



Practical Information Security Risk Management

Understanding the Big Picture to Focus on the Right Priorities

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213



Document Markings

Copyright 2023 Carnegie Mellon University.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

Carnegie Mellon® and CERT® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM23-0062

Agenda

Introductions

Risk Primer

Risk Context

Governance & Compliance

Putting it all Together

In-Class Discussion: What is your current risk evaluation process?

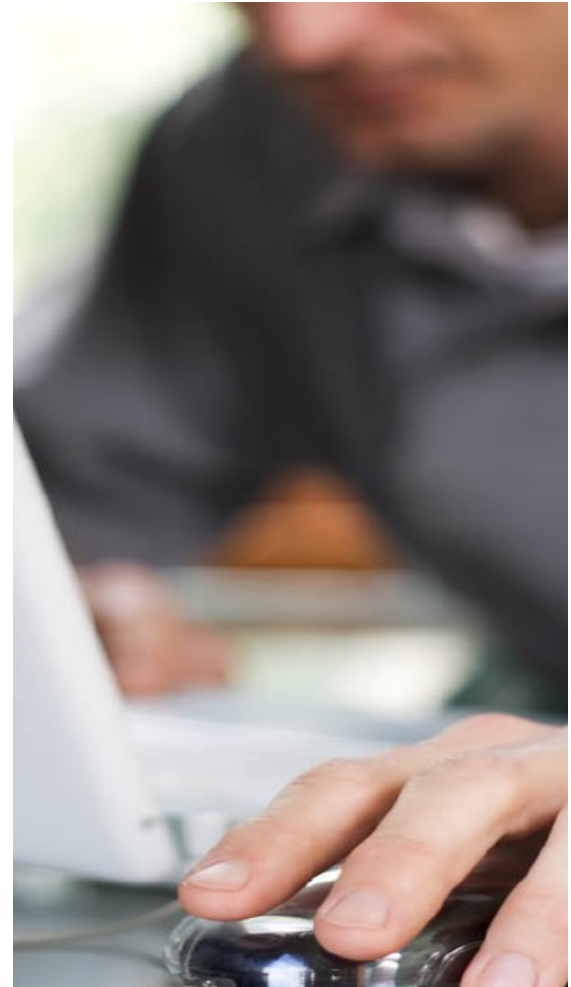


What is your current risk evaluation process?

- ***Is it consistent and repeatable?***
- ***What information do you need to evaluate risk?***

Practical Information Security Risk Management

Risk Primer



Why is Understanding Risk Important?



Knowing what and where your risks are help you decide where to spend your time and money.



A successful protection strategy is based on a solid understanding of risk and a comprehensive risk management program.



Critical decisions should not be based on best guess, or uninformed, generic external factors.



Not understanding risk may lead to errors in allocating protection mechanism and lead to exposures that might have been prevented.

Risk Equation

Risk is the result of a *threat* successfully exploiting a *vulnerability* and causing an *impact* on an *asset*.



Risk Equation

Risk = (Threat x Vulnerability)* x Impact

All three must exist for there to be a risk.

**(threat x vulnerability) represents the likelihood or probability that "bad things" might happen.*

Risk Analysis Example 1

Scenario

- This is your car
- It is parked on the street in front of your home.
- Car thefts in the area are at an all time high.
- Vandalism is also very common.

Is there a risk here?

- What threats should you consider?
- What mitigating factors can be applied?
- How do you determine impact?



Risk Analysis Example 2



Scenario

- This is your car
- It is parked on the street in front of your home.
- Car thefts in the area are at an all time high.
- Vandalism is also very common.

Is there a risk here?

- What changes in your evaluation of risk?
- Did the threats or vulnerabilities change?
- How do you determine impact?

In-Class Discussion: What has higher risk?



Is the risk higher for the older car or the new car?

- ***Why is that one higher risk? What factors did you consider?***
- ***What additional information do you need?***

Risk Analysis Example 3

You have a database of **personal consumer information**

- It has failed twice in the last year.
- There is no redundancy and the last back up was four months ago.
- The administrators do not want to patch in case it causes another failure – (no patches for 4 years).
- The database vendor has announced the fifth security vulnerability for the production version.

