively as intended. Individuals interviewed were comprised of CIO, Chief Information Security Officer (CISO), D-CISO, Director-Systems Engineering & Integration, Director-Operations Engineering & Technology, Deputy Director-Operations Technology (OT) Manager-Transit Systems Engineering, and Information Security Architect.

Objective 2:

To determine whether the agency has an effective oversight process in place to ensure remediation efforts required to address significant risks are continuously monitored, evaluated, and communicated for effectiveness, we performed the following procedures.

a. For the 4 areas examined, performed analysis of 25 treatment actions against corresponding audit evidence (i.e., documentary and inquiry/corroboration) to determine if the agency verifies remediation progress for adequate monitoring and reporting. Supporting documents reviewed included InfoSec risk reports (inclusive of external assessment briefings), ISO 27002 Assessment Control Matrix, redacted InfoSec risk register[8], prior InfoSec Risk Council minutes, analysis (e.g., active directory lists), and related manuals (e.g., OT Cybersecurity for Integrate Automation).
    i. Provided a summary of remediation progress (i.e., executed and pending actions) to determine to what extent treatment actions were implemented.
    ii. Performed analytical procedures (as appropriate) to test evidence received.

Conclusion

Consistent with Internal Auditing Standards, governance is an integrated process comprised of risk management and control (collectively referred to as GRC).[9] While ST has taken actions to administer oversight activities across key divisions, our audit revealed one finding related to an inadequately defined information security governance structure. Barring a formal ISG process, the agency's risk management approach is guided by well-defined information security policies; conducts comprehensive risk assessments for proposed risk treatments; and continues to manage and monitor information security risks within 'internal working groups' comprised of key stakeholders, InfoSec, and IT Leadership.

However, due to the lack of a formal and defined ISG process, the preceding finding identified has resulted in the following control deficiencies related to: (1) informal communications and reporting lines; and (2) inadequate continuous monitoring of

Security (Ver. 1, 05/08/18); Data Classification and Protection Standard (Ver.1.2, 03/828/17); and Policy 1101 – Acceptable Use of Technology Policy (dated, 05/08/17); **InfoSec Materials** – COP Material; InfoSec Awareness Training; and GRC Process Flowcharts; and related internal/external **Agency Assessments** – 2019 Annual Risk Assessment; Link Light Rail OT Assessment (dated, 02/21/20); 2018 & 2019 Information Security Maturity Compliance Assessment Reports; PCI Data Security Standard Assessment Report (dated, 09/23/19); and 2019 Data Security Assessment – DOL (dated, 12/24/19).

[8] For the purpose of our review, the InfoSec risk register was classified as 'restricted' in line the agency's 'Data Classification and Protection Standard'. As such, we obtained a redacted version of risk register excel file (e.g., risk treatment column), in which the information contained therein must be protected from public disclosure.

[9] International Professional Practices Framework (IPPF) section 2110 'Governance' requires the internal audit to assess and make appropriate recommendations to improve the agency's governance process for making strategic and operational decisions; overseeing risk management and control; and communicating risk and control information to appropriate areas of the organization.

performance actions (i.e., quality of risk treatment actions). Moreover, we observed in a separate ‘Management Letter’ that although other key risk management functions (e.g., Safety & Emergency Management) have differing policies, ST lacks a holistic ‘Risk Management Policy’ for consistency and application across the agency.

Thus, the audit concluded that there is ‘limited assurance’ that management controls in place are effective in supporting ISG activities and driving remediation efforts. To address the audit finding and related control deficiencies, we recommended two corrective actions for management’s review and disposition.

Findings and Recommendations

Information Security Governance has not been Formally Defined at the Agency

Policy 1100 (dated, 01/17/17) sections 2.2 (2.2.1)-(2.2.3) established the InfoSec division to administer and oversee the: (1) Communication of the agency's risk management strategy for information security; (2) Provision of clear InfoSec requirements to staff and contractors; and (3) report on the performance of information security risk posture. Since its establishment, InfoSec ISMS Charter (ver. 1.1, dated 08/19/19) – a document approved by the CISO – sections 3.3 and 5.5.26 enhanced Policy 1100 by requiring the need of an 'Information Security Risk Council' (or risk council) to support and provide oversight during the information security risk management process; and ensure the ISMS goals are aligned with the agency's strategic direction.[10]

