New York Metro Joint Cybersecurity Conference

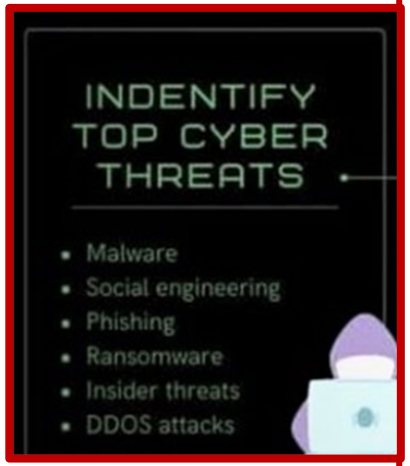
Enterprise Risk Management Strategy

Business Objectives supported by the Cybersecurity Program

Kathy Braun

ORGANIZE A STRATEGY

The logic for search and seizure is that if the source of the evidence is illegal, so is the evidence that came from the source. Following, if any part of the network access chain is compromised, all other points of the chain are compromised.

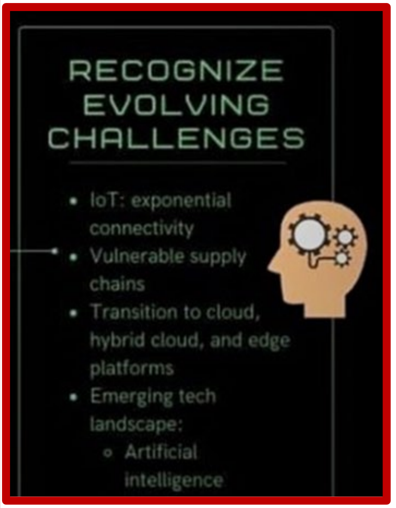


INDENTIFY TOP CYBER THREATS

- Malware
- Social engineering
- Phishing
- Ransomware
- Insider threats
- DDOS attacks

Under the umbrella of Cybersecurity ERM aligning with Zero Trust, how do you get buy in from the business areas?

- ➢ Speak to the business SME(s) about their objectives to confirm your understanding.
- ➢ Demonstrate through risk scenarios how the business processes aligned with the asset always have a potential to create risk - real-world threats and vulnerabilities.
- ➢ Next align security with protecting brand and potential monetary impact.
- ➢ Finally, include the subjective aspects of the organization - culture and skill sets to discern the degree of effort required to reap the expected benefits.
- ➢ Record in a Risk Register



RECOGNIZE EVOLVING CHALLENGES

- IoT: exponential connectivity
- Vulnerable supply chains
- Transition to cloud, hybrid cloud, and edge platforms
- Emerging tech landscape:
  - Artificial intelligence

Risk Management Maturity – Cybersecurity Baked into the Business

Compliance
Point in Time Analysis

Not Strategic In Nature

Policies and IT Operations do not handle "Exceptions" well to address the changing Threat Landscape

- ✓ Acquiring New Companies
- ✓ Introducing New Technology
- ✓ New or changing Applications
- ✓ Cloud Technologies
- ✓ New or changing Business Process

Versus

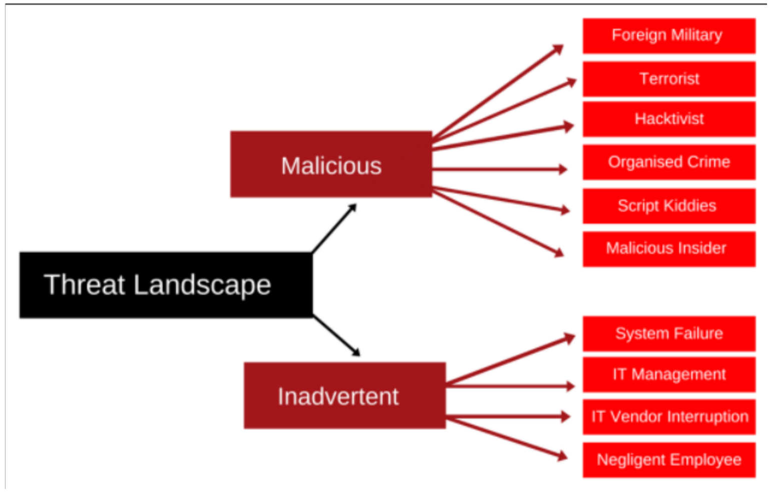
Business treated as Cybersecurity driven not limited to an IT Responsibility

Security goals baked into Business Requirements to protect the confidentiality of data, preserve the integrity of data, promote the availability of data for authorized users?

Cybersecurity
Real Time Analysis

Understand the changing Threat Landscape

Continuous Monitoring & Analysis



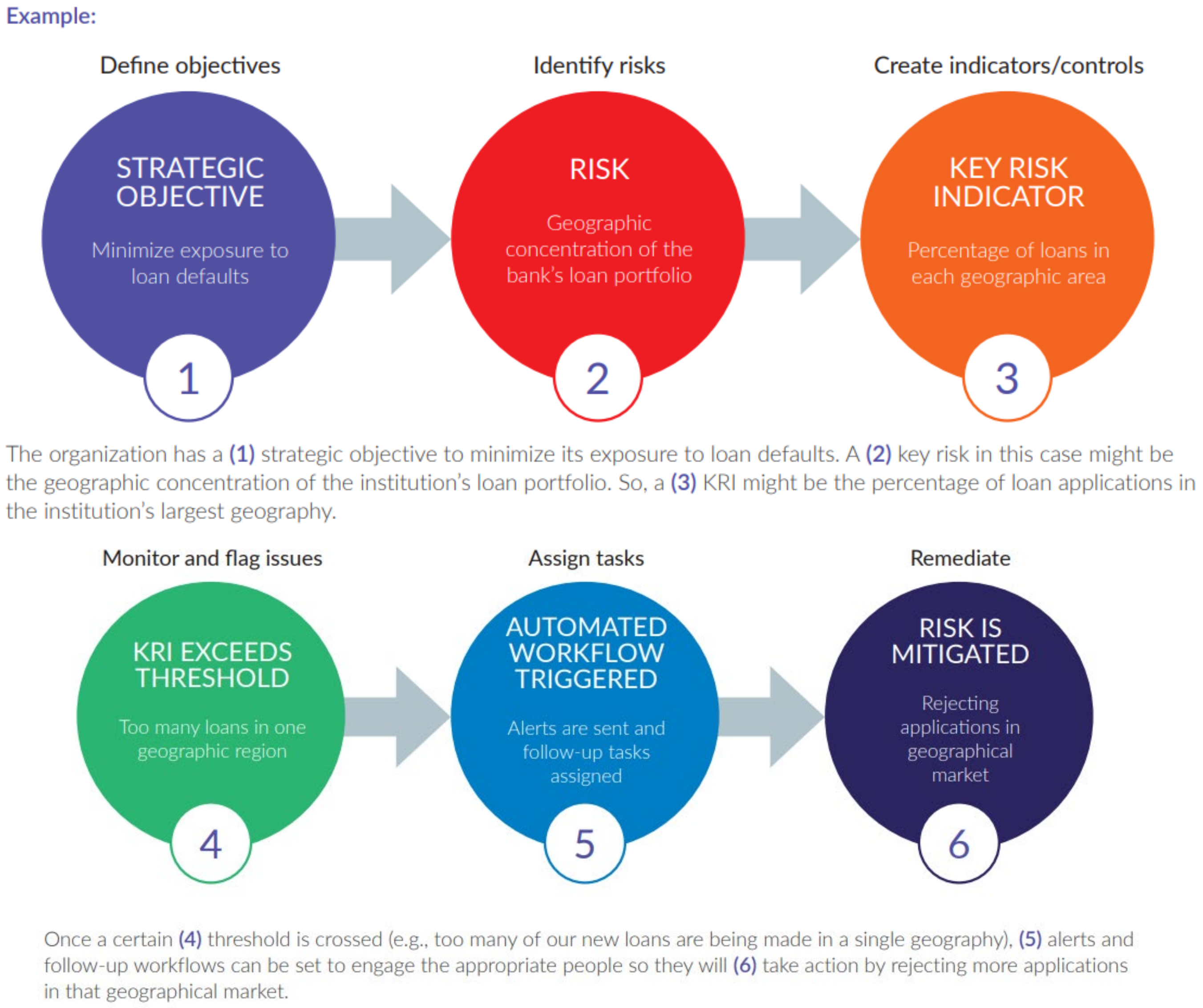
Metric Distinctions

The metrics key performance indicators (KPIs) (point in time/has already taken place) also called lagging indicators. Key Risk Indicators (KRIs) (event has not yet occurred but probability exists can occur, also called leading (KRI) indicators.

KCIs normally focus on controls, monitoring the operations and effectiveness of those controls. They provide direct insight into a specific control activity, procedure, or process which was not implemented or followed correctly

- KRI = Too many loans in one geographic region *(Trend)*
- KPI = number of loans for clients who have past defaults
- KCI = number of clients with insufficient collateral coverage not detected

Source of graphic provided by: Institute of Operational Risk, Operational Risk Sound Practice Guidance - Key Risk Indicators, (November, 2010)



Example:

Define objectives

STRATEGIC OBJECTIVE

Minimize exposure to loan defaults

1

Identify risks

RISK

Geographic concentration of the bank's loan portfolio

2

Create indicators/controls

KEY RISK INDICATOR

Percentage of loans in each geographic area

3

The organization has a **(1)** strategic objective to minimize its exposure to loan defaults. A **(2)** key risk in this case might be the geographic concentration of the institution's loan portfolio. So, a **(3)** KRI might be the percentage of loan applications in the institution's largest geography.

Monitor and flag issues

KRI EXCEEDS THRESHOLD

Too many loans in one geographic region

4

Assign tasks

AUTOMATED WORKFLOW TRIGGERED

Alerts are sent and follow-up tasks assigned

5

Remediate

RISK IS MITIGATED

Rejecting applications in geographical market

6

Once a certain **(4)** threshold is crossed (e.g., too many of our new loans are being made in a single geography), **(5)** alerts and follow-up workflows can be set to engage the appropriate people so they will **(6)** take action by rejecting more applications in that geographical market.

Core Objective: Evaluating how well the business solutions uphold the company’s risk appetite

A solid KRI process brings advantages to a firm. Risk is not just a threat it is a business opportunity as well.
Key Risk Indicators are parameters that effectively measure risks involved in the business procedure and <u>provides us with prior notification of its possible harmful consequences</u>, e.g., Enterprise Risk Management (ERM).