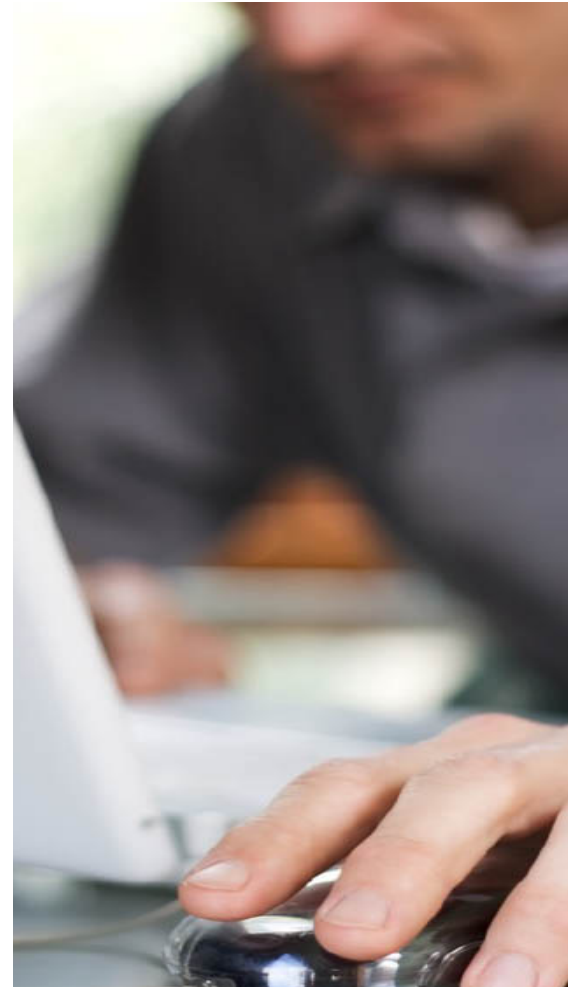
Is there a risk here?

- How much should be spent to address this?
- What other information is necessary?



Practical Information Security Risk Management

Risk Context



Risk is Defined by the Surrounding Context



Identifying Risk



Keys to determining risk level



Impact (or consequences)




- What type of data does the asset contain?
- How much of that type of information?
- Where is that information located (region of the world)?




Likelihood (or probability)

- Is there an existing, viable threat?
- Is the asset vulnerable to that threat?


Evaluating Risk Level

-  Both impact and likelihood can be ranked based on levels of significance.
-  Each organization may have different opinions on these levels.
-  Documenting the levels and criteria for each is essential.



Impact varies due to

- Financial costs
- Regulatory impacts
- Effects on reputation
- Volume of data exposed



Likelihood is determined by

- Threats present
- Vulnerabilities present

Common Impact Levels	
Critical	
Major	
Moderate	
Minor	
Insignificant	

Common Likelihood Levels	
Almost Certain	
Likely	
Possible	
Unlikely	
Rare	

Plotting Risk Level

- Each risk can be plotted according to its likelihood and impact
- Plotting risks on the same chart shows their relative importance
- Higher risks can be targeted for mitigation
- Monitoring risks over time can improve risk posture

Examples	Likelihood	Impact
A	Possible	Major
B	Unlikely	Moderate
C	Rare	Catastrophic

LIKELIHOOD	5	Almost Certain	Medium	Medium	High	Extreme	Extreme
	4	Likely	Low	Medium	High	High	Extreme
	3	Possible	Low	Medium	Medium	High A	High
	2	Unlikely	Low	Low	Medium B	Medium	Medium
	1	Rare	Low	Low	Low	Medium	Medium C
				Insignificant	Minor	Moderate	Major
			1	2	3	4	5
IMPACT							

Risk Analysis Revisited

- Has your risk ranking changed?
- What would mitigate current risk?

LIKELIHOOD	5	Almost Certain	Medium	Medium	High	Extreme	Extreme
	4	Likely	Low	Medium	High	High	Extreme
	3	Possible	Low	Medium	Medium	High	High
	2	Unlikely	Low	Low	Medium	Medium	Medium
	1	Rare	Low	Low	Low	Medium	Medium
				Insignificant	Minor	Moderate	Major
			1	2	3	4	5
			IMPACT				



Reducing Risk

Risk can be reduced by reducing or eliminating

- **Threats**

- Improving detection
- Situational awareness

- **Vulnerabilities**

- Patching
- Managing access

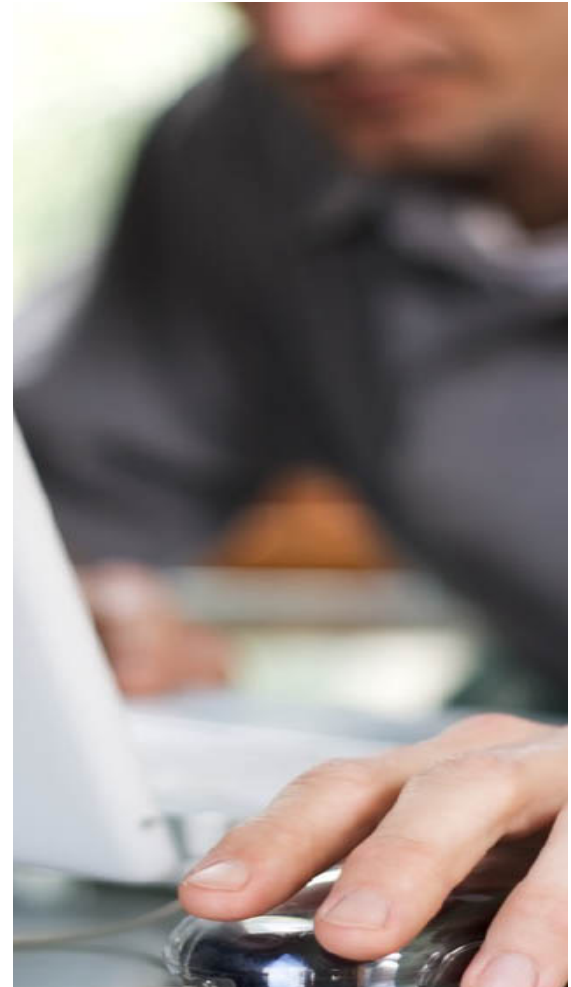
- **Impact**

- Reducing data volume stored
- Eliminating unneeded sensitive information



Practical Information Security Risk Management

How Risk fits with Governance & Compliance



Setting the Context

Security Governance

- The means by which *you* control and direct *your* organisation's approach to security. When done well, security governance will effectively coordinate the security activities of your organisation. It enables the flow of security information and decisions around your organisation.
- Just as security is the responsibility of everyone within an organisation, security decision making can happen at *all levels*. To achieve this, an organisation's senior leadership should **use security governance** to set out the kinds of **security risks** they are prepared for staff to take, and those they are not.

- UK's National Cyber Security Centre

Risk Management

- Uses the governance building blocks and management's stated risk appetite to build a picture of the organization's risk posture and inventory of risks. Continuous management of risks helps inform management's view of risk appetite. Risk management also provides insight on what is working well and what is not so that management knows where they might take more business risk to grow the business.

Compliance

- Meeting all of the requirements applicable to the organization and being able to provide evidence. Requirements may come from many sources. The organization is responsible for knowing where to look for applicable requirements and how to apply protections to ensure requirements are addressed sufficiently.

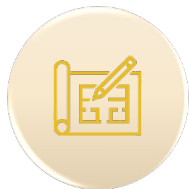
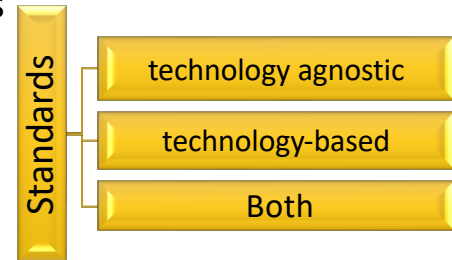
Governance



Policies - define high-level requirements also known as **controls**



Standards – provide instruction for implementing requirements



Guidelines – provide additional best practices or considerations



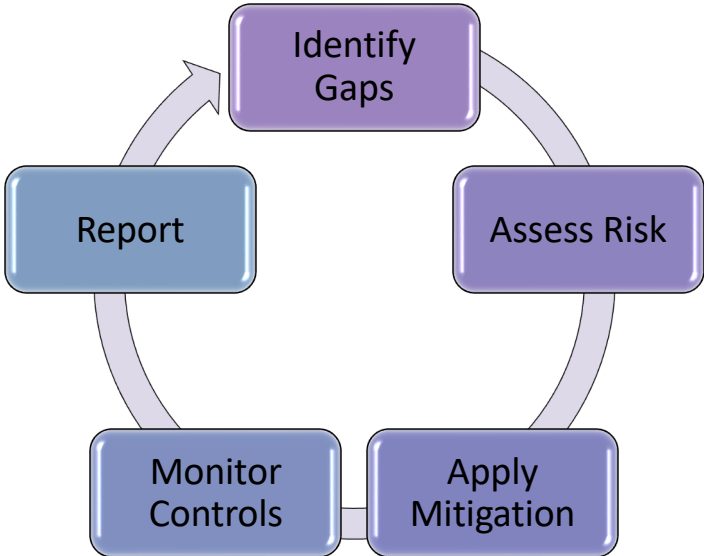
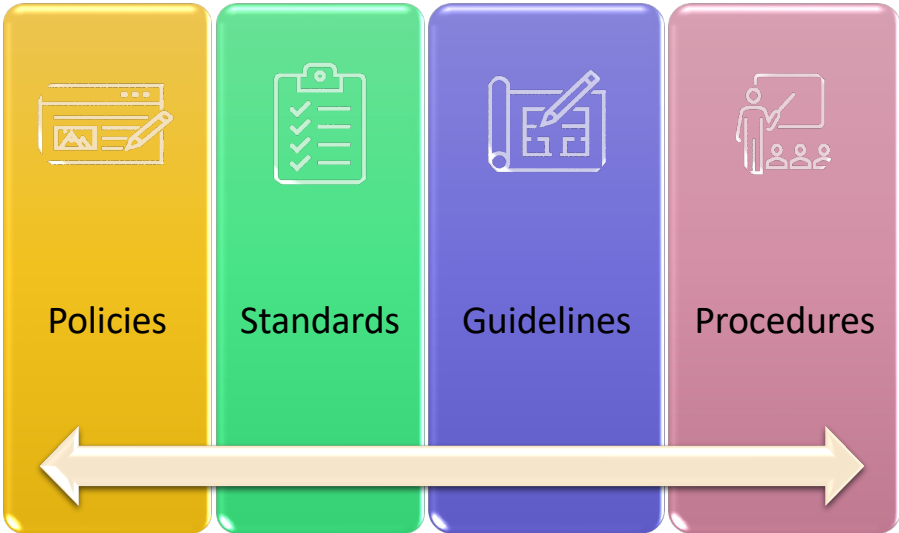
Procedures – hands-on, how to for implementing standards

Policies & Standards may come from external sources. Internally developed policies & standards are also very important.