In June 2019, the risk council was discontinued due to the formation of the agency's Governance Councils (supersedes Executive Leadership Team [ELT]) as part of ST's Design for Growth initiative. This in turn, essentially reauthorized InfoSec as the oversight function consistent with Policy 1100. Barring an agency risk council (an executive level function), the audit sought to provide assurance over controls in place to manage information security risks and communication of their effectiveness to those in charge with governance. The audit examined four areas related to the agency's oversight process:

Based on our review, we found control weaknesses related to (1) informal communication and reporting lines; and (2) inadequate continuous monitoring of performance actions (i.e., quality of risk treatment actions). Specific exceptions noted were as follows:

- Lack of documented 'risk treatment plans' (feedforward control) for all areas examined; and
- 76% treatment actions independently reviewed are still pending resolution within the last three years.

The conditions above occurred due to the lack of a formally defined ISG structure (e.g., separate committee or streamlined [e.g., governance or TIC]) designed to support and provide direction for the development of a 'risk management strategy.' Thus, there is an increased risk that mitigation efforts may be further delayed and of limited effectiveness, thereby impacting ST's ability to achieve a reasonable risk posture agency-wide.[11]

Reporting and Monitoring needs to be Strengthen for Proper Oversight

Consistent with Policy 1100, InfoSec Risk Management Manual (dated, 08/27/19) sections 2.3.1 and 3.3 specifies that a key component of the ISMS includes the development of an agreed-upon 'risk treatment plan[12]' and accompanying 'risk reviews' between InfoSec, key

[10] Per ISMS Charter section 3.3, the intent of the council was to oversee the agency's risk posture, provide sponsorship of remediation activities, assign single points of accountability for risk mitigation, and set the risk appetite for the agency.

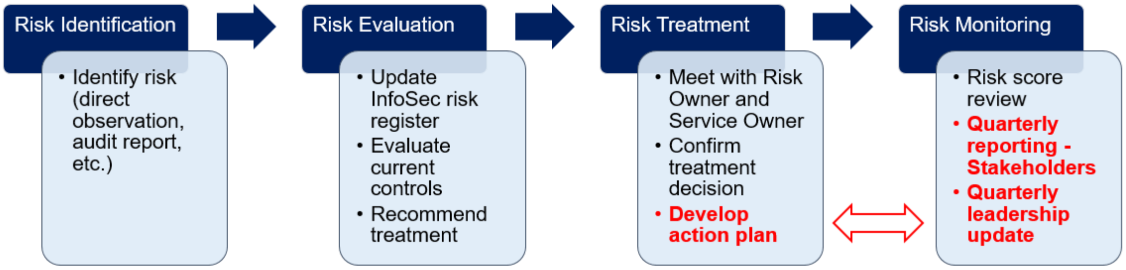
[11] InfoSec Maturity Compliance Assessment Report (dated, 09/30/19): External assessors determined that ST has increased its overall information security program maturity level from 2.2 in 2017 to 3.2 in 2019 of out of a possible score of 5 and compliance score from 58% in 2017 to 97.4% in 2019.

[12] Risk Treatment Plan: In alignment with Additionally, ISO 27001 section 6.1.3 (e)(f), recommendations from the InfoSec team in collaboration with key stakeholders to implement additional controls, processes or technologies to reduce risk to the agency. The Risk Treatment Plan should be signed-off with an expected date to complete the remediation activity(ies).

stakeholders,[13] and Leadership. On-going risk reviews are required to be held quarterly (at a minimum) and/or where appropriate to report InfoSec findings (or information security risks) derived from its 'risk reports.'[14] Key objectives of the risk reviews as it pertains to the risk treatment plan includes:

1. Gaining agreement on proposed remediation actions;
2. Establishing appropriate timeframes for mitigation; and
3. Validating the level of progress through sufficient evidence obtained (e.g., fieldwork observation and physical/documentation).

Per agency policy, the risk treatment plan must be signed-off with an expected date to complete the remediation activities. This is integral in ensuring continuous monitoring and evaluating of actions taken to address identified risks.[15]



Risk Identification
- Identify risk (direct observation, audit report, etc.)

Risk Evaluation
- Update InfoSec risk register
- Evaluate current controls
- Recommend treatment

Risk Treatment
- Meet with Risk Owner and Service Owner
- Confirm treatment decision
- **Develop action plan**

Risk Monitoring
- Risk score review
- **Quarterly reporting - Stakeholders**
- **Quarterly leadership update**

Source: AD prepared (Retrieved from: InfoSec Risk Management Manual [dated 08/27/19]; and process walkthroughs).

