# Cybersecurity Frameworks, Models, Standards, and Laws

Loic Niragire

School of Technology, Northcentral University

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

Dr. Gabe Goldstein

September 27th, 2023

In an era of ubiquitous digitalization, cybersecurity is not merely an IT concern but a critical business imperative. Organizations must safeguard sensitive data and ensure the integrity and availability of various business processes. The cybersecurity landscape becomes more complex and fraught with risk for companies handling recurrent customer payments across multiple channels such as credit cards, Automated Clearing House (ACH), and digit currencies.

This paper aims to inform the creation of an improved approach to cybersecurity with ABC Financials. It seeks to discern the relevance and importance of frameworks, models, standards, and roles in managing cybersecurity risk effectively. Our organization complies with the Payment Card Industry Data Security Standard (PCI DSS), so this paper will go beyond essential compliance to enhance cybersecurity practices. It will incorporate considerations related to regulations such as GDPR, KYC/AML, and standards like ISO/IEC 27002, explicitly tailoring recommendations to align with these additional layers of complexity.

As we aspire not only to sustain but also scale out operations, this paper serves as a strategic document aimed at upper management and C-level executives. It aims to provide a roadmap for immediate, medium-term, and long-term objectives, each with actionable insights. The paper will delve into the current regulatory landscape, evaluate our cybersecurity posture, and present a multi-tiered strategy encompassing Immediate Actions, Medium-term Strategies, and Long-term Vision for strengthening our cybersecurity measures.

## Regulatory Landscape

Before delving into the specifics of our cybersecurity strategy, it is crucial to understand the external regulatory frameworks and standards that shape our cybersecurity obligations and best practices. These regulations and guidelines are legal necessities and serve as a structured pathway to achieve robust cybersecurity. By comprehending these key directives, upper management and C-level executives can make more informed decisions concerning resource allocation, risk management, and strategic planning in cybersecurity.

## PCI DSS

Given our compliance with the Payment Card Industry Data Security Standard (PCI DSS), it serves as a starting point for cybersecurity infrastructure. PCI DSS is critical for any organization that handles credit card transactions and provides a robust framework for securing cardholder data. While this standard has stringent rules, it should be perceived as a minimum baseline because compliance should not be equated to a comprehensive security measure (Williams, 2013).

## GDPR

The General Data Protection Regulation (GDPR) imposes strict regulations on the handling and storage of personal data for EU citizens. Non-compliance could result in significant fines and reputational damage. This regulation compels us to employ data minimization techniques, provide data portability, and ensure robust data protection measures (Duncan, 2019). While we do not currently offer services in Europe, the GDPR has set a global data protection standard that other jurisdictions are increasingly adopting or considering (Greenleaf, 2019). Moreover, compliance with GDPR could be a prerequisite for future international expansion. Adherence to GDPR guidelines demonstrates our commitment to stringent data protection measures.

### KYC/AML

KYC and AML are regulatory frameworks that mandate the comprehensive identification, verification, and monitoring of customers, especially in financial transactions (Sadiq, Governatori, & Namiri, 2008). These regulations aim to prevent identity theft, financial fraud, and money laundering, and they require the institution to maintain extensive records of customer activities.

### ISO/IEC 27002

Although not a regulatory requirement, ISO/IEC 27002 provides best practice recommendations on information security controls (Solms & Niekerk, 2013). Adherence to this standard can serve as a testament to our commitment to maintaining a high level of security and can be a differentiating factor in competitive markets.

### Industry-Specific Threats

In addition to these frameworks and regulations, our organization faces threats specific to companies that handle multiple customer payments, including credit cards, ACH, and digital currencies. These range from card skimming to more complex threats like Advanced Persistent Threats (APTs) targeting financial data (Tankard, 2011).

## Current State of Affairs

To inform the creation of an improved approach to cybersecurity, it is essential first to assess the current state of our cybersecurity infrastructure, policies, and practices. This section outlines the existing measures, evaluates their effectiveness, and identifies potential areas for enhancement.

### Frameworks and Standards

Currently, we adhere to PCI DSS for securing recurrent customer payments. However, it is essential to acknowledge that while PCI DSS provides a robust framework for securing credit card transactions, it should be considered a baseline for broader cybersecurity measures (Williams, 2013).

### Cybersecurity Risks

- *Payment Data*: Given that our core business involves recurrent customer payments, payment data security is a paramount concern.
- *Multi-payment Methods*: We support various payment methods, including credit cards, ACH, and digital currency, each with unique risks.
- *External threats*: Phishing attacks, DDoS attacks, and malware are ever-present threats that require constant vigilance.
- *Internal threats*: The potential for internal data breaches, either accidental or malicious, remains an ongoing concern.