Governance & Risk

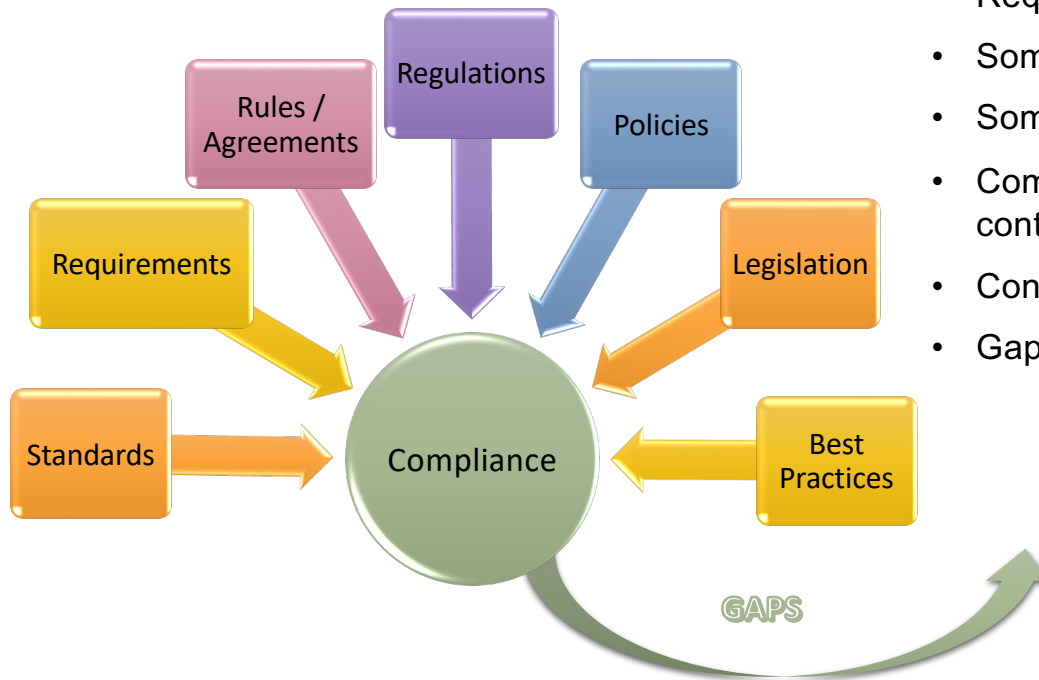
Security Governance
develops and manages

Risk Management
has a continuous cycle



Controls  Processes

Compliance



- Requirements come from many sources
- Some are mandatory
- Some are self-imposed
- Compliance assessments help determine what controls are effectively in place
- Controls that are not operating well reveal gaps
- Gaps must be assessed for risk

Example Control Inventory

Control ID	Control Name	Control	Discussion	Related Controls
AC-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]	Access control policy and procedures address the controls in the AC family that are implemented within systems and organizations.	IA-1, PM-9, PM-24, PS-8, SI-12.
AC-3	Access Enforcement	Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	Access control policies control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (i.e., devices, files, records, domains) in organizational systems.	AC-2, AC-4, AC-20, AC-21, AC-22,, IA-2, IA-5, IA-6, IA-11, MA-5, MP-4, PM-2, SC-12, SC-13, SC-28, SC-31, SI-4, SI-8.
AC-6	Least Privilege	Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.	Organizations employ least privilege for specific duties and systems. The principle of least privilege is also applied to system processes, ensuring that the processes have access to systems and operate at privilege levels no higher than necessary to accomplish organizational missions or business functions.	AC-2, AC-3, AC-5, AC-16, CM-5, CM-11, PL-2, PM-12, SA-8, SA-15, SA-17, SC-38.
AT-2	Literacy Training and Awareness	a. Provide security and privacy literacy training to system users (including managers, senior executives, and contractors):	Organizations provide basic and advanced levels of literacy training to system users, including measures to test the knowledge level of users.	AC-3, AC-17, AC-22, AT-3, AT-4, CP-3, IA-4, IR-2, IR-7, IR-9, PL-4, PM-13, PM-21, PS-7, PT-2, SA-8, SA-16.
AU-2	Event Logging	a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging];	An event is an observable occurrence in a system. The types of events that require logging are those events that are significant and relevant to the security of systems and the privacy of individuals.	AC-2, AC-3, AC-6, AC-7, AC-8, AC-16, AC-17, AU-3, SI-3, SI-4, SI-7, SI-10, SI-11.

<https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/downloads> - 1189 controls listed

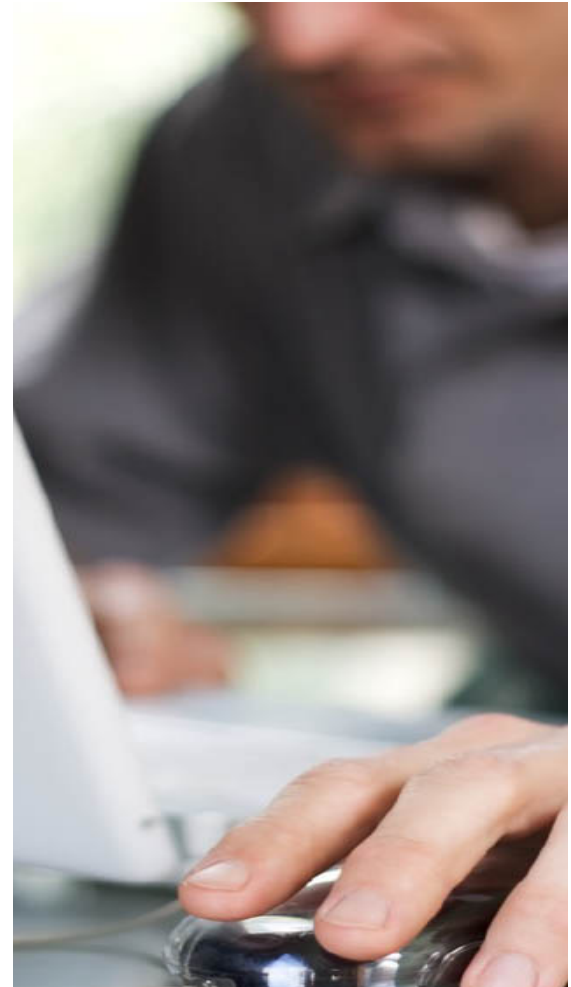
GOVERNANCE EXAMPLE

User registration and de-registration

Policy	Standard	Tech Standard	Guideline	Procedure
<ul style="list-style-type: none">• Unique user IDs assigned• Periodic review• Disable IDs upon departure	<ul style="list-style-type: none">• ID pattern<ul style="list-style-type: none">• First letter of first name• First 7 letters of last name• If redundant replace last letter with number• Example<ul style="list-style-type: none">• Sjohnson• Smudd123• IDs reviewed annually for redundancy and active use• Disable upon resignation	<ul style="list-style-type: none">• Windows Active Directory Standard<ul style="list-style-type: none">• UserID specific settings• Linux Standard<ul style="list-style-type: none">• UserID specific settings• MacOS Standard<ul style="list-style-type: none">• UserID specific settings	<ul style="list-style-type: none">• User ID management may be centralized in a single LDAP for ease of management• Windows AD can act as an LDAP for MacOS and Linux systems• Systems used for testing should be kept off the production user network and use separate user database	<ul style="list-style-type: none">• Configure Windows AD user settings<ul style="list-style-type: none">• ~~~• Configure MacOS user settings<ul style="list-style-type: none">• ~~~• Configure Linux user settings<ul style="list-style-type: none">• ~~~• Annual Review Steps<ul style="list-style-type: none">• ~~~• Disable user

Practical Information Security Risk Management

Putting it All Together



Critical Elements for Determining Impact

Data Classification

- 1-Public
- 2-Internal Only
- 3-Confidential
- 4-Restricted

Asset Inventory

- People
- Technology
- Information
- Facilities

Business Criticality

- 1-Business Critical
- 2-Severe Impact
- 3-Divisional Impact
- 4-Minimal Impact

Example Impact Guidance

Impact Rank	Description	Operational Impact Downtime	Operational Impact Incidents	Operational Impact Scale	Financial Impact by annual revenue	Reputational Impact	Data Exposure by type	Data Exposure by volume
1	Insignificant	0-4 hours	Minimal business criticality, minor site/service degradation	<2% users affected	<2%	Local City Customers / Consumers / Partners	Public Internal Only	<50 Records
2	Minor	4-8 hours	Minimal business criticality, increasing site/service degraded	2-4% users affected	2-4%	Regional Customers / Consumers / Partners	Internal Only	50-250 Records
3	Moderate	8-24 hours	Divisional Impact or business critical system, significant site/service degradation or local outages	5-15% users affected	5-15%	In-Country Customers / Consumers / Partners	Internal Only Confidential	250-750 Records
4	Major	1-3 days	Severe Impact to business-critical system, site/service availability questionable	16-20% users affected	16-20%	Global Consumers / Partners	Confidential	750-1000 Records
5	Critical	>3 days	Business critical Impact, Critical systems, site, service unavailable	20% users affected	20%	Global Customers	Restricted	>1000 Records

