Risk Analysis, Frameworks, and Standards

Loic Niragire

School of Technology, Northcentral University

TIM 7030: Managing Risk, Security, & Privacy in Information Systems

Dr. Gabe Goldstein

August 27th, 2023

This is an exploration of IT security risk analysis, frameworks, and standards. The aim is to raise security awareness and help technologists integrate appropriate security options and secure practices throughout an organization. It provides an overview of risk management and the steps that must be implemented by an organization to develop a risk management plan. For illustration purposes, the outcome of this exploration is applied to a fictitious organization called ABC Financials, which handles recurrent customer payments through various payment methods such as credit cards, ACH, and digital currency. ABC Financials maintains integration points with third-party systems to exchange sensitive personal and financial data to onboard new customers through an electronic application process.

The success of ABC Financials heavily relies on its credibility across the country. Customers expect the utmost safeguard of their sensitive data during and after their journey with the organization. Therefore, ABC Financials operates on a Zero Trust Security policy to guard against internal and external network security threats. Although protecting network resources provides a crucial line of defense, bad actors will eventually find loopholes to explore without adequate awareness of the organization's threats and their impact.

A comprehensive security measure across the organization requires individuals at all levels to understand their roles in protecting the organization. This entails a mindset shift in most organizations where security is viewed as a concern for security teams rather than a shared responsibility. Moreover, it requires executive buy-in for allocating the necessary resources and emphasizing the importance of security across the organization.

An Overview of Risk and Risk Management

Risk is the likelihood of a threat actor taking advantage of a vulnerability by using a threat against an IT system asset. Thus, organizations continuously strive to identify and categorize risks and then systematically put controls in place to manage them, minimizing their impact on the organization. This process requires balancing business functionality and security

due to limited resources – the more functionality, the less security, and vice versa. Security professionals aim to increase the system's confidentiality, integrity, and availability to protect the most important assets of an organization.

Any IT infrastructure with a tangible or intangible value to the organization is considered an asset, such as servers, workstations, applications, data, or personnel. Assets have inherent weaknesses that can leave them open to a threat. Likewise, a threat actor is anyone or anything with a motive and resources to attack an organization's asset. Examples of threat actors include hackers, script kiddies, competitors, or shadow IT. Risk management entails calculating the probability of someone or something damaging assets over a defined period.

By using security controls, actions can be taken to strengthen an asset's vulnerability to reduce or eliminate the corresponding threat. However, security controls do not dictate how to perform the steps to mitigate a threat, only that they must be performed. Hence, applying security controls in an organization is a complex process involving countless security controls to be applied. Luckily, by using Risk Management Frameworks, IT security teams can leverage industry-established knowledge to simplify this process. A Risk Management Framework (RMF) consists of well-defined steps to help an organization make informed decisions about the security controls and measures that must be implemented. In other words, organizations use one or more frameworks to apply various security controls. Table 1 lists a sample of RMFs published by several organizations and governing bodies across the globe.

Table 1. A sample of risk management frameworks

Organizations	Frameworks	Description
The National Institute of Standards and Technology (NIST)	NIST Risk Management Framework (NIST RMF)	Provides guidelines for applying the Risk Management Framework to federal information systems
The National Institute of	NIST Cybersecurity	Standards, guidelines, and

Standards and Technology (NIST)	Framework (CSF)	best practices to manage cybersecurity-related risks. Geared towards private industry.
International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC)	ISO/IEC 27005	Provides guidelines for information security management systems
International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC)	ISO/IEC 27002	The international standard to help organizations define their security controls by categorizing controls.
Information Systems Audit and Control Association (ISACA)	Risk IT Framework	Designed to help organizations understand and manage IT risk
Committee of Sponsoring Organizations of the Treadway Commission (COSO)	COSO Enterprise Risk Management (ERM) Framework	Widely used for risk management across various domains, including IT. It emphasizes aligning risk management with business strategy.
The Open Group	Factor Analysis of Information Risk (FAIR)	Provides a model for understanding, analyzing, and quantifying information risk in financial terms.
Center for Internet Security (CIS)	CIS Risk Assessment Method (CIS RAM)	A risk assessment method aligned with CIS controls

The types of security controls an organization uses result from industry regulations and laws such as the Patriot Act (2001), the Electronic Communications Privacy Act of 1986 (ECPA), the Computer Security Act of 1987, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and the Sorbanes-Oxley Act of 2002 (SOX). Similarly, the European Union (EU) created the General Data Protection Regulation (GDPR) to protect the privacy of any EU citizen visiting websites globally. Security controls are also affected by industry standards established to provide uniform products and services. For instance, the Payment Card

Industry Data Security Standard (PCI DSS) provides detailed security controls to mitigate credit card fraud in organizations processing credit card, debit card, or gift card transactions.

To develop a risk management plan, organizations must first conduct a risk assessment using frameworks such as NIST SP 800-30 or the Risk IT Framework from ISACA. The assessment helps the organization uncover potential risks by identifying threat sources and events, vulnerabilities, the likelihood of occurrence, and the magnitude of impact. Then, the organization decides how to respond to uncovered risks.