For the purposes of this audit, we examined unacceptable risks to determine if the current process is effective in capturing and reporting pertinent information within a defined timeframe that allows users to respond and carry out their responsibilities. As such, we obtained available documentation for review and conducted related interviews/walkthroughs to evaluate the current remediation progress (i.e., status of treatment actions); and management assertions that support mitigation efforts.[16]

Based on our review and audit procedures applied, we noted the following exceptions, evidencing control deficiencies related to (1) informal communication and reporting lines; and (2) insufficient monitoring of performance actions. Specifically:

- For all areas examined, while 'risk reports' were provided to establish mutual integration requirements and proposed risk treatments, we found that the agency (InfoSec and key divisions) did not fully develop a coherent risk treatment plan (as seen in the diagram above) detailing specific corrective action(s) and established timeframes as a whole.

Furthermore, the lack of a formal reporting structure has also contributed to inadequate 'feedback loops' (e.g., acknowledge receipt of proposed risk treatment and timelines; documented 'go-forward plans'; etc.) that reinforces continuous evaluation and accountability in driving mitigation efforts. An examination of 25 risk treatment activities for

[13] Key stakeholders include Risk Owners, Risk Owner Delegates, and Service Owners. 'Risk owners' and person who has ownership of quality and the end result. Risk owners may delegate the tactical ownership to a 'Risk Owner Delegate'. Additionally, 'Service Owners' are persons responsible for managing one or more services (or technologies) throughout their entire lifecycle, under the direction of the Risk Owner.

[14] An informational tool to ensure visibility of identified and documented and information security risks per delegated areas of responsibility.

[15] Retrieved from: ISMS Charter (dated, 08/19/19).

[16] Refer to 'scope & methodology section' for more details.

the 4 areas selected revealed 19 (or 76%) actions are still 'pending resolution' within the last three years.

Based on our analysis, we observed the following:

- For risk #1, 92% of actions remain outstanding as of May 2017. Specifically, of the 12 actions, 11 were additional recommendations identified; and one is related to the subsequent approval of 'InfoSec's Proposed Remediation Plan'.[17]
    - We noted that although internal deliberations are still on-going, further examination of the 'planning proposal' would require governance as a critical component in executing mitigation strategies (e.g., staffing, funding, implementation of technical work, etc.).
- For risk #2, 43% of actions remain outstanding as of September 2017; and is also related to a repeat audit finding.[18] The action items were assessed as being primarily related to subpar vendor performance (as oppose to governance).
- For risk #3, associated actions remain outstanding as of April 2018; and is also related to a repeat audit finding.[19]
    - We noted that pending treatment actions were identified as part of the InfoSec Strategic Roadmap, requiring dedicated staffing resources as the appropriate remediation effort. Further confirmation with Budget staff revealed that the preceding headcounts were not considered as part of the 'hiring exemptions list' for the current year.
- For risk #4, 67% of actions remain outstanding and were primarily related to the development of a go-forward plan by DECM (as the risk owner).

During the course of our audit, we noted that InfoSec has made strides in implementing its GRC ServiceNow module and has imported its risk register into the application. GRC application would provide structured workflows for risk management services and enhance on-going monitoring activities and collaboration with stakeholders agency-wide.

Overall, the preceding conditions occurred due to the current informal ISG process, evidencing (1) inadequate visibility of executed actions against mitigation plans; and (2) an insufficient mechanism required to evaluate the appropriate risk response for re-alignment (e.g., formal risk acceptance with documentation, leveraging an existing control for cost savings, etc.).[20]

Furthermore, while interviews with division staff revealed that the agency has implemented ad-hoc communication channels as a 'compensating control', the process does not allow for InfoSec to effectuate long-term 'enforcement capabilities' and escalate significant security issues to senior leadership. Thus, we noted that the lack of a deliberative body that promotes accountability and due diligence, increases the likelihood that unacceptable risks will continue to remain outstanding and exceed risk acceptance levels.