Risk Identified	KRI	Department
Delay in resolving issues may impact business reputation, loss of business and legal issues.	The average amount of time required for the support team to diagnose, resolve, and close an IT support request.	IT Systems Management
Lack of customer satisfaction will lead to the loss of customers and business failures.	Percentage of satisfied customers to total customers.	Marketing/Sales
Lack of training will enable attackers to gain access to confidential information that results in financial losses and even legal and regulatory compliance issues.	An increase in social engineering and phishing attacks.	Information Security & Security Operations / Cybersecurity

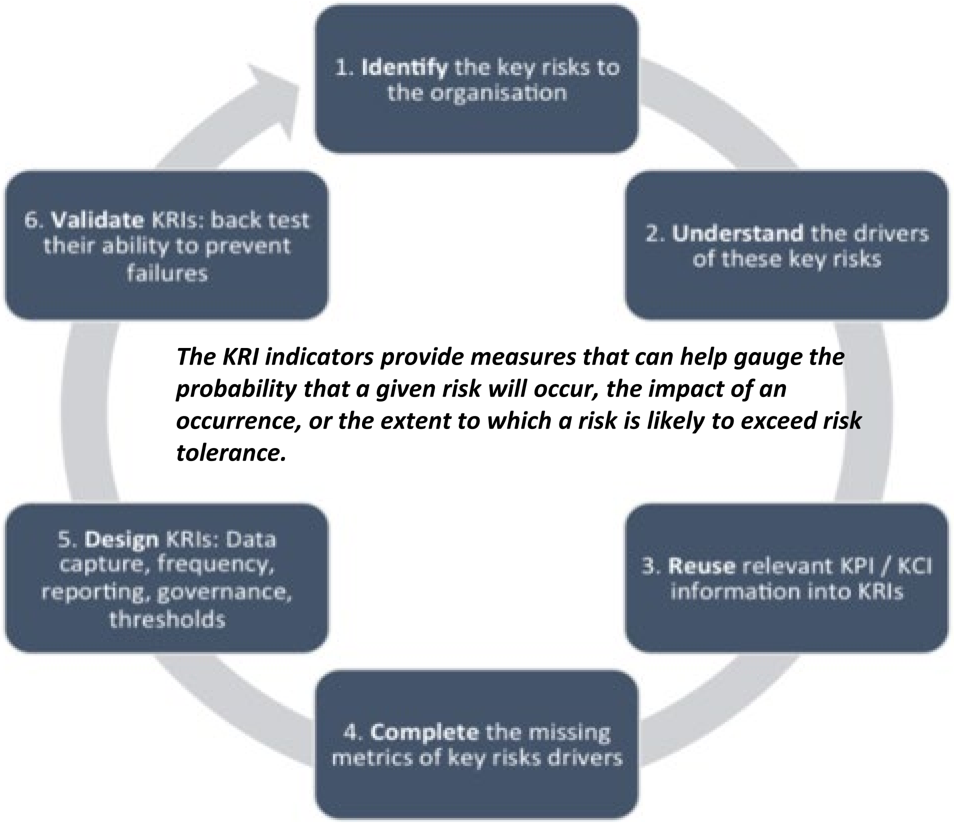
Determine the organization’s Top Risks

Focus on the potential financial, operational, and reputational impact associated with critical assets aligned with a business process.

Monitoring the organization’s risk posture trending.
Is risk increasing or decreasing?

<u>Compare</u> the company’s current performance (protecting sensitive data, operational or logistical risks, preventing data breaches, etc.) against the organization's risk appetite.

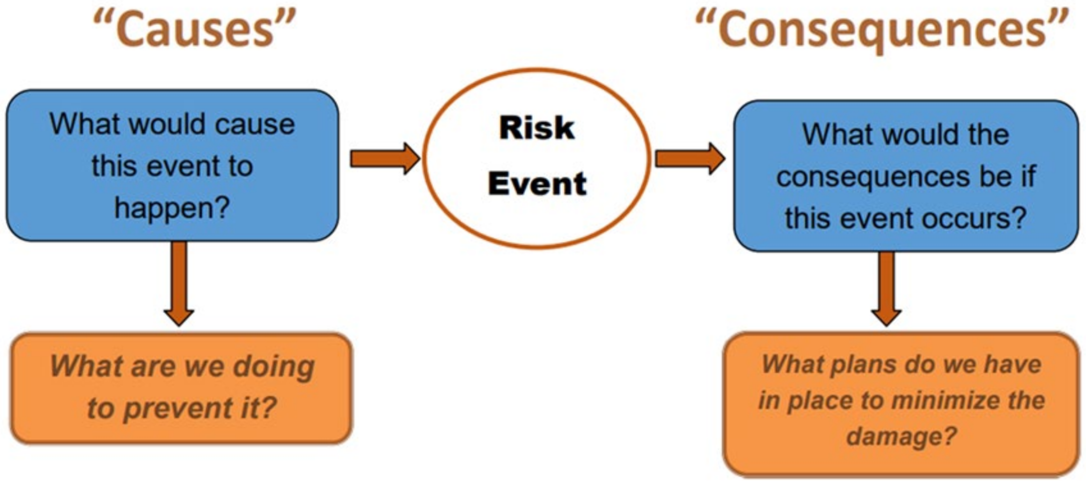
Leading Rather than Lagging Indicators



1. **Identify** the key risks to the organisation
2. **Understand** the drivers of these key risks
3. **Reuse** relevant KPI / KCI information into KRIs
4. **Complete** the missing metrics of key risks drivers
5. **Design** KRIs: Data capture, frequency, reporting, governance, thresholds
6. **Validate** KRIs: back test their ability to prevent failures

The KRI indicators provide measures that can help gauge the probability that a given risk will occur, the impact of an occurrence, or the extent to which a risk is likely to exceed risk tolerance.

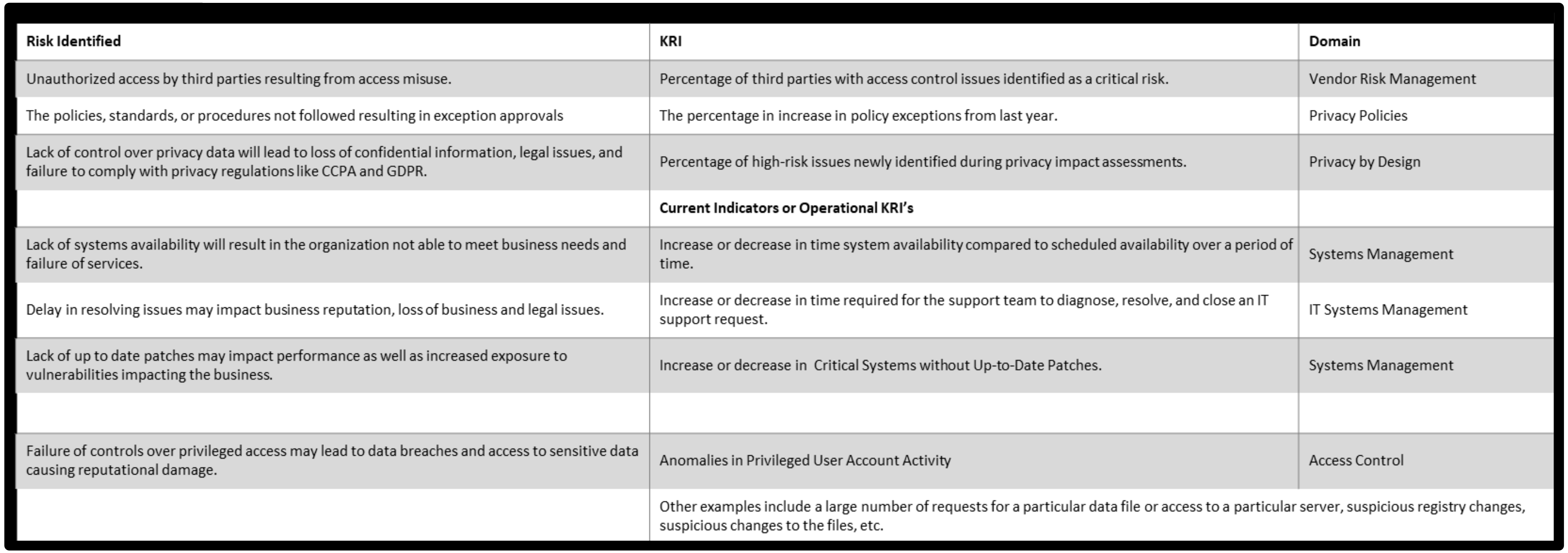
KRI Examples Proactive Risk Management



“Causes”
“Consequences”
What would cause this event to happen?
Risk Event
What would the consequences be if this event occurs?
What are we doing to prevent it?
What plans do we have in place to minimize the damage?

KRI Applies to Any type of Risk, Anywhere, Anytime

Not a point in time solution



Risk Identified	KRI	Domain
Unauthorized access by third parties resulting from access misuse.	Percentage of third parties with access control issues identified as a critical risk.	Vendor Risk Management
The policies, standards, or procedures not followed resulting in exception approvals	The percentage in increase in policy exceptions from last year.	Privacy Policies
Lack of control over privacy data will lead to loss of confidential information, legal issues, and failure to comply with privacy regulations like CCPA and GDPR.	Percentage of high-risk issues newly identified during privacy impact assessments.	Privacy by Design
	Current Indicators or Operational KRI's	
Lack of systems availability will result in the organization not able to meet business needs and failure of services.	Increase or decrease in time system availability compared to scheduled availability over a period of time.	Systems Management
Delay in resolving issues may impact business reputation, loss of business and legal issues.	Increase or decrease in time required for the support team to diagnose, resolve, and close an IT support request.	IT Systems Management
Lack of up to date patches may impact performance as well as increased exposure to vulnerabilities impacting the business.	Increase or decrease in Critical Systems without Up-to-Date Patches.	Systems Management
Failure of controls over privileged access may lead to data breaches and access to sensitive data causing reputational damage.	Anomalies in Privileged User Account Activity	Access Control
	Other examples include a large number of requests for a particular data file or access to a particular server, suspicious registry changes, suspicious changes to the files, etc.	

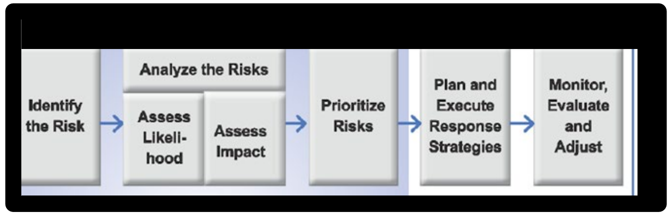
Business and Security Collaboration

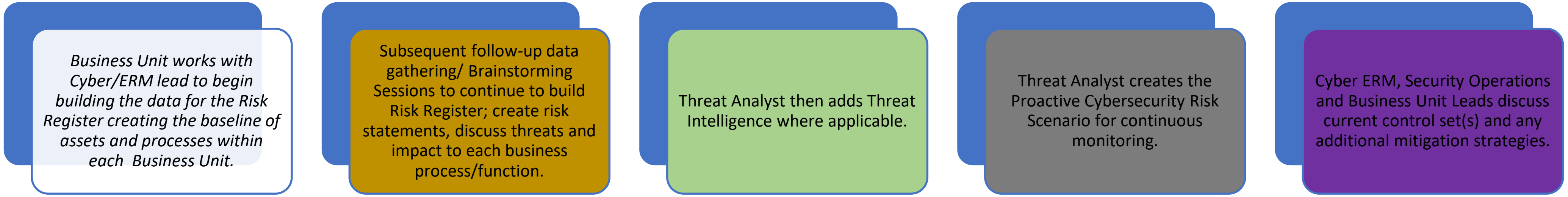
Agile in nature

Enterprise Risk Management (ERM) : *ERM is the process of identifying and addressing methodically the potential events that represent risks to the achievement of strategic objectives and provides the opportunity to gain competitive advantage.*

Purpose of Risk Register

Integrated Enterprise Risk Management Program*: The organization and cybersecurity are in lockstep. Business units implement best cybersecurity practices as part of the day-to-day business.*





Business Unit works with Cyber/ERM lead to begin building the data for the Risk Register creating the baseline of assets and processes within each Business Unit.