NIST CSF

The NIST Cybersecurity Framework has five core functions: Identify, Protect, Detect, Respond, and Recover. These functions are broken down into categories and sub-categories to provide a structured and granular approach to cybersecurity (The National Institute of Standards and Technolody, 2023). Table 2 illustrates a breakdown of each function into categories and action items to align ABC Financials with NIST CSF.

Table 2. NIST CSF Cores Functions, categories, and sub-categories

Core Functions	Categories	Action items
Identify	Asset Management	Create an inventory of all hardware, software, and data, and personnel who have access to them.
	Business Environment	Understand the business context, strategy, and cybersecurity requirements.
	Governance	Develop a governance model for cybersecurity governance, aligned with business objectives.
Protect	Access control	Implement robust access control mechanisms, possibly including Multi-Factor Authentication (MFA).
	Data security	Ensure that sensitive data is encrypted both at rest and in

		transit.
	Security Training	Conduct regular security awareness training for all employees.
Detect	Anomaly detection	Develop intrusion detection and prevention systems (IDPS) and Security Information and Event Management (SIEM) for real time monitoring.
	Security Audits	Regularly audit the security settings and logs to detect any unauthorized activity.
Respond	Incident Response Plan	Develop a comprehensive incident response plan detailing procedures for different types of cybersecurity incidents.
	Communication Plan	Establish a communication plan for internal and external stakeholders in case of security incident.
Recover	Recovery Plan	Develop a disaster recovery and business continuity plan.
	Improvements	After a security incident, identify lessons learned and areas for improvement.

NIST RMF

The NIST Risk Management Framework (RMF) consists of a six-step process as illustrated in Table 3. Its implementation is a continuous process that involves ongoing monitoring and periodic reauthorization (The Nation Institure of Standards and Technology, 2023)

Table 3. NIST RMF implementation details

Step	Categories	Action Items
Prepare	Establish Context	Understand the organizational context, risk tolerance, and the resources that the RMF will be applied to.
	Resource Allocation	Allocate necessary resources including personnel, technology,

		and budget.
Categorize	Identify Information Types	Categorize the type of information processed, stored, and transmitted by the information system.
	System Categorization	Based on the information types, categorize the system as low, moderate, or high impact.
Select	Baseline Controls	Select a set of security controls that are tailored to the categorization od the system.
	Tailoring	Modify the baseline controls to fit the specific needs and risks of the organization.
Implement	Control implementation	Implement the selected security controls.
	Documentation	Document the implementation details, including configurations and justifications for any tailoring.
Assess	Assessment Plan	Develop and implement plans to assess the security controls to ensure they are functioning correctly.
	Assessment Reports	Generate reports based on the assessments and identify any weaknesses or deficiencies.
Authorize	Authorization Package	Compile all documentation, including the security package and assessment reports.
	Authorization Decision	Review the package and make a risk-based decision to authorize the system.
Monitor	Continuous Monitoring	Implement continuous monitoring strategies to keep track of the security state of the information system.
	Incident Response	Develop and implement an incident response plan for addressing any security incidents.

PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is essential for organizations that store, process, or transmit credit card data. ABC Financials can implement PCI DSS in seven steps.

Table 4. PCI DSS implementation details

Step	Categories	Action items

Scoping and analysis	Scope definition	Identify all systems, processes, and personnel that store, process, or transmit cardholder requirements.
	Gap analysis	Conduct a gap analysis to identify areas where the organization does not meet PCI DSS requirements.
Remediation	Data cleanup	Remove any stored cardholder data that is not needed.
	System hardening	Implement security measures such as firewalls, intrusion detection systems, and encryption to protect cardholder data.
	Access control	Implement strong access control measures, including Multi-Factor Authentication (MFA) and least-privilege access.
	Vendor management	Ensure that third-party service providers comply with PCI DSS.
Policy and procedure development	Policy framework	Develop a set of security policies and procedures that align with PCI DSS requirements.
	Incident response plan	Develop and document procedures for responding to security incidents.
Implementation and training	Implement controls	Deploy the necessary technologies and processes to meet PCI DSS requirements.
	Employee training	Conduct training to ensure that employees are aware of their roles and responsibilities in protecting cardholder data.
Assessment	Self-assessment	Depending on the volume of transactions and the way cardholder data is processed, either complete a Self-Assessment Questionnaire (SAQ) or hire a Qualified Security Assessor (QSA) to perform an audit.
	Vulnerability scans and penetration testing	Conduct regular scans and tests to identify vulnerabilities.
Reporting and attestation	Report on compliance (ROC)	If a QSA performed the audit, a ROC will be generated. If self-assessed, complete the relevant SAQ
	Attestation of Compliance (AOC)	Submit the AOC to the acquiring bank and card brands with whom

		you do business.
Ongoing maintenance	Continuous monitoring	Implement monitoring mechanism like log reviews and regular scans.
	Quarterly scans	Conduct quarterly vulnerability scans using Approved Scanning Vendors (ASVs).
	Annual reassessment	Conduct annual assessments to ensure ongoing compliance

References

The Nation Institure of Standards and Technology. (2023, August 25). *NIST Risk Management Framework.* Retrieved from csrc.nist.gov: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

The National Institute of Standards and Technolody. (2023, August 25). *Framework for Improving Critical Infrastructure Cybersecurity.* Retrieved from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf