JOHNS HOPKINS

Institutional Computing Standards

Risk Assessment Guidance

Approved by the ICSC, January 2010
Revisions Approved, May 2018

I. Table of Contents

II. Summary

This guidance outlines the assessment process for security and related risks for Johns Hopkins systems. This document emphasizes the necessity for bringing together a risk assessment team, identifying assets, finding risks, and assessing the value of controls. It is critical that such assessments be undertaken for Restricted Systems (systems hosting PHI or PII) on a regular basis. It is the responsibility of the individual department owning the information assets to ensure appropriate risk assessment practices are implemented. IT@JH Information Security have provided tools for completing these assessments, but these are in the forms of guidance and checklists, not the principal substance of the assessment. There is no substitute for knowledgeable staff working through risk factors and cost effective controls.

III. Introduction

A. Background

Information Security Compliance and Risk Assessment practices are now required by the government when accessing or administering government data. The General Services Administration (GSA) has developed policy and framework for Controlled Unclassified Information (CUI). CUI is unclassified information that requires safeguarding and dissemination controls pursuant to law, regulation, or Government-wide policy, as listed in the CUI Registry by the National Archives and Records Administration (NARA). Partnering on government contracts and/or research projects now require compliance with various government defined standards e.g.

DFARS – Defense Federal Acquisition Regulation Supplement
https://www.federalregister.gov/documents/2018/01/31/2018-01781/defense-federal-acquisition-regulation-supplement-procurement-of-commercial-items-dfars-case

FISMA – Federal Information Security Management Act
https://csrc.nist.gov/projects/risk-management/detailed-overview

Information security is a practical discipline – including the hundreds of tactical decisions that users and administrators make regarding management of systems. There is also now a certain process and documentation requirements that together can be described as a three-step process:

- Risk Assessment
- Security Planning
- Security Evaluation

This guidance is geared towards the first two of these considerations. We believe that properly identifying risks and controls will provide the basis for sound management of IT resources and workable security plans.

It has become clear that federal HIPAA investigations hinge on the quality of the risk assessment for specific business processes and systems. It is therefore incumbent upon managers of Restricted Systems and applications to establish risk assessment processes. Guidance for HIPAA/HITECH Risk Analysis can be found at the following link; https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html

B. Policy

Johns Hopkins IT Policies require risk assessments:

SECURITY ADMINISTRATION OF RESTRICTED SERVERS AND APPLICATIONS

Risk assessment – Administrators of Restricted systems should conduct or solicit periodic (at least every three years) risk assessments regarding administrative, physical and technical vulnerabilities. Risk assessments should include inventories of interfaces, connectivity, vendor documentation and testing where appropriate. Risk assessments should be conducted in consultation with (internal or external) experts on security risk and in cooperation with technical and operational management. Documentation should include enumeration of security gaps and *updated remediation plans. In addition, administrators should work with operational management to determine whether use of private Restricted information is the minimum necessary to accomplish mission objectives.*

C. Audience

This Guidance is directed towards any systems administrator or data owner concerned with the security of their system with particular interest for systems considered at-risk or Restricted Systems hosting sensitive information.

D. Scope

This Guidance is for any system at Johns Hopkins where a risk assessment is an appropriate control. This approach is consistent with requirements in HIPAA, FERPA, GLBA, PCI/DSS, DFARS and the other primary legal and regulatory regimes.

E. Enforcement

Restricted systems are required by policy to have conducted risk assessments of *Johns Hopkins Information Technology Policies,* which are incorporated by reference.

IV. Risks

In general, JH considers IT security risk in several major categories, each of which require different, if not, overlapping controls. JH maintains several templates for conducting risk assessments, and most include an appendix enumerating common risks. These risks should not be considered exhaustive. Risk categories include:

- *Catastrophe* -- information security considers losses of integrity and availability. This is a good model for risk assessment and it goes well beyond security to things like power failures, failed upgrades and various systems interface issues. We seek to ensure that you prevent foreseeable problems and that systems fail gracefully rather than catastrophically. Much of this is considered in disaster recovery, but there are often a whole class of “component failure” or semi-catastrophes that can degrade your system without having to invoke a disaster recovery plan.

- *Hacked* – we should always consider what it means to be hacked. In the good old days, you could turn this problem over to your host or network administrators, but there are an increasing number of application layer hacks on the Internet, particularly those directed at Web applications.