Subsequent follow-up data gathering/ Brainstorming Sessions to continue to build Risk Register; create risk statements, discuss threats and impact to each business process/function.

Threat Analyst then adds Threat Intelligence where applicable.

Threat Analyst creates the Proactive Cybersecurity Risk Scenario for continuous monitoring.

Cyber ERM, Security Operations and Business Unit Leads discuss current control set(s) and any additional mitigation strategies.

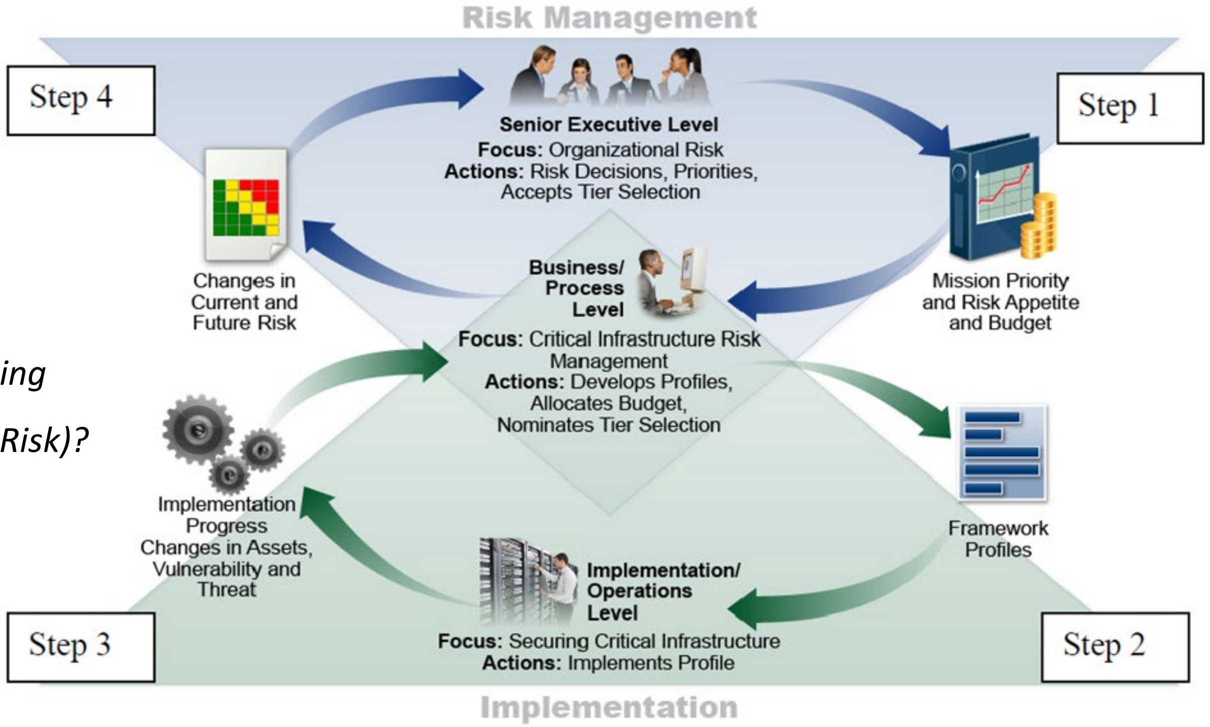
Brainstorming Sessions
A Collaborative Effort → Risk Register

Risk Register: The relationship between various risk indicators and their causes *The Risk Advisor of a firm (along with the respective business owners) assesses all its risks and scores their severity according to probability (or likelihood) and impact, it is then possible to determine the key risks.*

What does the conversation look like to create the Risk Register?

1. *What are the business processes?*
2. *What are the associated assets?*
3. *What if any are the shared resources?*
4. *What are the potential key risks?*
5. *Who is the most likely threat actor(s), e.g., internal, external?*
6. *What are the potential business impact conditions, e.g., affecting Financial Systems, Operational, Reputational/Brand (Inherent Risk)?*
7. *What are the current control sets applied?*

Risk Advisor Meets with Business Leads to Discuss Potential Risks


Risk Management
Step 4
Step 1
Senior Executive Level
Focus: Organizational Risk
Actions: Risk Decisions, Priorities, Accepts Tier Selection
Changes in Current and Future Risk
Mission Priority and Risk Appetite and Budget
Business/ Process Level
Focus: Critical Infrastructure Risk Management
Actions: Develops Profiles, Allocates Budget, Nominates Tier Selection
Implementation Progress Changes in Assets, Vulnerability and Threat
Framework Profiles
Implementation/ Operations Level
Focus: Securing Critical Infrastructure
Actions: Implements Profile
Step 3
Step 2
Implementation

The Risk Register provides an important mechanism for recording and communicating risk decisions.

Consider Risk Categories

❑ HARM TO OPERATIONS
❑ HARM TO ASSETS
❑ HARM TO OTHER ORGANIZATIONS
❑ HARM TO INDIVIDUALS
❑ HARM TO OTHER NATIONS

***Cyber Risk Quantification**:* In business, risk exposure is often used to rank the probability of different types of losses to determine which losses are acceptable or unacceptable and the cost to the business if lose is realized.

HARM TO OPERATIONS Conditions affecting Clients, Products, & Business Practices; product defects, fiduciary breaches	Non-Compliance with Regulatory and Contractual Requirements-- The threat covers the possibility that individual employees fail to comply with their respective responsibilities under applicable regulation and/or contractual requirements or The threat covers the possibility that a compliance requirement is understood incorrectly, and the requirement is not met.
HARM TO ASSETS Conditions affecting Damage or Loss to information systems and networks	Threat of Information and Information Processing Availability and Integrity Failures-- CIA Triad
HARM TO OTHER ORGANIZATIONS Conditions affecting Domestic or Foreign Market Interference	Internal - The average amount of time required for the support team to diagnose, resolve, and close an IT support request exceeds the SLA.
HARM TO INDIVIDUALS Identity Theft	Ineffective monitoring of Log file Data, e.g., PII in clear text
HARM TO OTHER NATIONS Conditions affecting Domestic or Foreign Market Interference	Attack Patterns: indicators leading to suspicion of leaks or data exfiltration with business process

Key Threat Categories

Key Threat Categories (Which are the most likely aligned with the Risk)

- Communications Failure-- Unavailability of Service Provider, Failure of data link Accidental delay in delivery, and Accidental denial of service Coordination between internal organizations.
- Non-Compliance with Regulatory and Contractual Requirements-- The threat covers the possibility that individual employees fail to comply with their respective responsibilities under applicable regulation and/or contractual requirements or The threat covers the possibility that a compliance requirement is understood incorrectly, and the requirement is not met.
- Unauthorized/Inappropriate Access-- The threat covers the possibility that development personnel have unauthorized or inappropriate access to production environments associated with information system assets or SDLC is not consistently followed.
- Ineffective Change Management Systems-- The threat covers the possibility of using multiple systems for change management allowing for multiple processes which do not have similar controls or conflicting controls ultimately resulting in service performance, confidentiality or availability issues.
- Asset Availability-- The threat covers the possibility that software or hardware assets are not available during critical times.
- Unauthorized Access or Use of a System-- The threat covers the possibility of individuals using information system assets for unauthorized purposes, including but not limited to production systems, network devices and software.
- Threat modeling is not an integral component of Software Development
- Ineffective monitoring of Log file Data, e.g., PII in clear text

Align Business Risk with Security Operations Incident Management
Use this information as part of the Risk Register to determine the Impact

Security Risk
<u>Levels</u>
Associated with
Business
Impact

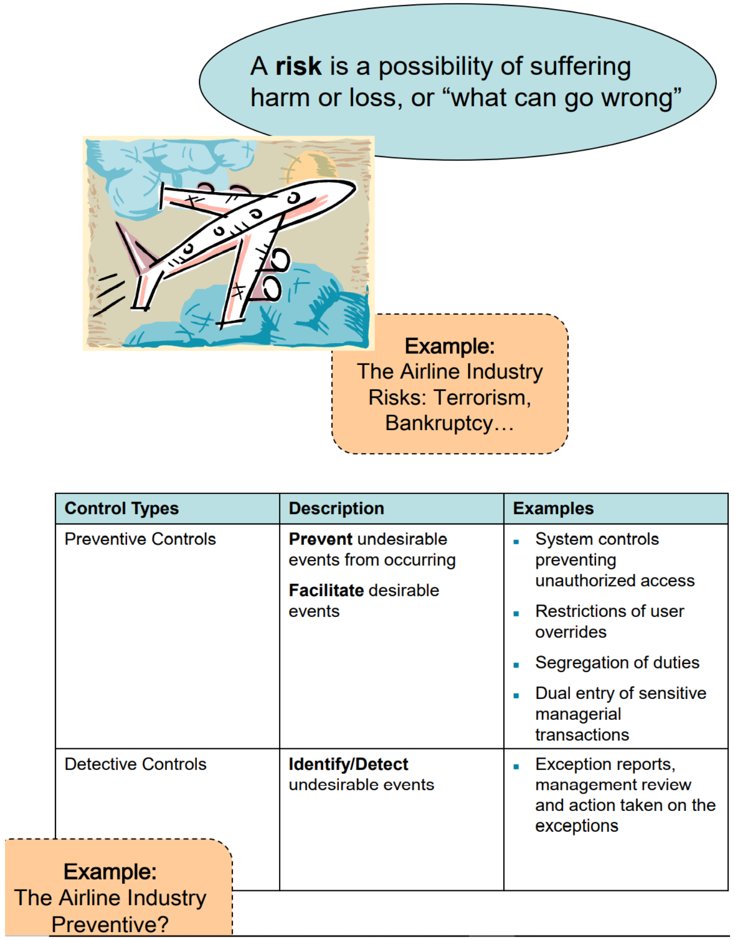
A Common Language

IMPACT	Inherent External Customer Facing (An incident visible to general public or has implications for company Brand Image)	Inherent Internal/Business Partner Facing (An incident involving external parties and may have implications for company Brand)	Inherent Internal Business Critical (An incident that does not involve external parties and is not publicly known, but is propagated throughout company)	Inherent Internal Non-Business Critical (An incident that does not involve external parties and is not publicly known, limited to few company critical assets.
Very High – > 1M +	A direct and significant threat to company brand. Financial loss has likely occurred and directly impacts a wide customer base. **Security Example:** Ransomware whereby Defacement of Public Website or Member Services may be affected. Large- scale disclosure of customer's PII.	A direct and significant threat to the internal company B2B related information assets or business partners. Financial loss is likely in such incidents and impact to business partners(s) may be widespread. **Security Example**: Large scale disclosure of company data.	A direct and significant threat to internal company business critical assets. Some financial loss is likely in such incidents and impact to internal business units may be widespread. **Security Example:** Unauthorized access to a privileged account on a mission critical system or application.	A direct and significant threat to internal company non-business critical information assets. Some financial/ monetary loss is likely in such incidents and impact to internal business units may be widespread. **Security Example**: non-business critical hosts that are connected to externally facing business critical assets.
High – 500K to 1M	An Indirect and potential Threat to company Brand. Financial Loss has likely occurred (but unrealized) in such incidents and customer impact may be intermittent	An indirect and potential threat to internal company B2B related information assets or business partners. Financial loss has likely occurred (but unrealized) in such incidents and impact to business partner(s) may be intermittent.	An indirect and potential threat to internal company business critical information assets. Some financial loss may be possible (but unrealized) in such incidents and impact to internal business units may be intermittent.	A direct and significant threat to internal company non-business critical information assets. Some financial loss is likely in such incidents and impact to internal business units may be widespread.
Moderate – 250K - 500K	May involve a potential (but unrealized) threat to company brand. No financial loss expected in such incidents and customer impact may be minimal. In some cases, anomalous but unconfirmed security incidents may be classified under this level.	May involve a potential (but unrealized) threat to internal company B2B related information assets or business partners. No financial loss expected in such incidents and impact to business partner(s) may be minimal. Incidents do not involve loss of sensitive data.	May involve a potential (but unrealized) threat to the company's information assets. In some cases, anomalous, but unconfirmed security incidents, may be classified at this level. The impacted not expected to be significant.	May involve a potential (but unrealized) threat to a limited number of the company's information assets. In some cases, anomalous, but unconfirmed security incidents, may be classified at this level.
Low - < 250K	**Security Operations Example**: Public Facing server affected by a virus which does not export sensitive data.	**Security Operations Example:** Repeated failed login attempts to B2B systems or applications.	**Security Operations Example:** A single system or workstation infected with a known form of malware (a virus with a confirmed signature).	**Security Operations Example**: Include: Small number of internal systems affected by a virus.

Cyber Risk = Threat x Vulnerability x Information/Asset Value

Controls Section

Control Categories



A **risk** is a possibility of suffering harm or loss, or "what can go wrong"

Example:
The Airline Industry
Risks: Terrorism, Bankruptcy…

Control Types	**Description**	**Examples**
Preventive Controls	**Prevent** undesirable events from occurring **Facilitate** desirable events	▪ System controls preventing unauthorized access ▪ Restrictions of user overrides ▪ Segregation of duties ▪ Dual entry of sensitive managerial transactions
Detective Controls	**Identify/Detect** undesirable events	▪ Exception reports, management review and action taken on the exceptions

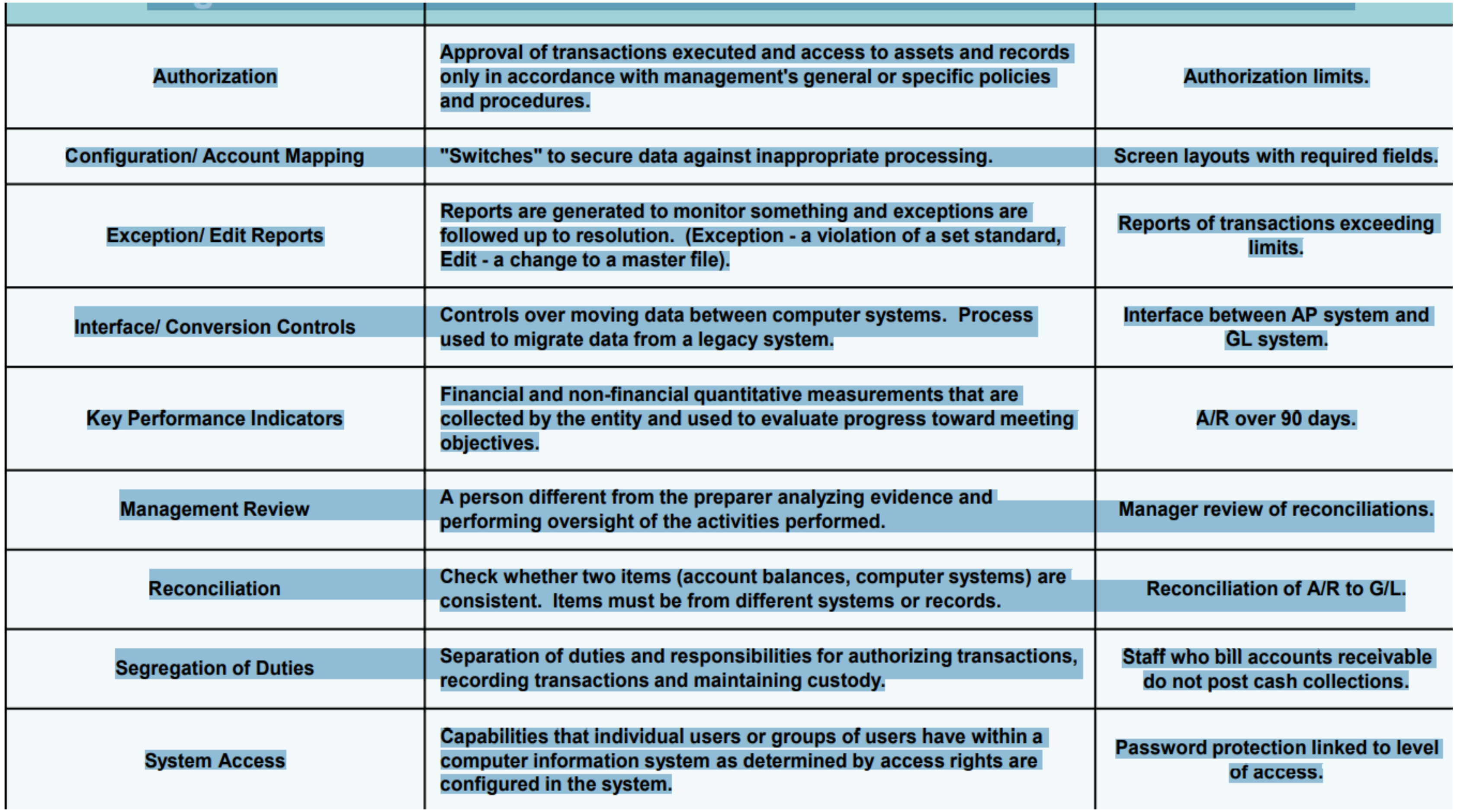
Example:
The Airline Industry
Preventive?

- **Manual** (performed by people)
  - Examples: Authorizations, Management reviews

- **Automatic** (embedded in application code)
  - Examples: Exception reports, Interface controls, System access

Example:
The Airline Industry
Manual controls? Automatic controls?

Non-Technical Controls Use Cases

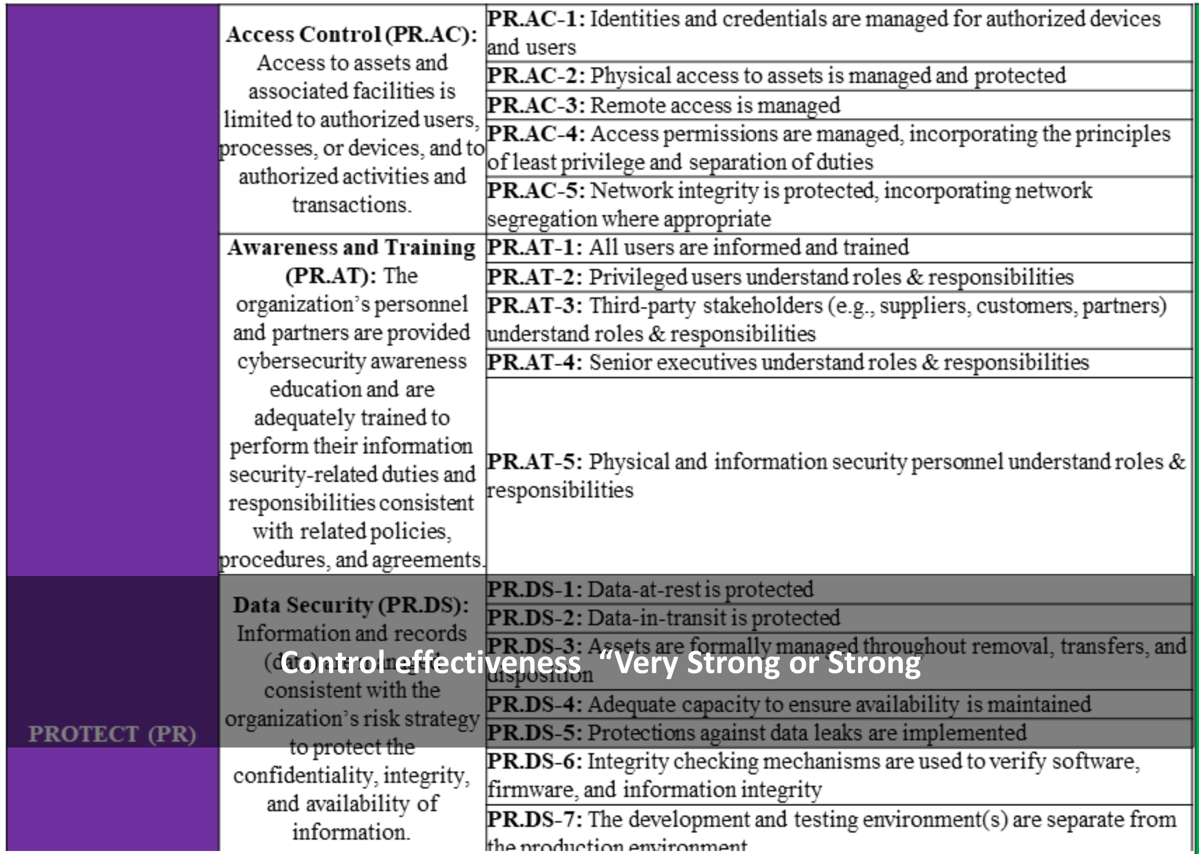


Authorization	Approval of transactions executed and access to assets and records only in accordance with management's general or specific policies and procedures.	Authorization limits.
Configuration/ Account Mapping	"Switches" to secure data against inappropriate processing.	Screen layouts with required fields.
Exception/ Edit Reports	Reports are generated to monitor something and exceptions are followed up to resolution. (Exception - a violation of a set standard, Edit - a change to a master file).	Reports of transactions exceeding limits.
Interface/ Conversion Controls	Controls over moving data between computer systems. Process used to migrate data from a legacy system.	Interface between AP system and GL system.
Key Performance Indicators	Financial and non-financial quantitative measurements that are collected by the entity and used to evaluate progress toward meeting objectives.	A/R over 90 days.
Management Review	A person different from the preparer analyzing evidence and performing oversight of the activities performed.	Manager review of reconciliations.
Reconciliation	Check whether two items (account balances, computer systems) are consistent. Items must be from different systems or records.	Reconciliation of A/R to G/L.
Segregation of Duties	Separation of duties and responsibilities for authorizing transactions, recording transactions and maintaining custody.	Staff who bill accounts receivable do not post cash collections.
System Access	Capabilities that individual users or groups of users have within a computer information system as determined by access rights are configured in the system.	Password protection linked to level of access.

