



National
Security
Agency



Cybersecurity and
Infrastructure
Security
Agency

Joint Cybersecurity Advisory

TLP:CLEAR

NSA and CISA Red and Blue Teams Share Top Ten Cybersecurity Misconfigurations

A plea for network defenders and software manufacturers to fix common problems.

Executive summary

The National Security Agency (NSA) and Cybersecurity and Infrastructure Security Agency (CISA) are releasing this joint cybersecurity advisory (CSA) to highlight the most common cybersecurity misconfigurations in large organizations, and detail the tactics, techniques, and procedures (TTPs) actors use to exploit these misconfigurations.

- https://media.defense.gov/2023/Oct/05/2003314578/-1/-1/0/JOINT_CSA_TOP_TEN_MISCONFIGURATIONS_TLP-CLEAR.PDF

Top Ten Cybersecurity Misconfigurations

- 1.** Default configurations of software and applications
- 2.** Improper separation of user/administrator privilege
- 3.** Insufficient internal network monitoring
- 4.** Lack of network segmentation
- 5.** Poor patch management
- 6.** Bypass of system access controls
- 7.** Weak or misconfigured multifactor authentication (MFA) methods
- 8.** Insufficient access control lists (ACLs) on network shares and services
- 9.** Poor credential hygiene
- 10.** Unrestricted code execution

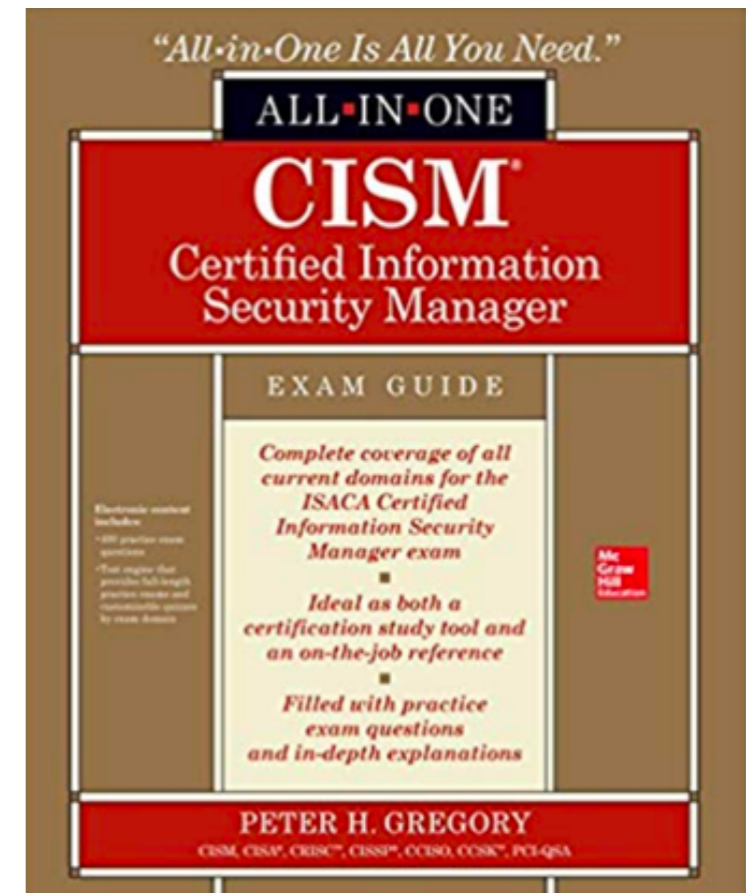
Extra Credit Quiz in Canvas

CNIT 160: Cybersecurity Responsibilities

3. Information Risk Management Part 4

Pages 158 - 182

Revised 10-11-23



Topics

- **Part 1 (p. 102 - 115)**
 - **Risk Management Concepts**
 - **Implementing a Risk Management Program**
- **Part 2 (p. 114 - 125)**
 - **The Risk Management Life Cycle**
- **Part 3 (p. 125 - 158)**
 - **The Risk Management Life Cycle**
- **Part 4 (p. 158 - 182)**
 - **Operational Risk Management**