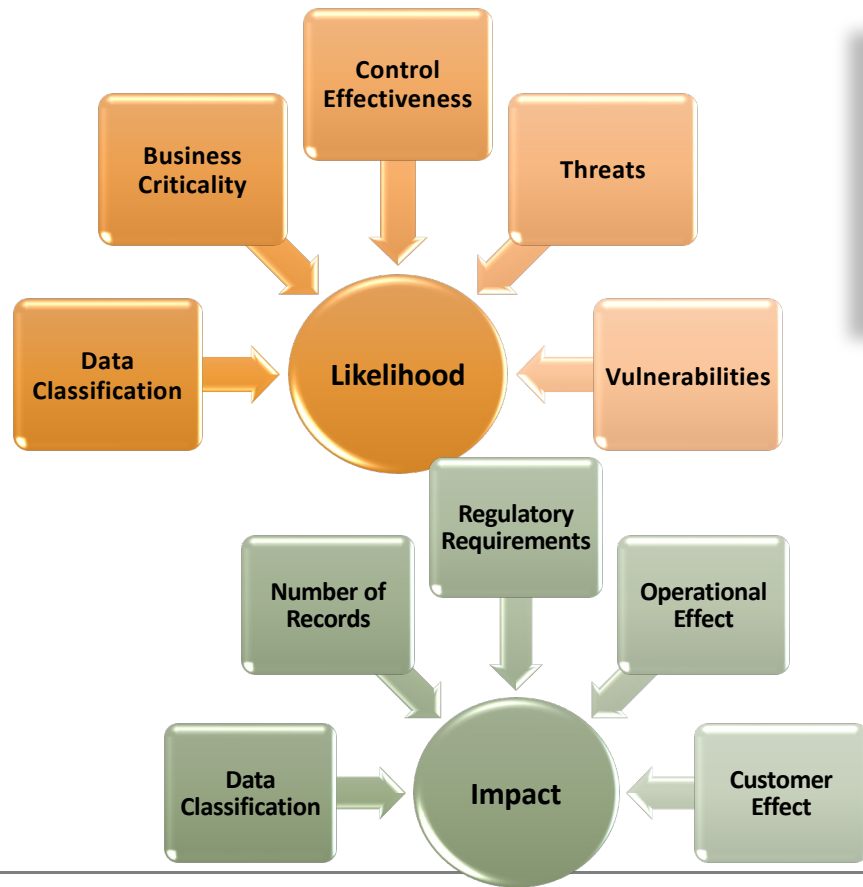
Controls are less effective for altering Impact

Example Likelihood Guidance

Impact Rank	Description	Inherent Probability	Previous Control Prevention	Frequency of Occurrence	Control Effectiveness	Threat Environment
1	Rare	Has not occurred and most likely will not occur	Very Effective	>1 per 5 years	No identified improvements needed	Minor or no current threats
2	Unlikely	Not likely to occur	Effective	1-3 per year	Minor improvements needed	Threats exist but no reported concerns
3	Possible	Likely to occur periodically	Moderate	1 per month	Obvious improvements needed	Reported concerns for potential occurrences
4	Likely	Highly likely to occur in given risk posture	Ineffective	Weekly	Significant improvements needed	Ongoing occurrences in industry peers
5	Almost Certain	Expected to occur in given risk posture or may be presently occurring	Non-Existent / Highly Ineffective	Daily	Critical improvements needed	Ongoing major occurrences