- Human Resources Security
- Covered Entity
- Performance Evaluation
- Personnel Security
- Consent And Authorization
- Confidential Communications
- Policies And Procedures
- Privacy Safeguards
- Program Management

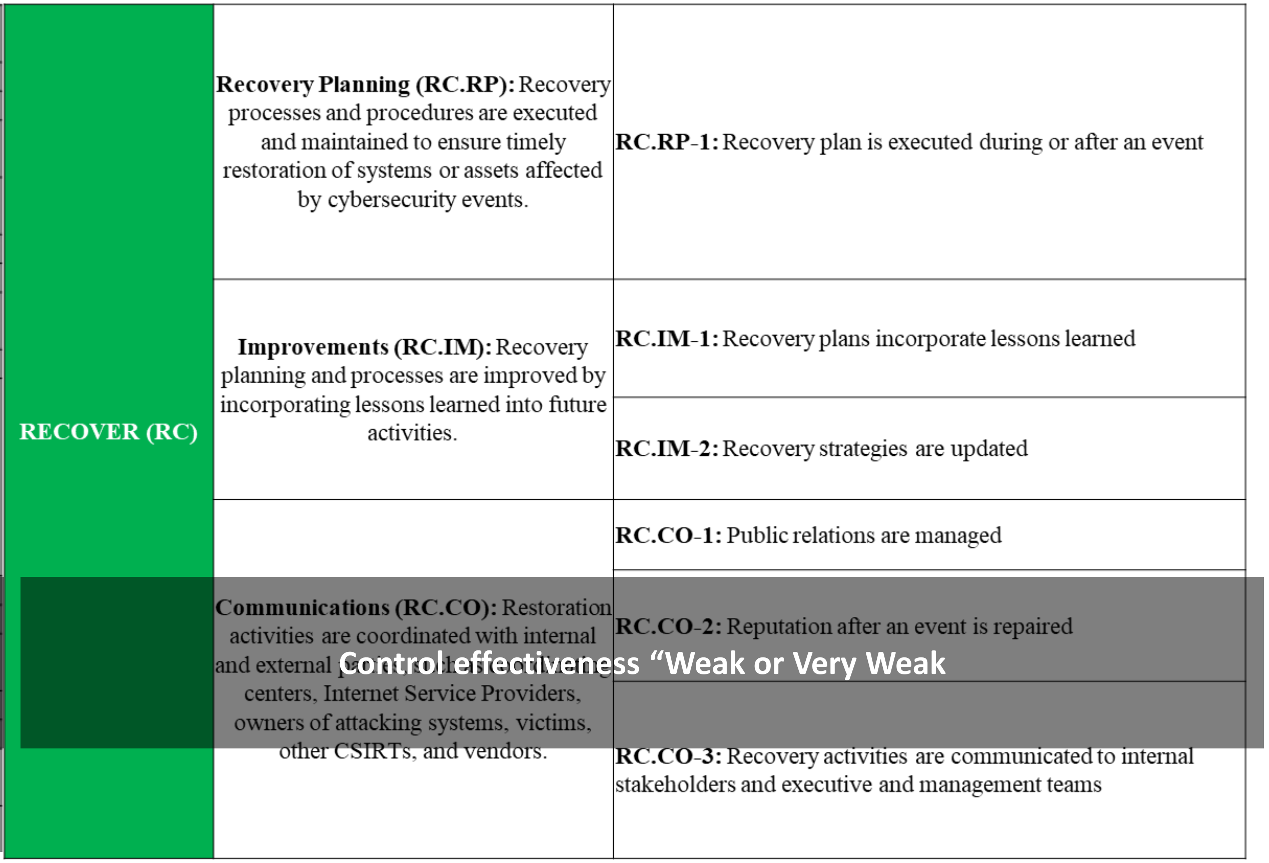
- Non-retaliation
- Use And Disclosure
- Workforce Sanctions
- Supplier Relationships
- Audit And Accountability
- Administrative Safeguards
- Physical And Environmental Protection

NIST Control Set



PROTECT (PR)	**Access Control (PR.AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are managed for authorized devices and users
		PR.AC-2: Physical access to assets is managed and protected
		PR.AC-3: Remote access is managed
		PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties
		PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	**PR.AT-1:** All users are informed and trained
		PR.AT-2: Privileged users understand roles & responsibilities
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities
		PR.AT-4: Senior executives understand roles & responsibilities
		PR.AT-5: Physical and information security personnel understand roles & responsibilities
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data-at-rest is protected
		PR.DS-2: Data-in-transit is protected
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition
		PR.DS-4: Adequate capacity to ensure availability is maintained
		PR.DS-5: Protections against data leaks are implemented
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity
		PR.DS-7: The development and testing environment(s) are separate from the production environment

Control effectiveness “Very Strong or Strong



RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	**RC.RP-1:** Recovery plan is executed during or after an event
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-1:** Recovery plans incorporate lessons learned
		RC.IM-2: Recovery strategies are updated
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	**RC.CO-1:** Public relations are managed
		RC.CO-2: Reputation after an event is repaired
		RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams

Control effectiveness “Weak or Very Weak

Assets & Business
Processes & Controls

Risk Register

Create Risk Statements/ Cyber Scenarios to Proactively address Business Risk

Identify the Business Process(es)

Maintaining customer profiles in Flight Bridge

Identify the asset and all dependencies

Confluence, Flight Bridge, Server

Identify the risk

Modification or deletion of customer profiles in Flight Bridge

Consider the Business Impact and Key Risk Categories

Conditions affecting Customer Client Account Management/Security, Conditions affecting Reputational Damage

Asset Management, e.g., Information Processing System Confidentiality or Misuse

Relevant Threat Actor (insider, Counterparty, Cyber Criminal Gang, or Nation-State)

Create a Cyber Risk Narrative

Modification or deletion of customer profiles In Flight Bridge*. An external threat actor exploits a vulnerability due to lax patching, or successful hacking technique, enabling information and information processing system confidentiality or misuse. The Confluence server and Flight Bridge data is potentially compromised or data exfiltrated. This results in an impact to customer profiles in Flight bridge and potential harm to brand reputation.*

What are the assets & resources for each business process?

What are the possible Business Conditions having a negative impact?

What are the possible Key Risk categories that determine the Probability /likelihood of a risk being realized?

Risk Statement Formula

There is a potential **<risk >** performed by **<threat actor>** **taking advantage of weaknesses<threat vectors>** leading to **<outcome/risk realized>** affecting an **<asset>** that causes an **<impact>**

Assets & Business Processes

Brainstorming: Information Supplied by Business SME(s)

Risk ID	Business Unit/Department Name	Business Lead Name and/or Responsible Person for business function	Business Process *(Please list all key processes and projects within your Department denoting one function per line)* For example, Under Sales,)	Asset Type/Category	Asset Name *(multiple assets exist for a single Business Process, Please list 1 per line)*	In-House /SaaS	Asset Rating *(Estimated Impact to Company if risk realized)* reference Impact Chart	Risk Category	Risk Description *(Evaluate Asset + Process/Function to determine gaps or lack of controls that may create risk)* There is a potential <risk > performed by <threat actor> taking advantage of weaknesses<threat vectors> leading to <potential outcome/risk realized> affecting an <asset> that causes an <impact>
Fin-1	Finance	Harry Jones	NetSuite - Accounts Payable	Names and addresses, payments (bank details, invoices), contractual information, medical details, passports	Production and QA environments	SaaS	Moderate	Confidentiality	vendor information, invoices, and payment history available on sandbox and production environments. User Profile roles and access management with potential for shared passwords and developer able to access production environment.

KRI Statements
Trend: indicators leading to suspicion of leaks or data exfiltration with business process

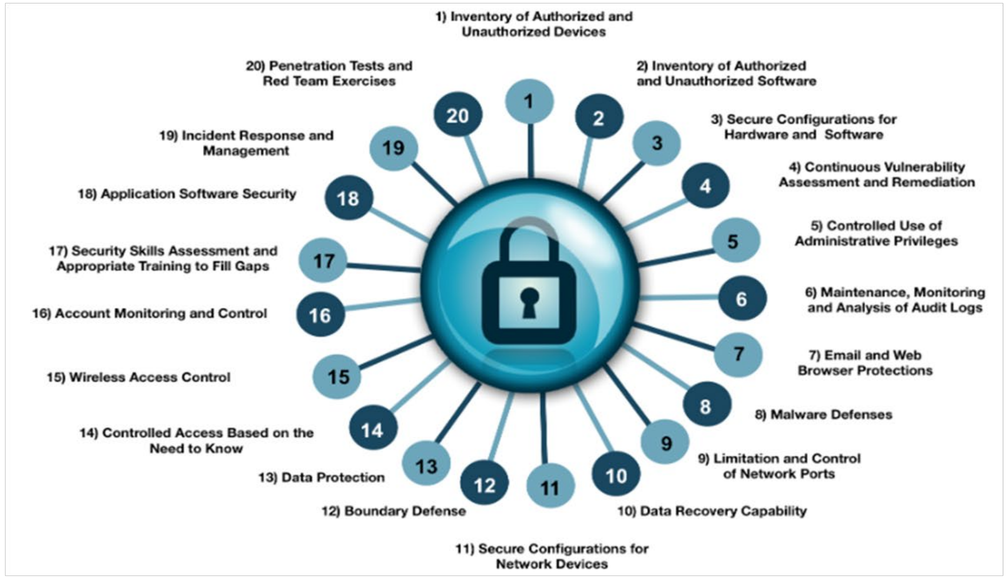
Estimated Inherent Impact Level Financial Cost (cost if risk realized) (Please reference Impact Chart)	Estimated Inherent Impact Level Operational (Please reference Impact Chart)	Estimated Inherent Impact Level Reputational/Brand (Please reference Impact Chart)	Estimated Inherent Likelihood Level (probability risk can be realized)	Estimated Risk Response Overall Cost to Business
Moderate	Moderate	Moderate	Moderate	250K

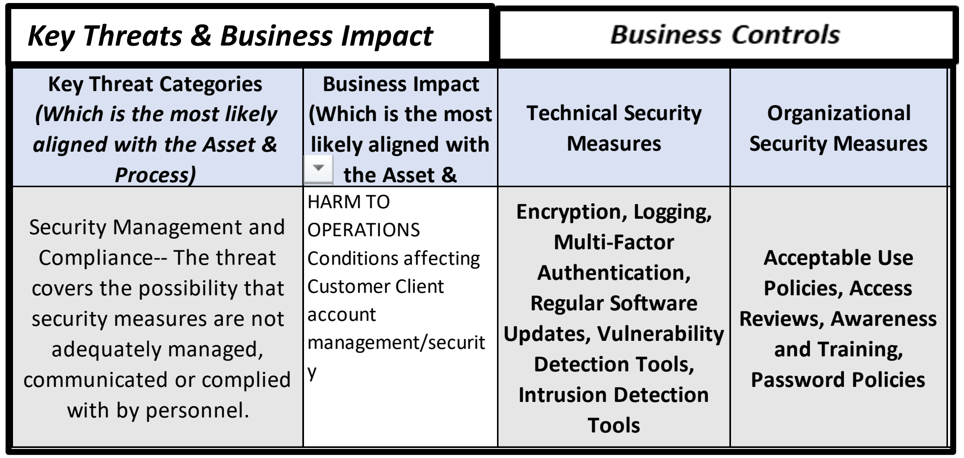
Key Threats, Business Impact, Controls & Cyber scenario

Control Categories

- ❖ Very Weak
- ❖ Weak
- ❖ Strong
- ❖ Very Strong

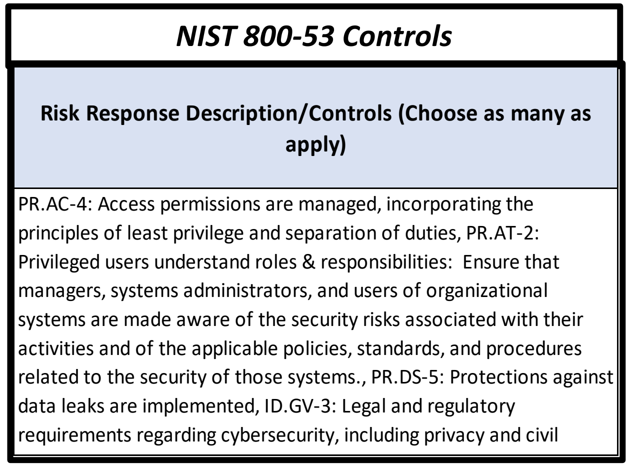
Technical Controls


1) Inventory of Authorized and Unauthorized Devices
2) Inventory of Authorized and Unauthorized Software
3) Secure Configurations for Hardware and Software
4) Continuous Vulnerability Assessment and Remediation
5) Controlled Use of Administrative Privileges
6) Maintenance, Monitoring and Analysis of Audit Logs
7) Email and Web Browser Protections
8) Malware Defenses
9) Limitation and Control of Network Ports
10) Data Recovery Capability
11) Secure Configurations for Network Devices
12) Boundary Defense
13) Data Protection
14) Controlled Access Based on the Need to Know
15) Wireless Access Control
16) Account Monitoring and Control
17) Security Skills Assessment and Appropriate Training to Fill Gaps
18) Application Software Security
19) Incident Response and Management
20) Penetration Tests and Red Team Exercises
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20



Key Threats & Business Impact		***Business Controls***	
Key Threat Categories *(Which is the most likely aligned with the Asset & Process)*	**Business Impact (Which is the most likely aligned with the Asset &**	**Technical Security Measures**	**Organizational Security Measures**
Security Management and Compliance-- The threat covers the possibility that security measures are not adequately managed, communicated or complied with by personnel.	HARM TO OPERATIONS Conditions affecting Customer Client account management/security	**Encryption, Logging, Multi-Factor Authentication, Regular Software Updates, Vulnerability Detection Tools, Intrusion Detection Tools**	**Acceptable Use Policies, Access Reviews, Awareness and Training, Password Policies**

Risk Register Controls to be Applied to Residual Risk



NIST 800-53 Controls
Risk Response Description/Controls (Choose as many as apply)
PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties, PR.AT-2: Privileged users understand roles & responsibilities: Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems., PR.DS-5: Protections against data leaks are implemented, ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil

Cybersecurity Operations Methodology

External Threat Intelligence Example

Vulnerability: "Sep 07, 2021 · Tracked as CVE-2021-26084, The Critical score, 9.9/10 CVSS score and is actively exploited in the wild. Recently, several threats actors were seen abusing the vulnerability to target public and private sector organizations. This exploit could allow an attacker to execute arbitrary code on a Confluence Server or Data Center instance and in the cloud. One of the internal servers suffered a breach due to a hijacked Confluence Server wherein attackers deployed a cryptocurrency miner, affecting service operations and potential data exposure.

The MITRE ATT&CK Framework is a threat intelligence framework based on real-world observations and incidents.
It demonstrates known adversary attack methods (malicious actor behavior), giving everyone in the security community a single tool to discuss and test against adversary activities.

MITRE a (not-for-profit organization) creates new ways to help the Business understand their adversaries' behaviors, goals, and methods to prioritize their offensive & defensive investments.

Business Impact

Condition affecting Financial loss & Fraud (External

Key Risk Leading Indicators

Identified threats, attack surface and Vulnerabilities

Log-In Red Flags, or anomalies in Privileged User Activity

Attack Trends: Vulnerabilities: Increase in Zero-Day, or increased sophistication of attack vector

Attack Surface: Aligns with Exploit

***Probability:* What is the motivation to attack that would make it more likely to occur?**

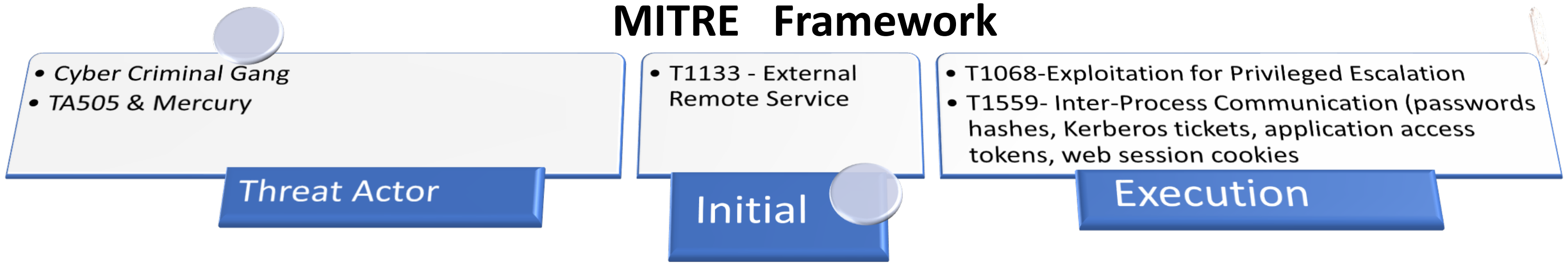
What is the criticality of the asset or business process to the firm?

Business Impact: What is the driver; Financial, Espionage/ Intellectual Property, Reputational damage, Operational loss?

What are the key risks, e.g., What are our critical domains, and are the external resources vulnerable to malicious use?

Is the risk statement/cyber scenario relevant to this type of attack?

MITRE   Framework



- *Cyber Criminal Gang*
- *TA505 & Mercury*

Threat Actor

- T1133 - External Remote Service

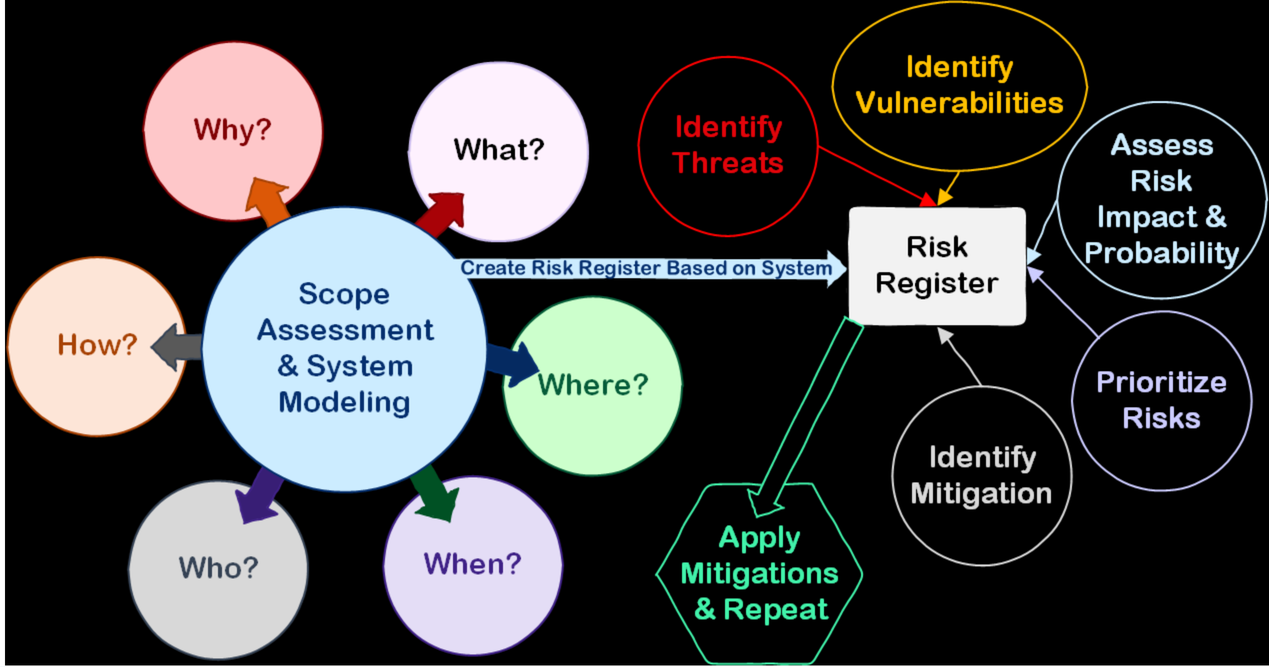
Initial

- T1068-Exploitation for Privileged Escalation
- T1559- Inter-Process Communication (passwords hashes, Kerberos tickets, application access tokens, web session cookies

Execution

Modification or deletion of customer profiles In Flight Bridge*. A cyber criminal gang exploits a known vulnerability via external remote services, then actor performs exploitation for privileged escalation toward lateral movement. The Confluence server and Flight Bridge data is potentially compromised as part of a ransomware attack, or data exfiltrated. This results in an impact to customer profiles in Flight bridge and potential harm to brand reputation.*

Threat Modeling – Cybersecurity Scenarios Attribution /Threat Intelligence


Why?
What?
Identify Threats
Identify Vulnerabilities
Assess Risk Impact & Probability
Create Risk Register Based on System
Risk Register
How?
Scope Assessment & System Modeling
Where?
Prioritize Risks
Identify Mitigation
Who?
When?
Apply Mitigations & Repeat

Cybersecurity Scenarios	MITRE Reconnaissance Attack Vector	MITRE Reconnaissance Attack Vector	MITRE Initial Access Vector	MITRE Execution	MITRE Persistence	MITRE Lateral Movement	MITRE Collection	MITRE C2C	MITRE Exfiltration	MITRE Impact
Risk to NetSuite accounts payable. A cyber criminal gang gathers host information and credentials from someone inside the organization via social engineering, then uses the deficiency to access the system with a valid account. The actor creates or modifies system processes, to allow for access to and removal of data from the local system, potentially resulting in data exfiltration of Netsuite Accounts Payable, PII, bank details, and PHI. Due to account access, potential impact to the organization's brand and financial systems incurring financial loss and loss of sensitive proprietary data of client accounts	Cyber criminal Gang	T1592- Gather victim's Host Information	T1078- Valid Account	T1203- Exploitation for Client Execution	T1543- Create or Modify System Process	T1210- Exploitation of remote Services	T1039- Data From Network Shared Drive	T1090- Proxy	T1048 Exfiltration Over Alternate Protocol	T1531- Account Access Removal

MITRE applies Control recommendations toward actionable Decisions Mitigating the Risk

Business Leads(SME)s determine the risk
BISA/SecOps determine the Threats
= Agility & Collaboration

Security Operations Mitigations					Business Controls
Threat ID	Tactic	Function	Threat Target	Detection Mitigation For SecOps	Suggested Mitigation for Business
T1213.001	Defense Evasion, Persistence, Privilege Escalation	Audit	Confluence	Monitor file systems for moving, renaming, replacing, or modifying. Changes that are loaded by a process (compared to past behavior) that do not correlate with known software, patches, etc., are suspicious. Hijacking Scanner can be used to identify applications vulnerable to hijacking.(Citation: Wardle Hijack Vulnerable Apps)(Citation: Github EmpireProject HijackScanner)	**Consider periodic review of accounts and privileges for critical and sensitive Confluence repositories.**
T1213.001	Defense Evasion, Persistence, Privilege Escalation	User Account Management	Confluence	Look for changes to binaries and service executables that may normally occur during software updates. If an executable is written, renamed, and/or moved to match an existing service executable, it could be detected and correlated with other suspicious behavior. Look for abnormal process call trees from typical processes and services and for execution of other commands that could relate to Discovery or other adversary techniques.	**Enforce the principle of least-privilege. Consider implementing access control mechanisms that include both authentication and authorization.**
T1213.001	Defense Evasion, Persistence, Privilege Escalation	User Training	Confluence	Monitor for changes to environment variables and files associated with loading shared libraries such as <code>LD_PRELOAD</code> and <code>DYLD_INSERT_LIBRARIES</code>, as well as the commands to implement these changes. Monitor processes for unusual activity (e.g., a process that does not use the network begins to do so). Track library metadata, such as a hash, and compare libraries that are loaded at process execution time against previous executions to detect differences that do not correlate with patching or updates.	**Develop and publish policies that define acceptable information to be stored regarding Confluence repositories.**

Workshops

Residual Risk

Business Area & Functional Unit xxx:

***Modification or deletion of customer profiles In Flight Bridge**. A cyber criminal gang exploits a known vulnerability via external remote services, then actor performs exploitation for privileged escalation toward lateral movement. The Confluence server and Flight Bridge data is potentially compromised as part of a ransomware attack, or data exfiltrated. This results in an impact to customer profiles in Flight bridge and potential harm to brand reputation.*

Threat likelihood is the probability that an undesirable event will occur.

Likelihood Axis	Likelihood Rating
Inherent Likelihood Rating	Likely
Aggregate Control Effectiveness Rating	Strong
Residual Likelihood Rating	Unlikely

Impact Axis	Financial Systems	Operational	Reputational (Brand)
Inherent Impact Rating	Low	High	High
Aggregate Control Rating		Strong	
Residual Impact Rating	Low	Low	Moderate
Residual Impact Rating (High Water Mark)		Moderate	

IMPACT

Very High – > 1M +

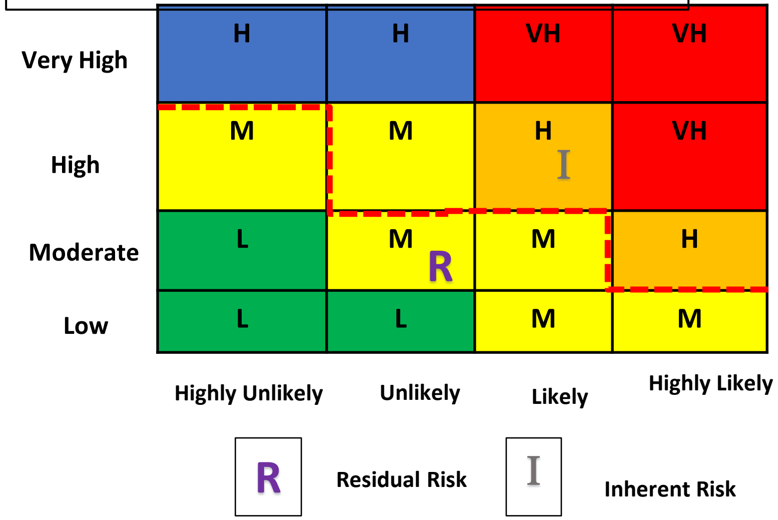
High – 500K to 1M

Moderate – 250K - 500K

Low - < 250K

Mitigating Controls	Is the Control Mitigating the Impact or Likelihood?	Design Effectiveness Rating	Very Weak	Weak	Strong	Very Strong
SI-4(5)- System Monitoring & Alerts	Impact	Effective			x	
Business Area Acceptable Use Policies	Impact	Effective			x	
AC-4 –Information Flow Enforcement	Likelihood	Effective			x	
AC-6(3) -Least Privilege | Network Access to Privileged Commands	Likelihood	Effective			x	

The graph represents Inherent risk ("I" without controls) and a Residual Risk threshold ("R" with controls) to determine if risk is within the company's risk acceptance level



	Highly Unlikely	Unlikely	Likely	Highly Likely
Very High	H	H	VH	VH
High	M	M	H I	VH
Moderate	L	M R	M	H
Low	L	L	M	M

R **Residual Risk**

I **Inherent Risk**

Cybersecurity Threat Intelligence for improved Governance & Communication

Analysis / Continuous Monitoring

Evaluate in Relation to Residual Risk Thresholds: Determine Imminent or Emerging Patterns & Trends

In the wild Zero Day exploitation with a severity rating of High or greater affecting a significant asset population holding an asset risk level of high or greater, probability /likelihood the conditions affecting financial loss- Theft or Fraud are increased.

The exploitation of Active Directory leading to control of data stores. Cyber risk scenario is within its residual risk threshold when it is highly unlikely that an adversary gains access to the Data Stores to exfiltrate customer data, resulting in moderate impact to the firm's reputation due to subsequent loss of trust in the firm to secure sensitive data.

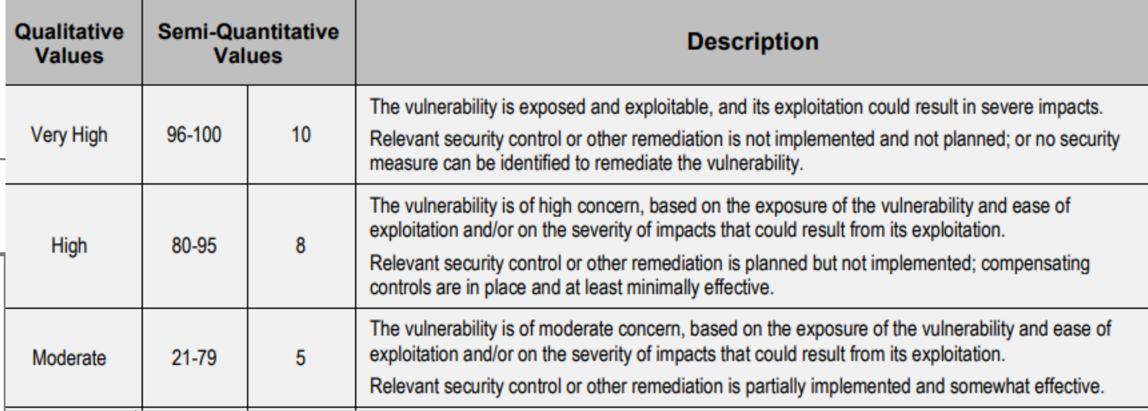
- *If the criticality of the asset group, Rating moderate or greater, then document*
- *If not a high or critical asset, but the Asset Density > 20%, then document*
- *If the vulnerability is actively exploited, then document*
- *If the sophistication of threat actor has increased or vectors gaining popularity within the threat actor groups, then document*
- *If the threat actor is covering a broad threat landscape, then document*
- *If the threat score is high or attribution aligns, then document*
- *If the known controls are not wholly effective in relation to the vulnerability or exploit TTP's, then document*
- *If Patch cycle is not sufficient, then document*
- *If the severity of Security Assessment / Incident & Investigation OR*
  - *Vulnerability Findings, OWASP, App Scan, Third Party Vendors, CVEs, IR Forensics, Investigation Findings, etc., have a high finding, document*

Findings

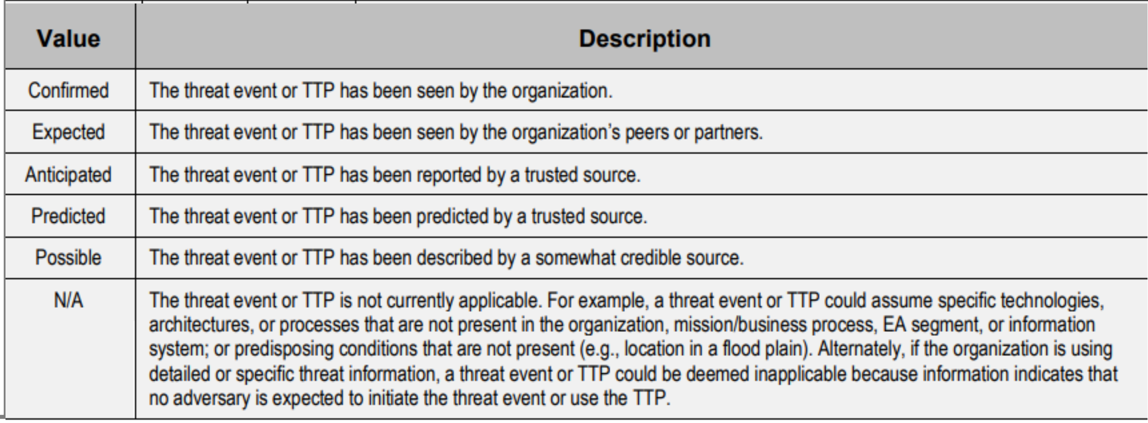
The investigation and analysis is fully documented. The data is stored at a secure centralized location and can be reproduced in support of company determination.

Analysis Criteria**: **For the "Zerologon" vulnerability evaluate the residual risk threshold by evaluating the cyber threat intelligence against the residual risk for each cyber security scenario across the Business Areas.

- ✓ *Keyword Search terms were documented and verified as adequate to produce the correct population*
- ✓ *The Threat Intelligence align wit the Business Impact, e.g., conditions affecting financial loss, theft & fraud, and the KRI: Log-In Red Flags, or anomalies in Privileged User Activity and Attack Trends: Vulnerabilities: Increase in Zero-Day, or increased sophistication of attack vector*
- ✓ *No Findings or Events were reported*
- ✓ *At this time there is no demonstrated or foreseeable intent to target company and/or affiliated industries (contractors, 3rd party vendors, partner businesses*
- ✓ *Patch Cycle is sufficient. Vulnerability was patched on Month/Year.*
- ✓ *Controls are effective in relation to cyber scenarios in play with exception of clearly documenting a single control. Has multi-factor authentication (MFA) for all accounts or least privilege has been applied. In this case even if a privileged account is compromised, this access attempt would still be denied.*
- ✓ *Residual Risk Threshold is documented as within the acceptable range per Business Area citing Highly Unlikely for Residual Likelihood, and Low for Residual Risk Impact.*



Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The vulnerability is exposed and exploitable, and its exploitation could result in severe impacts. Relevant security control or other remediation is not implemented and not planned; or no security measure can be identified to remediate the vulnerability.
High	80-95	8	The vulnerability is of high concern, based on the exposure of the vulnerability and ease of exploitation and/or on the severity of impacts that could result from its exploitation. Relevant security control or other remediation is planned but not implemented; compensating controls are in place and at least minimally effective.
Moderate	21-79	5	The vulnerability is of moderate concern, based on the exposure of the vulnerability and ease of exploitation and/or on the severity of impacts that could result from its exploitation. Relevant security control or other remediation is partially implemented and somewhat effective.



Value	Description
Confirmed	The threat event or TTP has been seen by the organization.
Expected	The threat event or TTP has been seen by the organization's peers or partners.
Anticipated	The threat event or TTP has been reported by a trusted source.
Predicted	The threat event or TTP has been predicted by a trusted source.
Possible	The threat event or TTP has been described by a somewhat credible source.
N/A	The threat event or TTP is not currently applicable. For example, a threat event or TTP could assume specific technologies, architectures, or processes that are not present in the organization, mission/business process, EA segment, or information system; or predisposing conditions that are not present (e.g., location in a flood plain). Alternately, if the organization is using detailed or specific threat information, a threat event or TTP could be deemed inapplicable because information indicates that no adversary is expected to initiate the threat event or use the TTP.