Operational Risk Management

- **Concerned with financial losses and survival of an organization**
- ***Operational risk is***
 - **Risk of loss resulting from**
 - **Failed controls, processes, and systems**
 - **Internal and external events**
 - **Other occurrences that impact business systems**

Recovery Objectives

- **Time intervals for**
 - **Business resiliency and recovery**
 - **From security and disaster events**
- **Pay attention to third-party risk**
 - **More difficult to obtain usable risk information**

Risk Register

- **The key business record in risk management**
- **Log of historic and newly identified risks**
- **Contains risk metadata about each risk**
 - **Helps understand which risks are more serious than others**

Risk Management Objectives

Risk Management Objectives

- **Recovery Time Objective (RTO)**
- **Recovery Point Objective (RPO)**
- **Recovery Capacity Objective (RCapO)**
- **Service Delivery Objective (SDO)**
- **Maximum Tolerable Downtime (MTD)**
- **Maximum Tolerable Outage (MTO)**
- **Service Level Agreements (SLA)**

Recovery Time Objective (RTO)

- **The period of time from the onset of an outage until the resumption of service**
- **Different processes have different RTO's**
- **The RTO may vary with time**
 - **Point-of-sale terminals**
 - **Short RTO during peak business hours**
 - **Longer RTO at other times**

RTO Considerations

- **RTO is interrelated with**
 - **Data classification**
 - **Asset classification**
- **Processes with short RTO's**
 - **Likely to have data and assets that are classified as operationally critical**

Establishing RTOs

- **Security managers interview**
 - **Personnel in middle management**
 - **Senior and executive management**
- **Executive prioritization prevails**
- **RTOs come from Business Impact Analysis (BIA)**
 - **A cornerstone in Business Continuity Planning (BCP)**

Recovery Point Objective (RPO)

- **The period of acceptable data loss**
 - **From an incident or disaster**
- **Period between backups or data replication**
- **Shorter RPOs have higher costs**

Recovery Capacity Objective (RCapO)

- **Capacity of a temporary or recovery process**
- **A percentage of the normal process**
 - **Example: hand-writing paper receipts might mean that cashiers do 80% as much work**

Service Delivery Objective (SDO)

- **Level or quality of service**
 - **Required after an event**
 - **Compared to normal operation**
- **Measured in transaction throughput, response time, available capabilities and features, etc.**
- **SDO, RTO, RPO, and RCapO are all related**

Maximum Tolerable Downtime (MTD)

- **Theoretical time period**
 - **Measured from start of a disaster**
 - **After which the organization's ongoing viability would be at risk**
- **Organizations may start with MTD**
 - **And then derive RTO, RPO, and RCapO**
- **MTD is also called *Acceptable Interruption Window (AIW)***

Maximum Tolerable Downtime (MTD)

- **Different for each major business function**
 - **Ex: MTD is 7 days for website, but 28 days for payroll**

Maximum Tolerable Outage (MTO)

- **Maximum period of time**
 - **That organization can tolerate operating in recovery mode**
- **Example: CCSF has two layers of firewalls**
 - **When one fails, we operate with a reduced level of security**

Service Level Agreements (SLA)

- **A written agreement**
 - **Specifies quantity of work, quality, timeliness**
 - **And remedies for shortfalls**

Risk Management and Business Continuity Planning (BCP)

Similarities

- **Risk Management and BCP both**
 - **Seek to discover risks and remedies**
 - **Rely on risk assessments**
 - **Can rely on Business Impact Analysis (BIA)**
 - **Identify threats that can lead to disasters**

Third-Party Risk Management (TPRM)

Third-Party Risk Management (TPRM)

- **Activities to discover and manage risk**
 - **Associated with external organizations**
 - **Performing operational functions**
- **Outsourcing to the cloud**
 - **Software as a Service (SaaS)**
 - **Platform as a Service (PaaS)**

Third-Party Risk Management (TPRM)

- **Complexities in identifying risks in third-party organizations**
- **Must solicit information to identify risks**
 - **Outside of organization's direct control**
- **More than half of all breaches come through third parties**