[17] InfoSec 'May 2020 Proposed Remediation Plan' would consist of a 4 to 5 year program, estimating $6.3 million. Key activities would require a combination of governance, technical work, and dedicated staffing resource, if approved.
[18] Retrieved from: PCI Data Security Standard Assessment Report (dated, 09/23/19). AD notes that detailed testing of accounts (i.e., accuracy and completeness) will be conducted in AD concurrent report – 'Consultant On/Off-Board Practices Audit'.
[19] Retrieved from: 2019 Information Security Maturity Compliance Assessment Reports.
[20] ISO 27001 delineates four risk responses: (1) Apply security controls; (2) Transfer the risk; (3) Avoid the risk; and (4) accept the risk.

Recommendations

We recommend agency Leadership and InfoSec staff increase collaborative efforts to enhance the agency's current oversight process as shown below:

1. Accelerate current initiatives to strengthen communication, reporting, and monitoring controls that support information security governance. Specifically as it relates to:
    a. Enhancing communication protocols between senior leadership and InfoSec for continuous monitoring and evaluation of the quality of performance of risk treatment activities. This may also include providing a 'direct channel' for the CISO to discuss with agency leadership relevant enablers (e.g., InfoSec resources and tools) that can deliver results consistent with the risk tolerance set by agency leadership.
    b. Strengthening adherence to the development of an agreed-upon risk treatment plan for each area of responsibility and ensure results are captured in a comprehensive risk management strategy reportable to leadership.

2. Evaluate existing governance structure and related policies (e.g., Policy 1100, ISMS Charter, etc.) to determine the appropriate level of oversight tailored to meet ST's needs and desirable risk posture. Key considerations include (not an exhaustive list):
    a. Defining the roles and responsibilities for information security governance.
    b. Determining appropriate level of representation.
    c. Identifying criteria for escalating significant security issues.

Management Response

The Information Security Division of Sound Transit IT agrees with the findings and observations noted in the Management Letter and in the Audit Report provided in connection with the recently conducted audit of Information Security Governance at the agency.

For the two recommendations in the Audit Report, Information Security is committed to implementing enhancements to the following areas:

- Strengthening communication, reporting, and monitoring controls that support information security governance and risk management.
  - In May 2020, Information Security deployed a Governance, Risk and Compliance module within the agency's Service Now platform, to help address concerns around the risk management and compliance processes, as outlined in the 5-year Information Security Strategic Plan and the 2020 Information Security Roadmap.
  - The new module is now live for both Compliance and Risk Management activities, and should help alleviate resource constraints associated with the existing volume of risks being managed, through the automation of heavily-manual processes.
  - Information Security will work individual Risk Owners and delegates to review the current risk register, develop comprehensive risk treatment plans, and continuously monitor risk treatment progress.
  - Information Security will be meeting with individual Risk Owner Delegates and Service Owners on a quarterly basis to ensure communication and reporting is strengthened.
  - Information Security will offer training to Risk Owners and delegates to ensure they are able to proactively consume the information on identified risks in their respective areas of responsibility. Two of such sessions have already been completed as of the date of this response.
  - Information Security will review and update the program charter and risk management manual to align with the new processes driven from the recommendations.
  - Information Security will continue to expand coverage of its risk management processes and risk reporting, to ensure all agency functions are being addressed through the standard processes.
  - This process is being launched in July of 2020
  - **Estimated Completion Date: Q4 2020**

- Evaluate and implement the appropriate level of executive oversight
  - Information Security is currently working with Executive Leadership (CIO and DCEOs) to design and implement a relaunched Information Security Risk Council.
  - The proposed Risk Council will begin to meet on a quarterly basis in Q3 2020 and will be tasked with providing direction, sponsorship and oversight of the agency's Information Security Program, while serving as the collective risk owner for the agency's information security risks.
  - The implementation of the new Risk Council will include redefining roles and responsibilities as well as developing criteria for escalating security risks and

issues.

- **Estimated Completion Date: Q4 2020**

Regarding the recommendation listed in the Management Letter, given that the successful implementation of an Enterprise Risk Management function is an organizational-level initiative, it would require input and participation from the rest of with risk management functions besides Information Security. Such an effort has the highest likelihood of success if it is championed by executive leadership, in the context of agency transformation activities. Information Security is committed to providing input and assisting with the process of developing and implementing an overarching enterprise risk management policy and program that align with industry standards and adequately account for the needs and nuances of information security risks. Information Security is also committed to procuring the necessary sponsorship from executive leadership, and driving the development of a board-level policy to supplement Agency Policy 1100 to address the identified gap when compared to the other cited risk management functions.