- *Information leakage* – information may not be stolen, but it gets out. Lost media, laptops, desktops, back-up tapes, inadvertent publication on the Internet. Most of us in the risk assessment business spend too much time worrying about hackers and not enough time thinking about problems caused by mis-configuration or carelessness.

- *Insider threat access* -- this can take the form of shared passwords, allowing authorized and unauthorized users access to a system without creating an accurate audit trail. Authorized users abusing their access rights by viewing records of their friends and enemies. It can also arise from administrative access problems and problems regarding semi-insiders, such as vendors.

Information Systems risks should also be evaluated for compliance to current IT Standards and Policies. These policies are administered by the Institutional Computing Standards Committee (ICSC) and can be found at;
http://www.it.johnshopkins.edu/policies/standards.html
http://www.it.johnshopkins.edu/policies/

V. Departmental Risk Assessment Process

The National Institute of Standards and Technology (NIST) recommends an approach to risk assessment under the reference of SP 800-30 at the following link;
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf
Johns Hopkins follows this guidance in general form.

A. Identify Technology Assets

Technology assets, in the context of this process, are defined as any hardware, software, systems, services, and related technology assets that are important to a department/entity. These assets should be identified at an appropriate level of granularity (not too much detail, not too little) in a manner such that overlap among technology assets is minimized. In some cases it may be appropriate to combine assets (for example, all workstations for faculty, printers, etc.) while other situations may suggest specific assets (for example, special use server, It might also be appropriate to have some clear point of accountability (e.g. principal investigator, systems administrator).

B. Aggregate and Prioritize Assets

Risk assessment documentation may include criteria to be used to prioritize the list of technology assets as critical, essential, and normal. Candidate criteria include characteristics like criticality, impact, costs of a failure, publicity, legal and ethical issues, etc. It is not necessary to quantify these criteria, but administrators will need to consider criteria in aggregate and use judgment and experience to classify assets. The number of technology assets in any priority group is somewhat arbitrary but becomes unwieldy as asset numbers grow and become larger.

C. Identify Risks

A list of common risks is included in Appendix 2. One may select applicable risks from this common list, or identify risks that are specific to an application or business process. Risks must be tangible and specific with respect to one or more assets.

D. Prioritize Risks

Risks (both those selected from the Appendix 2 list and specific ones identified for the department) can then be prioritized. NOTE: It is not a requirement to prioritize the risks but doing so might provide the department/entity with an idea of where action(s) need to be planned. Priorities often make subsequent steps in the process more manageable if risks (which again include problems and threats) are so ordered. That is, items toward the top of the priority list should be those that have the potential to affect larger numbers of more heavily weighted assets.

E. Validate Identified Risk and Priorities

Application owners, departments and entities are generally in the best position to identify assets, evaluate criticality and identify risks. Effective risk assessments usually also include consultation and validation by experts in security and risk management. At JH such expertise is found generally:

- Office of the Chief Information Security Officer
- Office of Hopkins Internal Audits
- Third party consultants

While there are a large number of individuals with expertise in a specific area of security (e.g. networking, host, application), it is a good idea to utilize a generalist expert when reviewing risk assessments. Such experts will often call on specialists where needed.

F. Recommendations for Resolving Risks (Controls)

There are a number of ways to establishing risk controls:

- The risk (or risks) for an asset will be addressed within a specific timeframe, and a brief explanation should be included to identify concrete remediation steps.
- The risk (or risks) for an asset will be defined, but no plans for controls implemented should be identified because of special situations in the risk analysis (e.g. new software expected, moving to new location, etc.).
- Controls addressing the risk (or risks) for an asset will be or not implemented because of persistent factors (e.g. time, budget, etc.) and the risk is accepted.

If a risk will not be addressed in the short-term security plan, it should be documented and explained. Remediation plans and controls should be updated at least annually.

Additional Risk Assessment/Controls information can be found at https://www.cisecurity.org/controls/

VI. Documentation

Various forms and checklist used for Security Risk Assessments can be found at the following link on the IT@JH Portal
http://www.it.johnshopkins.edu/policies/risk.html

- *HIPAA RFP/Contracting Checklist* -- when buying a new system that stores, processes or transmits and JHM counsel is reviewing the contract, the vendor will likely be required to complete this document. The document serves as an inventory of security capabilities and designed for the evaluation of applications. If the product does not have one of the controls, it is a red flag, but does not necessarily mean that the system is, "out of compliance with HIPAA." On the other hand, passing this review does not mean that the system is even remotely secure. It is one thing to have a security capability, quite another to turn it on. (See our IT Vendor checklist for additional information.) http://www.it.johnshopkins.edu/policies/files/VendorChecklist12318.docx

These are all tools for risk assessment and may not be required in all cases. Additionally our risk management practices are evolving based on the threat landscape. If there are questions please send these to ITRisk@jhu.edu. This mailbox is monitored by the Information Security Office and should not be used as a replacement for reporting information security issues that are urgent in nature. These should continue to be reported to the IT@JH Help Desk.

VII. Frequency

Risk assessments should be conducted for IT infrastructure (e.g. server cluster, desktop support group, help desk) and specific applications that store, process or transmit Restricted information. Any new infrastructure or Restricted System requires a full risk assessment prior to implementation (this may not apply to proof of concept applications)

Full risk assessments on Restricted Systems should be conducted at least every three (3) years. Applications that require formal risk assessments under PCI-DSS must undergo recertification annually. Full or partial risk assessments should be conducted whenever there is a substantial change in System configuration or functionality.

Proposed remediation controls and security plans should be reviewed and updated annually.

VIII. Difficult Issues

Successful risk assessments require more than completing forms. They require the risk assessment team to address difficult issues that often cross department and staff boundaries. At Hopkins we have identified a number of areas that have proven particularly difficult and important for assessments. These are addressed in the forms, and should be emphasized in discussions.

Interfaces

It may be you know what your interfaces are, but you have no idea what happens to the information once it has been handed off. You should at least put it back on your interfaced party to document need-to-know and good security practices.

Logging

Every interaction with the system, even unsuccessful interactions with the system (like failed log-ins) should be logged somewhere. Sometimes this is done in the database, application or host. You need to be able to piece together an account of the who-what-when of user and administrator access. In addition, that means individuals access -- including vendors (see our IT

Logging Policy for additional information.)

http://www.it.johnshopkins.edu/restricted/standards/StandardLogManAPPROVED0612.pdf

Log Checking

It is not enough to log. Many of your logs should be checked regularly and anomalies investigated. Preferably, logs would be integrated into a tool such as Splunk managed by the Enterprise Monitoring team for comprehensive filtering and management.

Record Level Access Logging

For Restricted information, the logs must also tell us "User X, accessed Record Y at Time Z. Just recording that User X was on the system at Time Z is by itself good enough for major systems (it is probably as good as we can do for many small research systems.) Nor is it sufficient to merely log modifications at a user level. It is also a good idea for such logging to be normalized, and provide time signatures for the beginning and end of patient access to a specific patient record.

Effective log management practices are also required under HIPAA guidance.

User Authorization and Access Control Lists

How are master access control lists managed? How are users registered, trained and terminated? Most of this is out of the hands of IT. Even so, it may be the responsibility of the technical team to maintain the access control list. If so, is anyone reviewing it? Are detailed reviews of the accuracy of access control lists checked at least annually?

Vulnerability Management

Hosts must be configured to minimize vulnerabilities and that usually means active scans from centralized Tenable/NESSUS or a utility such as SMS/MOM or Altiris. Applications people generally have little idea what level of host security is being applied. Signature-based host monitoring should also be considered as a potential control.

Single Sign On

Most new applications support LDAP and SSO but they often claim that the best features in their security model are only available with native authentication. In this case, you can have a security trade-off between better security *in this application* and better security overall (due to reduction or stabilization in the number of passwords to be remembered by users). These types of tradeoffs are common in security, and it is important to document risk trade-offs.

Web application security

Developers and vendors should test the application for common Web development vulnerabilities. Many do not. Fortunately, we have the tools to test these internally, but we are still developing expertise in the training process. In addition, tools like Web application firewalls and proxy blockers are useful for ongoing security. Security plans should therefore state medium term objectives for Web application testing -- even for applications that we do not control. (See *Standards and Guidance on Web Application Standards link*) http://www.it.johnshopkins.edu/restricted/standards/WebAppSecurityTableAPPROVED071015.docx

Inventories

You should have an inventory of applications, servers and devices that is as complete as possible. Moreover, you should have a process for reviewing and updating inventories in each of these areas. It is best if the latter is automated. For now, you should undertake some sort of manual review of users and sites in order to identify machines that have not been inventoried.