Cloud Service Providers

- **Operational Responsibility**

Component	On-Premise	IaaS	PaaS	SaaS
Applications	Org	Org	Org	Provider
Data	Org	Org	Org	Provider
Runtime	Org	Org	Provider	Provider
Middleware	Org	Org	Provider	Provider
Operating system	Org	Org	Provider	Provider
Virtualization	Org	Provider	Provider	Provider
Servers	Org	Provider	Provider	Provider
Storage	Org	Provider	Provider	Provider
Networking	Org	Provider	Provider	Provider
Data center	Org	Provider	Provider	Provider

Cloud Service Providers

- **Security Responsibility**

Activity	On-Premise	IaaS	PaaS	SaaS
Human resources	Org	Shared	Shared	Provider
Application security	Org	Org	Shared	Provider
Identity and access management	Org	Org	Shared	Provider
Log management	Org	Org	Shared	Provider
System monitoring	Org	Org	Shared	Provider
Data encryption	Org	Org	Shared	Provider
Host intrusion detection	Org	Org	Shared	Provider
Host hardening	Org	Org	Shared	Provider
Asset management	Org	Org	Shared	Provider
Network intrusion detection	Org	Org	Provider	Provider
Network security	Org	Org	Provider	Provider
Security policy	Org	Shared	Shared	Provider
Physical security	Org	Provider	Provider	Provider

TPRM Life Cycle

- **Initial Assessment**
- **Legal Agreement**
- **Classifying Third Parties**
- **Questionnaires and Evidence**
- **Assessing Third Parties**
- **Risk Mitigation**

Initial Assessment

- **Evaluate third party for suitability**
- **Often competitive**
- **Often requires each third party to provide information**
 - **Through a Request for Information (RFI)**
 - **Or a Request for Proposal (RFP)**
 - **Often including sections on security and privacy**

Legal Agreement

- **Describes**
 - **Services provided**
 - **Service levels**
 - **Quality, pricing, other terms**

Legal Agreement

- **Security and privacy section**
 - **Formal security and/or privacy program**
 - **Security and/or privacy controls**
 - **Vulnerability assessments**
 - **External audits and certifications**
 - **SOC1, SOC2, ISO 27001, HITRUST, PCI ROCs, etc.**
- **Formal incident response capability**

Legal Agreement

- **Security and privacy section**
 - **Security incident notification**
 - **Must notify organization within a specific time frame, typically 24 hours**
 - **Careful language around "suspected" and "confirmed"**
 - **Ex: Uber concealed a ransomware incident by calling it a "Bug Bounty"**

Legal Agreement

- **Security and privacy section**
 - **Right to Audit**
 - **Periodic review**
 - **Annual due diligence**
 - **Questionnaires and evidence**
- **Cyber insurance**

Classifying Third Parties

- **Wide range of risk among third parties**
- **Risk level depends on what services are used**
- **Risk level may change as more functions are outsourced**


Questionnaires and Evidence

- **Questionnaires to periodically assess third parties**
- **Can also request Evidence**
 - **Specific artifacts to support the questionnaire responses**

PCI-DSS

ASSESSING THE SECURITY OF YOUR CARDHOLDER DATA

Ideal for small merchants and service providers that are not required to submit a report on compliance, a Self-Assessment Questionnaire (SAQ) is designed as a self-validation tool to assess security for cardholder data.

 pcisecuritystandards.org/pci_security/completing_self_assessment



Complete Your Assessment

There are two components to the Self-Assessment Questionnaire:

1. A set of questions corresponding to the PCI Data Security Standard requirements designed for service providers and merchants.
2. An Attestation of Compliance or certification that you are eligible to perform and have performed the appropriate Self-Assessment.
An appropriate Attestation will be packaged with the Questionnaire that you select.