### Current Controls

- *Firewalls and Intrusion Detection Systems*: To monitor and manage network traffic.
- *Encryption*: Encryption protocols are in place to secure sensitive data transmission.
- *Employee Training*: Periodic cybersecurity awareness training sessions for employees.

### Maturity Level

Based on an internal evaluation using the Cybersecurity Maturity Model Certification (CMMC), our organization currently stands at Level 2, indicating that we have established a baseline of cybersecurity practices but still have room for improvement. The CMMC framework consists of five maturity levels (Office of the Under Secretary of Defense for Acquisition & Sustainment, 2023):

- *Level 1* – Basic Cyber Hygiene: Includes basic cybersecurity practices, such as using antivirus software and ensuring that data is backed up. Compliance at this level is foundational but limited.
- *Level 2* – Intermediate Cyber Hygiene: This is our current level. It means we have documented practices and policies and established a baseline of cybersecurity measures beyond essential protection.
- *Level 3* – Good Cyber Hygiene: Achieving this level requires that we manage the maturity of our processes and implement more advanced cybersecurity practices. This often involves automating specific security tasks and more sophisticated incident response plans.
- *Level 4* – Proactive: At this level, the organization has advanced and mature cybersecurity practices, regularly adapts to evolving threats, and deploys automated solutions to detect and counter threats.
- *Level 5* – Advanced/Progressive: At this apex level, the organization has highly advanced cybersecurity practices and optimizes its security posture to adapt to the constantly changing cyber threat landscape.

Moving to Level 3 would involve:

- *Advanced Threat Intelligence*: Actively monitor and analyze threats specific to our industry and implement corresponding controls.
- *Automated Incident Response*: Develop and implement automated response mechanisms to quickly contain and mitigate threats.

- *Management Buy-In*: Secure commitment and resources from upper management for ongoing security assessments and improvements.
- *Comprehensive Audits*: Undertake exhaustive internal and external audits to assess the effectiveness of implemented measures.

## Immediate Actions (0-6 months)

Immediate actions are vital to navigate the complex landscape of cybersecurity risks, frameworks, and standards. These actions are strategically designed to address pressing vulnerabilities while laying the groundwork for more comprehensive, long-term strategies.

### Update and Patch Software

- *Importance*: Outdated software is a prime target for cyber-attacks, given the known vulnerabilities (Cui, Yang, Chen, & Ming, 2023).
- *Action*: Implement an automated patch management system to ensure that all software gets updated promptly.

### Strengthen Access Controls

- *Importance*: Weak access controls can easily be exploited to gain unauthorized entry to critical systems.
- *Action*: Adopt a Zero Trust approach, whereby every user, even those within the organization, must verify their identity before accessing network resources.

### Employee Training

- *Importance*: Human error remains one of the most common causes of cybersecurity incidents (Kirlappos, Parkin, & Sasse, 2014).
- *Action*: Roll out an immediate mandatory training program focusing on the most prevalent cybersecurity threats, like phishing and social engineering.

### Data Encryption

- *Importance*: With various payment methods supported, encrypting sensitive data is crucial.
- *Action*: Ensure end-to-end encryption for all data transactions, including those involving digital currency.

### Incident Response Plan

- *Importance*: A swift and efficient response to security incidents can significantly mitigate damage.
- *Action*: Update the incident response plan and conduct immediate drills to gauge effectiveness.

## Medium-term Strategies (6-24 months)

While immediate actions address the most pressing vulnerabilities, medium-term strategies are geared toward sustainability and robustness. These plans incorporate technological solutions and organizational changes to create a more secure environment.

### Migration to Cloud Service

- *Importance*: Utilizing cloud-based services can offer more robust security features than traditional in-house solutions, including better scalability and incident recovery options.
- *Action*: Assess, select, and begin migration to a cloud service provider with solid cybersecurity credentials.

### Enhancing Security Architectures

- *Importance*: As cybersecurity threats evolve, so must our defensive measures.

- *Action*: Integrate next-generation firewalls, intrusion detection/prevention systems, and other advanced security technologies into the existing infrastructure.

### Risk Assessment

- *Importance*: Comprehensive risk assessments are crucial for understanding the organization's security landscape.
- *Action*: Conduct bi-annual cybersecurity risk assessments to identify new vulnerabilities and update risk profiles.

### Advance Monitoring

- *Importance*: Enhanced monitoring capabilities can provide more timely and accurate detection of cyber threats.
- *Action*: Implement Security Information and Event Management (SIEM) systems for real-time analysis of security alerts.

### Vendor Risk Management

- *Importance*: Third-party vendors can introduce security vulnerabilities into an organization's network.
- *Action*: Conduct cybersecurity audits of critical vendors and establish protocols for ongoing assessment.

## Long-term Vision (2-5 years)

In an ever-evolving digital landscape, the importance of a forward-thinking cybersecurity strategy cannot be overstated. Our long-term vision is a guiding light for sustained growth and resilience against increasingly sophisticated cybersecurity threats.

### Cybersecurity Culture

- *Importance*: Developing a security-centric culture is vital for enduring success.

- *Action*: Implement continuous employee training and establish cybersecurity as a regular agenda item in executive meetings.

### AI and Machine Learning

- *Importance*: Advanced technologies can provide unprecedented capabilities in threat detection and response.
- *Action*: Invest in AI and machine-learning technologies to automate threat detection and response mechanisms.

### Regulatory Adaptability

- *Importance*: Regulatory landscapes are ever-changing, and compliance will become increasingly complex.
- *Action*: Establish a dedicated regulatory compliance team to monitor and adapt to new cybersecurity regulations continuously.

### Zero Trust Architecture

- *Importance*: The Zero Trust model is quickly becoming the gold standard in cybersecurity.
- *Action*: Pan and initiate a multi-year migration to a Zero Trust architecture.

### Global Expansion Preparedness

- *Importance*: Cybersecurity considerations will evolve as the organization grows and potentially enters new markets.
- *Action*: Conduct global risk assessments to prepare for potential entry into new markets, considering regulations like GDPR, even if we currently do not operate in Europe.

As we navigate our organization's multifaceted cybersecurity terrain, the necessity for a well-defined, multi-tiered approach to cybersecurity risk cannot be overstated. This paper elucidated the pertinence of adopting a comprehensive cybersecurity plan that pivots on an intricate web of frameworks, models, standards, and roles. Frameworks such as PCI DSS and CMMC provide essential roadmaps for organizations, offering a structured approach to identifying, managing, and mitigating risks. However, it's imperative to recognize these as minimum baselines for cybersecurity rather than comprehensive solutions. Maturity models like CMMC offer an evaluation lens and actionable insights for staged improvements.

Standards like ISO/IEC 27002 and regulations such as GDPR, even if not immediately applicable due to geographical factors, offer valuable guidelines for best practices. They create a controlled environment wherein cybersecurity risks can be adequately mapped, assessed, and mitigated. The evolving nature of regulatory landscapes like KYCA/AM further underscores the need for adaptive, long-term strategies.

The roles of different stakeholders, especially upper management and C-level executives, are indispensable in shaping and sustaining a cybersecurity-focused organizational culture. Implementing strategies, whether immediate, medium-term, or long-term, heavily relies on the commitment and understanding of these key individuals. By aligning frameworks, models, standards, and roles, our organization can mitigate prevailing cybersecurity risks and build a resilient and adaptive security posture capable of countering future threats.

# References

Cui, L., Yang, S., Chen, F., & Ming, Z. (2023). A survey on application of machine learning for Internet of Things. *International Journal of Machine Learning and Cybernetics. DOI:10.1007/s13042-018-0834-5*.

Duncan, B. (2019). EU General Data Protectin Regulation Compliance Challenges for Cloud Users. *The International Conference on Cloud Computing, GRIDs, and Virtualization.* Venice, Italy: ResearchGate.

Greenleaf, G. (2019). *Global Data Privacy Laws 2019: 132 National Laws & Many Bills.* 157 Privacy Laws & Business International Report, 14-18, Available at SSRN:https//ssrn.com/abstract=3381593.

Kirlappos, I., Parkin, S., & Sasse, A. (2014). Learning from "Shadow Security:" Why Understanding Non-Compliant Behaviors Provides the Bases for Effective Security. *Journal of Information Security and Applications*, 55-66.

Office of the Under Secretary of Defense for Acquisition & Sustainment. (2023, September 25). *Cybersecurity Maturity Model Certification (CMMC) Version 1.02.* Retrieved from United States Department of Defense: https://dodcio.defense.gov/CMMC/Model/

Sadiq, S., Governatori, G., & Namiri, K. (2008). Modeling Control Objectives for Business Process Compliance. *Proceedings of the 5th International Conference on Business Process Management* (pp. 149-161). Berling, Heidelberg: Springer.

Solms, R., & Niekerk, J. (2013). From information security to cyber security. *Computer & Security, https://doi.org/10.1016/j.cose.2013.04.004*, 97-102.

Tankard, C. (2011). Advanced Persistent threats and how to monitor and deter them. *Network security, Volume 2011, Issue 8, https://doi.org/10.1016/S1353-4858(11)70086-1*, 16-19.

Williams, B. L. (2013). *Information Security Policy Development for Compliance: ISO/IEC 2001, NIST SP 800-53, HIPAA Standard, PCI DSS V2.0, and AUP V5.0*. Auerbarch Publications.