Encryption

The first objective in encryption is to ensure that information potentially stored on mobile devices is encrypted. The best way to ensure that is to limit storage on local devices, unless you also manage all of those devices and can install encryption (e.g. Bitlocker/FileVault). The next big challenge is to ensure that all transmissions external to the Hopkins network are encrypted. We also encourage that encryption take place inside the network where possible. In the next few years, you will be expected to encrypt instances (e.g. caches, database columns) of particularly sensitive or at-risk information. You should identify these in the risk assessment also.

Problems with encryption are often related to the inventory question and are a matter of queuing devices and ensuring that key management is handled correctly. For transmissions, the issue is muddied somewhat by the security capabilities of our interlocutors. Again, this is an issue of setting up a schedule and benchmarks for encryption in the documentation. (See Standards and Guidance)
http://www.it.johnshopkins.edu/restricted/standards/EncryptedStandardsRevisedAPPROVED030116.pdf

Report Writing

It takes a while to understand what a serious vulnerability report writing is for many of our more sophisticated applications. Reports often take large amounts of Restricted information out of relatively secure environments and move them to less secure environments, such as spreadsheets, locally managed MS Access databases, etc.. To manage reports properly, you almost need a secondary access control system, but that is often onerous. The next best approach is severely limit the number of individuals who can write custom reports and provide some sort of report logging (even though that will not tell us specifically which reports are being written.

Administrator Access

Do you have a method for updating administrator access control lists? What about remote access of administrators? Are accounts individuated and are you using tools such as RADIUS servers? How are database and applications administrators handled differently than host administrators? Are administrative authentication credentials strong? Is multi-factor authentication appropriate? Are there “break glass” procedures for emergency access?

Vendor Access

Many departments have sensible policies for their administrative and user staff, yet allow third parties access with fewer controls than for Hopkins personnel. This incongruity often results from how vendors normally support their systems. Because of the size and diversity of our system and application environment, risks of exposure that are manageable for a smaller hospital are more problematic here. It is therefore critical to document processes for ensuring that all vendor staff that access Hopkins assets are authorized and tracked as individuals and not through generic user accounts. Change control procedures that require vendors to provide prior notice and document systems changes benefit operations and security. It is also important that the principal of minimum necessary be observed – it may not, for example, be necessary for an application support team to have administrative rights on a server.

Testing, Penetration Testing and Audits

For large applications and infrastructures, there should be some approach to testing beyond, “when it breaks, we know it has been tested.” Penetration testing is a valuable tool but should be coordinated with network security, host administrators. In general, we recommend that “pen testing” be managed by the CISO to ensure that reasonable objectives and methods are put in place.

IX. References

- Johns Hopkins Risk Assessment Guidance - http://www.it.johnshopkins.edu/policies/risk.html
- Consensus Audit Guidelines -- http://www.sans.org/critical-security-controls/
- NIST 800 Special Publications (800-30, 800-53, 800-66) -- http://csrc.nist.gov/publications/PubsSPs.html
- PCI/DSS Self Assessment -- https://www.pcisecuritystandards.org/saq/index.shtml

X. Appendices

Appendix 1 – Principal Risk Factors

Appendix 2 – Summary Risk Assessment Form

Appendix 1 – Principal Risk Factors

Departmental systems face many of the same threats as major systems. However, usually the system is smaller and risks less immediate. Authorization can be simpler with these types of systems, and usually requires more input from departmental administration.