Typical Artifacts

- **Security policy**
- **Security controls**
- **Security awareness training records**
- **New-hire checklists**
- **Details on employee background checks (not necessarily actual records but a description of the checks performed)**
- **Nondisclosure and other agreements signed by employees (not necessarily signed copies but blank copies)**
- **Vulnerability management process**
- **Secure development process**
- **Copy of general insurance and cyber insurance policies**
- **Incident response plan and evidence of testing**

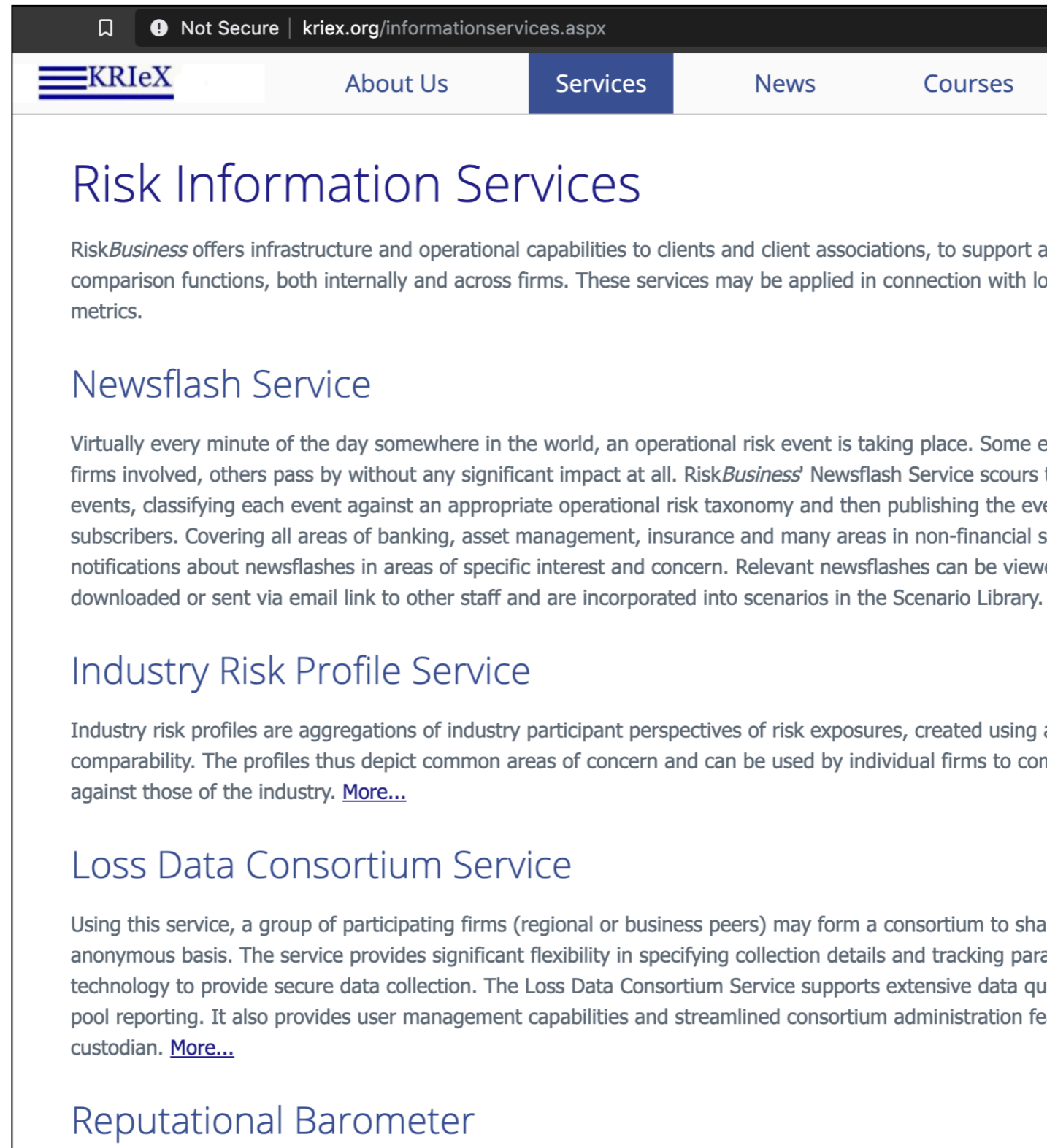
Assessing Third Parties

- **Required at the onset of the business relationship**
- **And periodically thereafter**
- **Assess**
 - **IT and security controls, and**
 - **Other information on next slide**