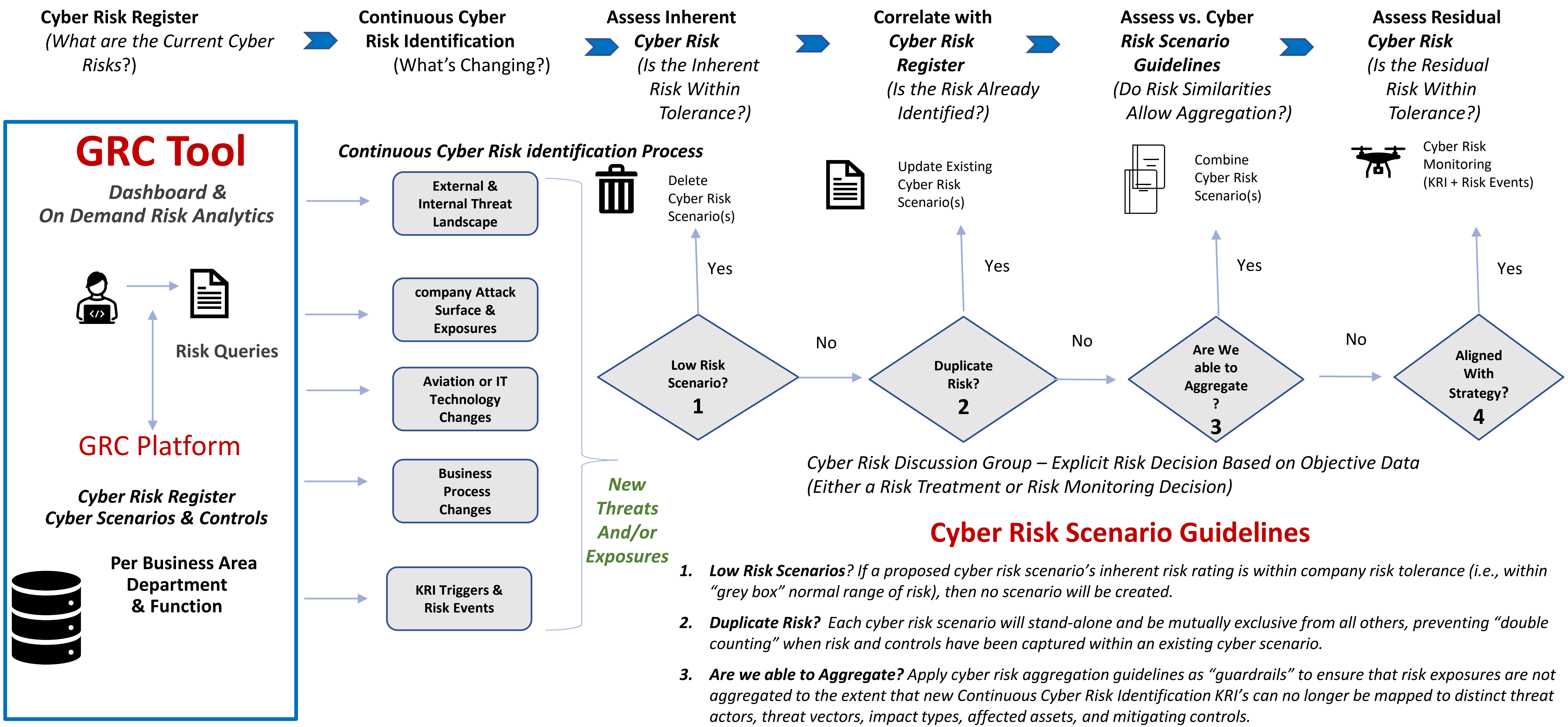
Initiate Cyber Risk Discussion (Lead Group). If MFA has been applied and Use Cases effectively apply to privilege escalation, the Cyber Risk scenario is not in imminent danger of exceeding its current threshold at this time.

Next Steps:

- ✓ *Communication: SecOps/Threat Intelligence Analyst to communicate with Security Team regarding the exploit and the current Use Cases surrounding privilege escalation in correlation to the related asset community. SecOps to communicate with Business and possibly where feasible, associated Technology SME(s) to verify if MFA has been applied.*
- ✓ *Continued Monitoring:*

  Since sophisticated cyber criminal groups have actively exploited the vulnerability in the wild and is gaining confidence by threat actor community as a packaged attack vector, the asset rating is moderate, and the potential for takeover of domains, the confidentiality, integrity, and availability would be impacted as a result of exploiting the vulnerability if successful, company will continue to actively monitor.

Cyber Security Proactive Program Workflow *Verifiable, Repeatable, Documented Process*



Cyber Risk Register *(What are the Current Cyber Risks?)*

Continuous Cyber Risk Identification (What's Changing?)

Assess Inherent *Cyber Risk* *(Is the Inherent Risk Within Tolerance?)*

Correlate with *Cyber Risk Register* *(Is the Risk Already Identified?)*

Assess vs. Cyber *Risk Scenario Guidelines* *(Do Risk Similarities Allow Aggregation?)*

Assess Residual *Cyber Risk* *(Is the Residual Risk Within Tolerance?)*

GRC Tool

Dashboard & On Demand Risk Analytics

Risk Queries

GRC Platform

Cyber Risk Register
Cyber Scenarios & Controls

Per Business Area Department & Function

Continuous Cyber Risk identification Process

External & Internal Threat Landscape

company Attack Surface & Exposures

Aviation or IT Technology Changes

Business Process Changes

KRI Triggers & Risk Events

New Threats And/or Exposures

Low Risk Scenario? 1 — Yes: Delete Cyber Risk Scenario(s) — No

Duplicate Risk? 2 — Yes: Update Existing Cyber Risk Scenario(s) — No

Are We able to Aggregate? 3 — Yes: Combine Cyber Risk Scenario(s) — No

Aligned With Strategy? 4 — Yes: Cyber Risk Monitoring (KRI + Risk Events)

Cyber Risk Discussion Group – Explicit Risk Decision Based on Objective Data (Either a Risk Treatment or Risk Monitoring Decision)

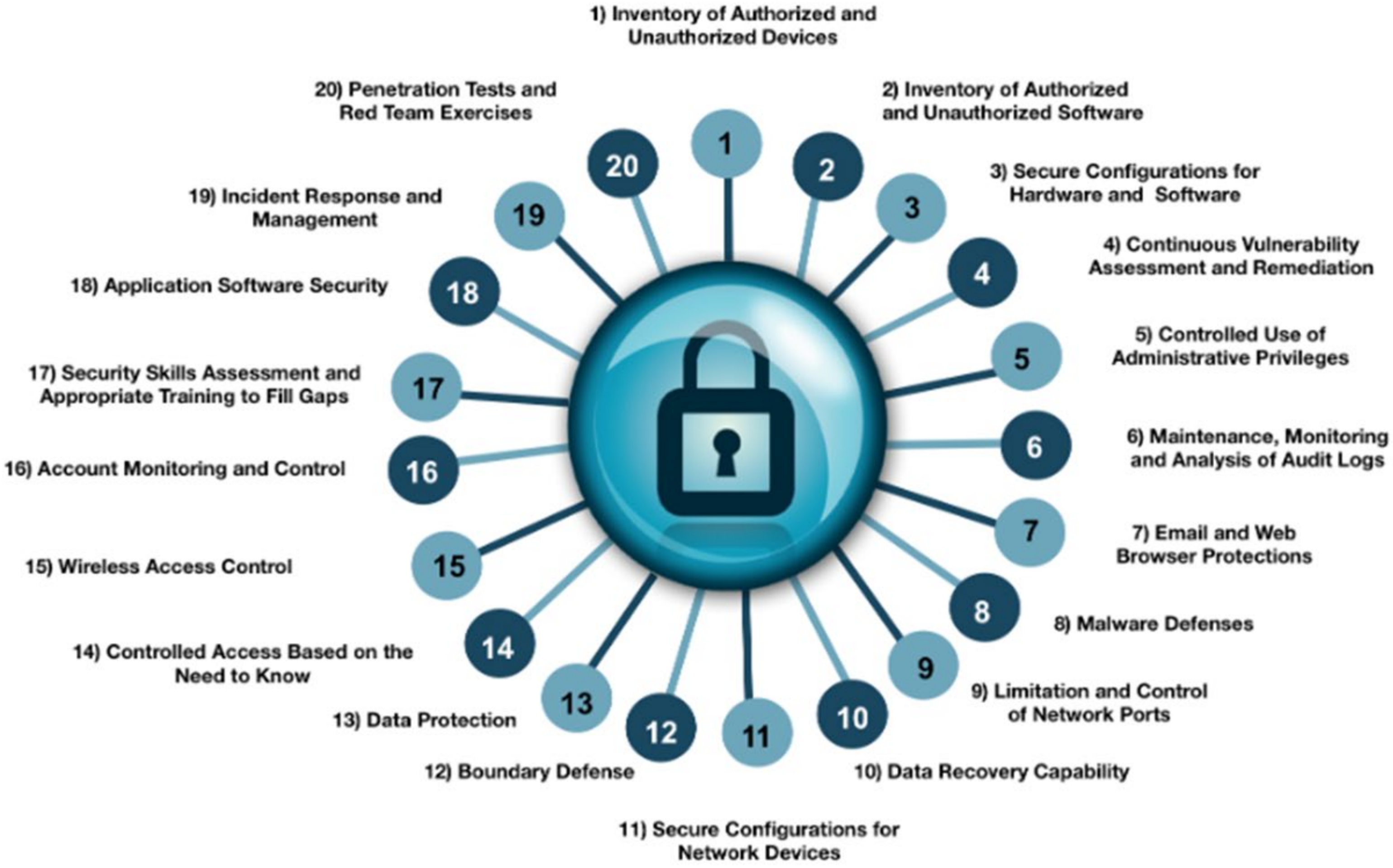
Cyber Risk Scenario Guidelines

1. ***Low Risk Scenarios****? If a proposed cyber risk scenario's inherent risk rating is within company risk tolerance (i.e., within "grey box" normal range of risk), then no scenario will be created.*
2. ***Duplicate Risk?*** *Each cyber risk scenario will stand-alone and be mutually exclusive from all others, preventing "double counting" when risk and controls have been captured within an existing cyber scenario.*
3. ***Are we able to Aggregate?*** *Apply cyber risk aggregation guidelines as "guardrails" to ensure that risk exposures are not aggregated to the extent that new Continuous Cyber Risk Identification KRI's can no longer be mapped to distinct threat actors, threat vectors, impact types, affected assets, and mitigating controls.*
4. ***Aligned with Strategy?*** *If the scenario is within the normal range of cyber risk, then we will monitor the risk through the continuous cyber risk identification process. If out of tolerance, then a Cyber Risk Discussion Group will convene.*

Technical Controls

Control Categories

- Very Weak
- Weak
- Strong
- Very Strong



1) Inventory of Authorized and Unauthorized Devices

2) Inventory of Authorized and Unauthorized Software

3) Secure Configurations for Hardware and Software

4) Continuous Vulnerability Assessment and Remediation

5) Controlled Use of Administrative Privileges

6) Maintenance, Monitoring and Analysis of Audit Logs

7) Email and Web Browser Protections

8) Malware Defenses

9) Limitation and Control of Network Ports

10) Data Recovery Capability

11) Secure Configurations for Network Devices

12) Boundary Defense

13) Data Protection

14) Controlled Access Based on the Need to Know

15) Wireless Access Control

16) Account Monitoring and Control

17) Security Skills Assessment and Appropriate Training to Fill Gaps

18) Application Software Security

19) Incident Response and Management

20) Penetration Tests and Red Team Exercises