Threat	Description	Risk	Controls
System penetration	Attack of the bots and other malicious code. Automated scanning tools are used to scan for and exploit vulnerabilities. This is especially a problem for Unix/Linux machines. Machine are compromised with rootkits, add'l accounts and warez code.	Very High	1. Prompt patching and security updates reduces risk dramatically 2. Disabling unnecessary services and ports 3. NESSSUS scanning through Tenable. 4. Host firewalling – IP Tables 5. Private space host addressing
Disaster Recovery and Contingency Planning	Disaster recovery is important, prone to audit, and straightforward to address. The main issue is the existence of a plan. Departmental systems should be part of a JH DR plan, interfaces and inter-dependencies assessed.	Very High	1. Documented and tested DR/BCP plan 2. DR/BCP representative 3. Recovery objectives are established 4. Back-up plans are integrated 5. Plans for component failures 6. Plans for notifying users
Unauthorized use -- authorization	Authorization not authentication is usually the culprit here. It is often difficult to keep up with the number of users. Using RACF/JHED/AD and a number of tools for terminating users, but it is critical that business management be involved.	High	1. RACF authorization processes 2. JHED services with regular communications for systems of record 3. Quarterly audit of access control lists for unneeded accounts
Environmental hazards	Departmental systems should be in a data center.	High	1. Standard Hopkins data center controls 2. Work with data center owners in limiting the number of those authorized for physical entry
Data Leakage – Physical Devices or Media	Lost or stolen media can be a problem even if information is protected. Document physical security controls and encrypt information when leaving the site	High	1. Standard Hopkins data center controls 2. Physically secure media and devices (e.g. back-ups) 3. Encrypt media for transport 4. Contractual provisions for off-site storage and transport
Unauthorized use -- authentication	Good (compliant) user password policies are hard to maintain. JHED/AD/Siteminder should be used whenever possible.	Medium	1. Allow very long pass phrases (e.g. 15 or more characters) 2. System forces good passwords 3. Authentication halted after 5-12 unsuccessful attempts 4. Credentials should be encrypted in transit 5. JHED enforces all of these and should be used where possible
Data Interception	Switched networks reduce risk here for internal communications. External communications could be intercepted en masse.	Medium	1. Deploy secure ftp or https solutions 2. Further protect data by using blind puts or watching progress
Unauthorized administrative access	Insider attacks are often associated with poor administrative access practices (e.g. too many accounts, out of data access). This is a common point of contention audits, yet usually relatively easy to control, through sound policy and fundamental security tools	Medium	1. Require encrypted channel (e.g. SSH) and user authentication 2. No shared administrative accounts 3. Use pass phrases 4. Audit accounts using Tripwire, MOM or e-Trust 5. Process for providing emergency access. 6. Separation of duties between app administrators and DBA's

Appendix 2 – Summary Risk Assessment Form

Johns Hopkins Health System

JOHNS HOPKINS
MEDICINE
JOHNS HOPKINS
HEALTH SYSTEM

- ## APPLICATION RISK ASSESSMENT

- ### Overview

This document is a one-time assessment of information security risk for specific system/application or entity associated with Johns Hopkins.

Date: (date of risk assessment completion)

Application Name:

Technical Support Contact:	
Johns Hopkins Application Owner:	
Date of Completion for Security Review:	
Survey Completed by:	

- ### Brief Description: (Provide a brief description of the environment & functionality of the system)

Risks Identification: (identify information security risks associated with this application)

-
-
-
-
-
-
-
-

Risk Controls

Standards documents have been generated by the Institutional Computing Standards Committee (ICSC), and can be found: http://www.it.johnshopkins.edu/policies/standards.html

Information Technology Policies:

http://www.it.johnshopkins.edu/policies/itpolicies.html

Applications specific controls

-
-
-

Enterprise Controls

Access Control	Current Status
Is user access controlled through the Johns Hopkins domain login ID (Active Directory)?	Yes:☐ No: ☐
Does the application have a more granular role base access options for different data access abilities?	Yes:☐ No: ☐
Is there a documented process for adding and removing individuals from authorized access?	Yes:☐ No☐
Is user activity (e.g. data insertions, revisions or deletions) logged and stored? (http://www.it.johnshopkins.edu/policies/standards.html)	Yes:☐ No: ☐
Is Multi-Factor Authorization (MFA) used for accounts with access to sensitive information (i.e. Systems Administrators or DBA)?	Yes:☐ No: ☐

Application Security	Current Status
Does the application send or display information over encrypted channels?	Yes:☐ No: ☐
Is database or field level encryption, or masking, possible for the application?	Yes:☐ No: ☐
Are all transmission of user credentials (i.e. internal or external) encrypted? (Note: SSL log-ins and Siteminder automatically encrypt)	Yes:☐ No: ☐
Does the application allow for file transfers?	Yes:☐ No: ☐
Does the system avoid insecure user interfaces such as automatic faxes, e-mails or messaging of Restricted information?	Yes:☐ No: ☐
Are report writing tools and procedures in place to ensure that minimum necessary information is used for reports? (*Draft Web Application Standards*)	Yes:☐ No: ☐
Are ad hoc reports of Restricted information prohibited or otherwise monitored by application owners? (*Draft Web Application Standards*)	Yes:☐ No: ☐
Does the Web interfaces restrict to Hopkins IP space and/or use ROBOT.TXT or equivalent to prevent search engines from indexing Restricted information? (*Draft Web Application Standards*)	Yes:☐ No: ☐
Has the application (especially Web applications) undergone any security testing for commonly exploited vulnerabilities (e.g. SQL Injection, buffer overflow)? (*Draft Web Application Standards*)	Yes:☐ No: ☐
Has the application had any security scan (Nessus/ Acunetix) scan completed?	Yes:☐ No: ☐
Are there Flash/Java type dependencies, and what versions, are there plugins, or mix-ins?	Yes:☐ No: ☐
Does the application automatically log-out after a period of user inactivity? (*HIPAA Technical Security Policies*)	Yes:☐ No: ☐
Does the application store any data (credentials) on the client, especially mobile?	Yes:☐ No: ☐
Does the application owner maintain a list and communicate with systems administrators known application vulnerabilities?	Yes:☐ No: ☐