Other Information

- **Financial risk**
- **Geopolitical risk**
- **Inherent risk**
- **Recent security breaches**
- **Lawsuits**
- **Operational effectiveness/capabilities**

Risk Information Services



The screenshot shows a web browser window with the address bar displaying 'kriex.org/informationsservices.aspx'. The website header includes the KRIeX logo and navigation links for 'About Us', 'Services', 'News', and 'Courses'. The main content area is titled 'Risk Information Services' and contains several service descriptions:

Risk Information Services

RiskBusiness offers infrastructure and operational capabilities to clients and client associations, to support a comparison functions, both internally and across firms. These services may be applied in connection with lo metrics.

Newsflash Service

Virtually every minute of the day somewhere in the world, an operational risk event is taking place. Some e firms involved, others pass by without any significant impact at all. *RiskBusiness'* Newsflash Service scours t events, classifying each event against an appropriate operational risk taxonomy and then publishing the eve subscribers. Covering all areas of banking, asset management, insurance and many areas in non-financial s notifications about newsflashes in areas of specific interest and concern. Relevant newsflashes can be viewe downloaded or sent via email link to other staff and are incorporated into scenarios in the Scenario Library.

Industry Risk Profile Service

Industry risk profiles are aggregations of industry participant perspectives of risk exposures, created using a comparability. The profiles thus depict common areas of concern and can be used by individual firms to con against those of the industry. [More...](#)

Loss Data Consortium Service

Using this service, a group of participating firms (regional or business peers) may form a consortium to sha anonymous basis. The service provides significant flexibility in specifying collection details and tracking para technology to provide secure data collection. The Loss Data Consortium Service supports extensive data qu pool reporting. It also provides user management capabilities and streamlined consortium administration fe custodian. [More...](#)

Reputational Barometer

Risk Mitigation

- **Often, third parties have unacceptable practices**
 - **Such as lacking annual security awareness training or encryption**
- **Possible responses**
 - **Convince third-party to change processes**
 - **They may refuse because of the expense**

Kahoot!

Ch 3d-1

The Risk Register

Risk Register

- **Contains information about business risks**
 - **And information about**
 - **Origin**
 - **Potential impact**
 - **Affected assets**
 - **Probability of occurrence**
 - **Treatment**

Risk Register

- **Central business record in an organization's risk management program**
- **Focal point of evidence**
 - **That an organization is at least attempting to manage risk**

Typical Risk Register Entry

Item	Description
Entry number	A unique numeric value identifying the entry. This can be in the form of a date, such as 20180127a.
Status	Current status of the entry. <ul style="list-style-type: none">• Open• Assigned• Closed
Date entered	The date the risk register entry was created.
Entered by	The person who created the risk register entry.
Source	The activity or event that compelled someone to create this entry. Sources include the following: <ul style="list-style-type: none">• Risk assessment• Vulnerability assessment• Security incident• Threat intelligence• External party
Incident number	Reference to an incident record, if applicable.
Title	Short title describing the risk entry.
Description	Description of the risk.
Threat description	Description of the potential threat activity.

Typical Risk Register Entry

Threat actor	Description of the type of threat actor: <ul style="list-style-type: none">• Worker• Former worker• Supplier, vendor, or partner• Cybercriminal• Nation-state
Vulnerability description	Description of one or more vulnerabilities that increases the probability or impact of threat realization.
Third-party organization	Name of the third-party organization where the risk is present, if applicable.
Third-party classification	Classification level of the third-party organization, if applicable.
Business impact	Business language description of the impact of threat realization.
Technical impact	Technical language description of the impact of threat realization, if applicable.
Asset	The specific asset, asset group, or asset class affected by the risk.
Asset owner	The owner of the affected asset.
Risk owner	The owner of the risk.
Control group	A reference to the affected control group, if applicable.
Control	A reference to the affected control, if applicable.
Process	A reference to the affected process, if applicable.
Untreated probability of occurrence	An estimate of the probability of occurrence of the threat event associated with the risk. Usually expressed as high, medium, or low or on a numeric scale such as 1 to 5.