Controls are most effective in altering Likelihood

Putting it All Together



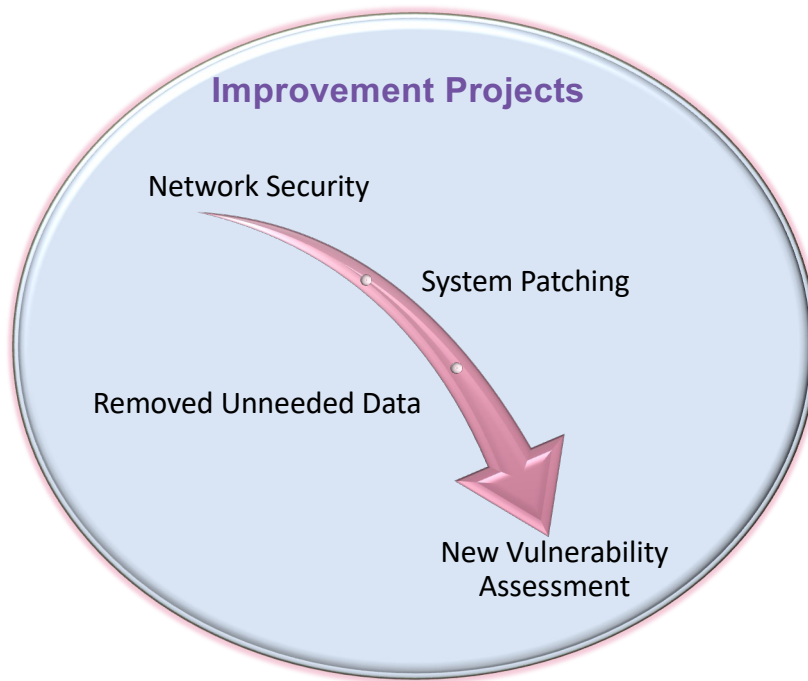
LIKELIHOOD	5	Almost Certain	Medium	Medium	High	Extreme	Extreme
	4	Likely	Low	Medium	High	High	Extreme
	3	Possible	Low	Medium	Medium	High	High
	2	Unlikely	Low	Low	Medium	Medium	Medium
	1	Rare	Low	Low	Low	Medium	Medium
			Insignificant	Minor	Moderate	Major	Catastrophic
		1	2	3	4	5	
IMPACT							

Asset Inventory – Risk

ID	Asset	Scope	Criticality	Classification	Likelihood	Impact	Risk Level
1	Email Services	Org-Wide	2-Severe Impact	2-Internal Only	3-Possible	4-Major	High ¹
2	Customer Portal	Cust Svc / Externally facing	3-Divisional Impact	3-Confidential	3-Possible	3-Moderate	Medium ²
3	Corporate Web Server	IT Web Svc / Externally Facing	4-Minimal	1-Public	4-Likely	3-Moderate	High ³

LIKELIHOOD	5	Almost Certain	Medium	Medium	High	Extreme	Extreme
	4	Likely	Low	Medium	High	High	Extreme
	3	Possible	Low	Medium	Medium	High	High
	2	Unlikely	Low	Low	Medium	Medium	Medium
	1	Rare	Low	Low	Low	Medium	Medium
			Insignificant	Minor	Moderate	Major	Catastrophic
		1	2	3	4	5	
IMPACT							

Risk Treatment & Trending



ID	Asset	Likelihood	Impact	Initial	6m Check	Trend
1	Email Services	3-Possible 2-Unlikely	4-Major 3-Moderate	High	Medium	↓
2	Customer Portal	3-Possible 2-Unlikely	3-Moderate	Medium	Medium	→
3	Corporate Web Server	4-Likely 3-Possible	3-Moderate 2-Minor	High	Medium	↓

LIKELIHOOD	5	4	3	2	1
	Almost Certain	Medium	Medium	High	Extreme
Likely	Low	Medium	High	High	Extreme
Possible	Low	Medium	Medium	High	High
Unlikely	Low	Low	Medium	Medium	Medium
Rare	Low	Low	Low	Medium	Medium
	Insignificant	Minor	Moderate	Major	Catastrophic
	1	2	3	4	5
	IMPACT				

Questions?



If You Want to Know More

- NIST guidance on prioritizing systems - <https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8179.pdf>
- NIST Cyber Risk Management Framework - <https://www.nist.gov/cyberframework/risk-management-framework>
- UK National Cyber Security Centre - <https://www.ncsc.gov.uk/section/advice-guidance/all-topics?allTopics=true&topics=risk%20management&sort=date%2Bdesc>
- Secure Controls Framework - <https://www.securecontrolsframework.com/>