Cybersecurity Compliance and Risk Management

An Executive Summary

Prepared by Sergio Gutierrez

Updated: 1/3/2022

Bayside Networks

Experienced·Ethical·Responsive

Established 1986

Current Cybersecurity Landscape

3 out of 4 organizations have fallen victim to a ransomware attack

- *– The State of Email Security 2022 |* *Mimecast*

The United States sees the most expensive data breaches in the world, with an average of $4.24 million per attack.

- *– Cost of a Data Breach Report |* *IBM*

The DoD released a memorandum announcing the CMMC program which will require compliance of cyber practices of vendors and their supply chains to win or renew contracts

- *- Office of the Under Secretary of Defense, Memorandum|* DoD

44% of Companies Require Vendors to Provide Proof of Cybersecurity as Part of Their RFPs

- *- Key Trends and Forces Shaping Risk and Compliance Management in 2021|* ACA Compliance Group

Why do compliance programs matter?

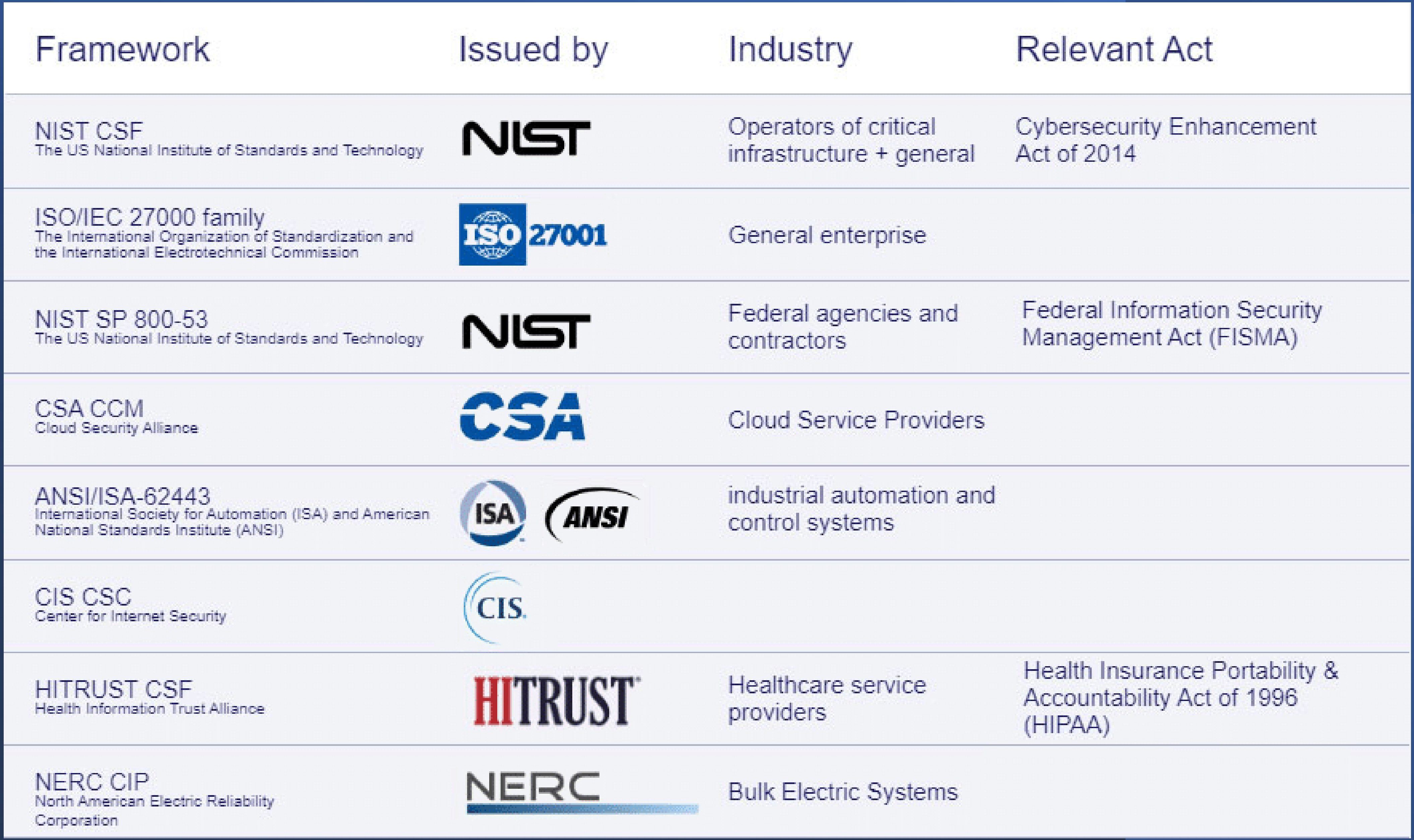
- Cybersecurity threats are on the rise
- Compliance is required by law
- Non-compliance can lead to fines and other penalties
- Cybersecurity compliance can improve customer trust
- Cybersecurity compliance can reduce legal liability