Typical Risk Register Entry

Untreated impact of occurrence	An estimate of the impact of occurrence of the threat event associated with the risk. Usually expressed as high, medium, or low or on a numeric scale such as 1 to 5.
Untreated risk score	An overall risk score that is generally a product of probability, impact, and asset value.
Treated probability of occurrence	An estimate of the probability of occurrence of the threat event associated with the risk, after risk treatment. Usually expressed as high, medium, or low or on a numeric scale such as 1 to 5.
Treated impact of occurrence	An estimate of the impact of occurrence of the threat event associated with the risk, after risk treatment. Usually expressed as high, medium, or low or on a numeric scale such as 1 to 5.
Treated risk score	An overall risk score that is generally a product of probability, impact, and asset value, after risk treatment.
Estimated cost of risk treatment	An estimated cost of risk treatment. This is expressed in dollars or the local currency.
Estimated level of effort of risk treatment	An estimated level of effort of risk treatment. This can be expressed as high, medium, or low or on a numeric scale such as 1 to 5 or as an estimate of range of man-hours, as follows: <ul style="list-style-type: none">• Less than 1 hour• Less than 10 hours• Less than 100 hours• Less than 1,000 hours• Less than 10,000 hours

Typical Risk Register Entry

Risk treatment	The chosen method of risk treatment: <ul style="list-style-type: none">• Accept• Mitigate• Transfer• Avoid
Risk treatment approver	The person or body that approved the risk treatment method.
Risk treatment approval date	The date that the risk treatment method was approved.
Risk treatment owner	The person responsible for carrying out risk treatment.
Risk treatment description	A description of the risk treatment.
Risk treatment planned completion	Date when risk treatment is expected to be completed.
Actual cost of risk treatment	The actual cost of risk treatment, which would be known when risk treatment has been completed. This is expressed in dollars or the local currency.
Actual level of effort of risk treatment	The actual level of effort of risk treatment, which would be known when risk treatment has been completed. This is expressed in man-hours.
Risk treatment closure date	Date when risk treatment is actually completed.

Sources of Information for the Risk Register

- **Risk assessment**
- **Vulnerability assessment**
- **Internal audit**
- **Security incident**
- **Threat intelligence**
- **Industry development**
- **New laws and regulations**
- **Consultants**

Strategic vs. Tactical Risks

- **Strategic risks belong in the risk register**
 - **Affect the entire organization**
 - **Ex: a systemic problem with server patching**
 - **Third party risks belong in the risk register**
- **Tactical risks do not belong in the risk register**
 - **Tactical: associated with individual assets**
 - **Such as complete vulnerability scans**

Risk Analysis Contribution

- **Detailed risk analysis required for each entry in the risk register**
- **For example: software development team continues to produce defective code**
 - **Possible remedies on next two slides**

Possible Remedies

- **Secure development training**
- **An incentive program that rewards developers who produce the fewest security defects**
- **Code scanning tools present in each developer's integrated development environment (IDE)**
- **Code scanning tools in the organization's software build system**

Possible Remedies

- **Periodic application penetration tests performed by a qualified external party**
- **Web application firewall appliances**
- **Web application firewall in the organization's content delivery network (CDN) service**

Residual Risk

- **Even after risk treatment, some risk remains**
- **An individual risk may undergo two or more cycles of treatment**
- **Until the residual risk is accepted**

Integration of Risk Management into Other Processes

Integration of Risk Management into Other Processes

- **Software development**
- **Change management**
- **Configuration management**
- **Incident and problem management**
- **Physical security**
- **Enterprise risk management**
- **Human resource management**
- **Project management**

Secure Software Development

- **Threat modeling during design phase**
- **Coding standards, specifying allowed and disallowed techniques**
- **Code reviews**
- **Code scanning**
- **Application scanning**
- **Application penetration testing**