Are there procedures (and individuals identified) in place for systems or applications administrators to respond to incidents in a timely manner – incident@jhu.edu?	Yes:☐ No: ☐
Does the application produce logs that can be reviewed for admin or user activities down to the screen level of the application? http://www.it.johnshopkins.edu/restricted/standards/StandardLogManAPPROVED0612.pdf	Yes:☐ No: ☐
Are there processes or tools in place to monitor database activities and or check for data leakage?	Yes:☐ No: ☐

Quantify Risk

Likelihood of Risk: (score 1-5 based on the following table)

Level	Likelihood	Expected or actual frequency experienced
1	Rare	May only occur in exceptional circumstances; simple process; no previous incidence of non-compliance
2	Unlikely	Could occur at some time; less than 25% chance of occurring; non-complex process &/or existence of checks and balances
3	Possible	Might occur at some time; 25 – 50% chance of occurring; previous audits/reports indicate non-compliance; complex process with extensive checks & balances; impacting factors outside control of organisation
4	Likely	Will probably occur in most circumstances; 50-75% chance of occurring; complex process with some checks & balances; impacting factors outside control of organisation
5	Almost certain	Can be expected to occur in most circumstances; more than 75% chance of occurring; complex process with minimal checks & balances; impacting factors outside control of organisation

Consequence: (score 1-5 based on the following table)

Level & descriptor	Health Impacts	Critical services interruption	Organizational outcomes/ objectives	Reputation and image per issue	Non-compliance
Insignificant (1)	First aid or equivalent only	No material disruption	Little impact	Non-headline exposure, not at fault; no impact	Innocent procedural breach; evidence of good faith; little impact
Minor (2)	Routine medical attention required (up to 2 wks incapacity)	Short term temporary suspension – backlog cleared < 1 day	Inconvenient delays	Non-headline exposure, clear fault settled quickly; negligible impact	Breach; objection/complaint lodged; minor harm with investigation
Moderate (3)	Increased level medical attention (2 wks to 3	Medium term temporary suspension – backlog cleared by	Material delays; marginal under-achievement of target performance	Repeated non-headline exposure; slow resolution;	Negligent breach; lack of good faith evident; performance review initiated

	mths incapacity)	additional resources		Ministerial enquiry/briefing	
Major (4)	Severe health crisis (incapacity beyond 3 mths)	Prolonged suspension of work – additional resources required; performance affected	Significant delays; performance significantly under target	Headline profile; repeated exposure; at fault or unresolved complexities; ministerial involvement	Deliberate breach or gross negligence; formal investigation; disciplinary action; ministerial involvement
Catastrophic (5)	Multiple severe health crises/injury or death	Indeterminate prolonged suspension of work; non performance	Non achievement of objective/ outcome; performance failure	Maximum high level headline exposure; Ministerial censure; loss of credibility	Serious, wilful breach; criminal negligence or act; prosecution; dismissal; ministerial censure

Results Risk Matrix: (score the following table based on prior table scores)

	CONSEQUENCE				
LIKELIHOOD	Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Extreme (5)
Rare (1)	Low	Low	Low	Low	Low
Unlikely (2)	Low	Low	Low	Medium	Medium
Possible (3)	Low	Low	Medium	Medium	Medium
Likely (4)	Low	Medium	Medium	High	High
Almost certain (5)	Low	Medium	Medium	High	Extreme

- **Remediation/Mitigation Strategy** (identify steps to reduce eliminate risks)

1.
2.
3.
4.
5.
6.
7.
8.

• Approval

• Additional comments