Change Management

**Begins
with
*formal
request
for
change***

- **Description of the change**
- **Reason for the change**
- **Who will perform the change**
- **When will the change be performed**
- **A procedure for making the change**
- **A procedure for verifying the change**
- **A back-out procedure in case the change cannot be verified**
- **Security impact of the change and also of not implementing the change**
- **Privacy impact**
- **Dependencies**
- **Defined change windows**

Change Management

- ***Change review board* discusses change requests**
- **Often includes security personnel**

Configuration Management

- **Usually uses automated tools**
- **Configuration management database (CMDB)**
 - **Repository of this information**
- **Security considerations**
 - **Protecting configuration data from unauthorized access**
 - **Inclusion of security-related information in configuration management data**

Incident and Problem Management

- **Incidents and problems include outages, errors, bugs, etc.**
- **Four security considerations**
 1. **Personnel analyzing a problem need to understand its security impacts**
 - **Ex: malfunctioning firewall**
 2. **Actions taken to restore service may have security impacts**
 - **Ex: rebooting a server**

Incident and Problem Management

3. Root-cause analysis may have security impacts

- **Ex: file permission changes**

4. Corrective action may have security impacts

- **Ex: elevating a service account privileges**

Physical Security

- **Integrating information and physical security**
 - **Ensure that risk and threat assessments, BCP, and DRP cover both areas**
 - **Include both on the risk register**
 - **Ensure that high-availability systems have appropriate physical security**

Physical Security

- **Integrating information and physical security**
 - **Incorporate IT-based physical security assets into**
 - **Overall technology and security architecture**
 - **Information and asset classification**
 - **Identity and access management program**

Physical Security

- **Integrating information and physical security**
- **Ensure that SCADA and ICS systems monitor and control the environmental systems (heating, ventilation, and air conditioning)**

Information Risk and ERM (Enterprise Risk Management)

- **ERM has its own risk register**
 - **For business-specific risks**
- **It may make sense to use a common risk register for both information risk and ERM**

Human Resource Management

- **Background checks**
- **Legal agreements**
- **Training**
- **Development**
- **Management of the Human Resource Information System (HRIS)**
 - **Often integrated with Identity and Access Management (IAM) platform**

Project Management

- **At onset of a project, perform a risk analysis**
- **Establish impact on security, compliance, and privacy before implementing a project**
- **Verifiable security requirements need to be included in any activity where requirements are developed**

Risk Monitoring and Reporting

Risk Monitoring and Reporting

- **Typical activities:**
 - **Internal audit**
 - **Control self-assessment**
 - **Vulnerability assessment**
 - **Risk assessment**
- **Primary audience is executive management**
 - **Often done with dashboards**

Key Risk Indicators



Key Risk Indicators (KRIs)

- **Measure of information risk**
- **Used to reveal trends**
- **Often derived from operational activities**
 - **Examples:**
 - **Number of vulnerabilities found (useless to executives)**
 - **Time to remediate critical vulnerabilities (better)**

Other KRIs

- **Number of security incidents resulting in external notifications**
- **Changes in attrition rates for IT workers and for key business employees**
- **Amount of money paid out each quarter in an organization's bug bounty program**
- **Percentage of employees who have not completed the required security training**
- **Numbers of critical and high risks identified in risk assessments**

Training and Awareness

Factors

- **Lack of awareness of the risks associated with general computing and Internet use**
- **Lack of training and experience in the configuration and operation of systems and applications**
- **Lack of training and awareness of key business processes and procedures**
- **Lack of information on workers' responsibilities for reporting problems and incidents**

Risk Documentation

Risk Documentation

- **Policy and objectives, such as how risk management is run in the organization**
- **Roles and responsibilities, such as who is responsible for various activities**
- **Methods and techniques, such as how probability and impact of risks are evaluated and scored**
- **Locations for data storage and archival, such as where the risk register and risk treatment records reside**

Risk Documentation

- **Risk tolerance, such as how acceptable and unacceptable risks are defined**
- **Business rules for why something is included in the risk register**
- **Risk treatment procedures and records**
- **Procedures and methods for the development of metrics and key risk indicators**
- **Communication and escalation protocols defined**
- **Review cycle defined to be sure the program is in alignment with the business**

Kahoot!

Ch 3d-2