What is a (cybersecurity) compliance framework?

A cybersecurity framework is a collection of best practices that an organization should follow to mange its cybersecurity risk

Selecting The Appropriate Compliance Framework – Key Questions

- What is the organizations mission, objectives, and goals?
- What product/service are you selling?
- What certification are your customers and clients looking/asking for?
- What certification would allow your organization reach a competitive advantage?



Framework	Issued by	Industry	Relevant Act
NIST CSF The US National Institute of Standards and Technology	NIST	Operators of critical infrastructure + general	Cybersecurity Enhancement Act of 2014
ISO/IEC 27000 family The International Organization of Standardization and the International Electrotechnical Commission	ISO 27001	General enterprise	
NIST SP 800-53 The US National Institute of Standards and Technology	NIST	Federal agencies and contractors	Federal Information Security Management Act (FISMA)
CSA CCM Cloud Security Alliance	CSA	Cloud Service Providers	
ANSI/ISA-62443 International Society for Automation (ISA) and American National Standards Institute (ANSI)	ISA ANSI	industrial automation and control systems	
CIS CSC Center for Internet Security	CIS.		
HITRUST CSF Health Information Trust Alliance	HITRUST	Healthcare service providers	Health Insurance Portability & Accountability Act of 1996 (HIPAA)
NERC CIP North American Electric Reliability Corporation	NERC	Bulk Electric Systems	

ISO 27001 Certification

THE ISO 27001 CERTIFICATION IS INCREASINGLY ASSOCIATED WITH BUILDING BRAND REPUTATION AND CUSTOMER LOYALTY.

LACK OF ISO 27001 CERTIFICATION CAN BE SEEN AS A RISK, ESPECIALLY IN REGULATED INDUSTRIES

THE GOAL IS TO MINIMIZE RISK AND ENSURE BUSINESS CONTINUITY BY PROACTIVELY LIMITING THE IMPACT OF A SECURITY BREACH.

Why adopt a cybersecurity compliance framework?

- It helps ensure that the business is meeting relevant cybersecurity regulations and requirements
- Reaffirms trust to all stakeholders of the organizations commitment to reducing operational risk and legal liability. If a breach does occur, can help demonstrate that the business took the appropriate measures to protect its sensitive information
- Improves operational efficiency of the business

Key Risk Management Questions

What are our most critical assets and do we have the appropriate measures in place to protect them?

Are we investing in the right processes and controls, and how do we evaluate the results of our decisions?

Do our cybersecurity risk management capabilities and competencies align to industry standards and how do they compare with peer organizations?

How do we evaluate the effectiveness of our cybersecurity risk management program, and how do we determine if it aligns with our risk appetite?

What is an IT Policy?

IT policy is a document that outlines the rules and guidelines for the use of a business's information technology (IT) assets

Helps employees understand their responsibilities and the expectations for their use of the business's IT assets.

Establishes security measures, protocols, to protect the business's data and systems from unauthorized access or cyber threats

Ensures that the business's IT assets are used in a way that is consistent with the business's goals and values

Why does the organization need an IT policy?

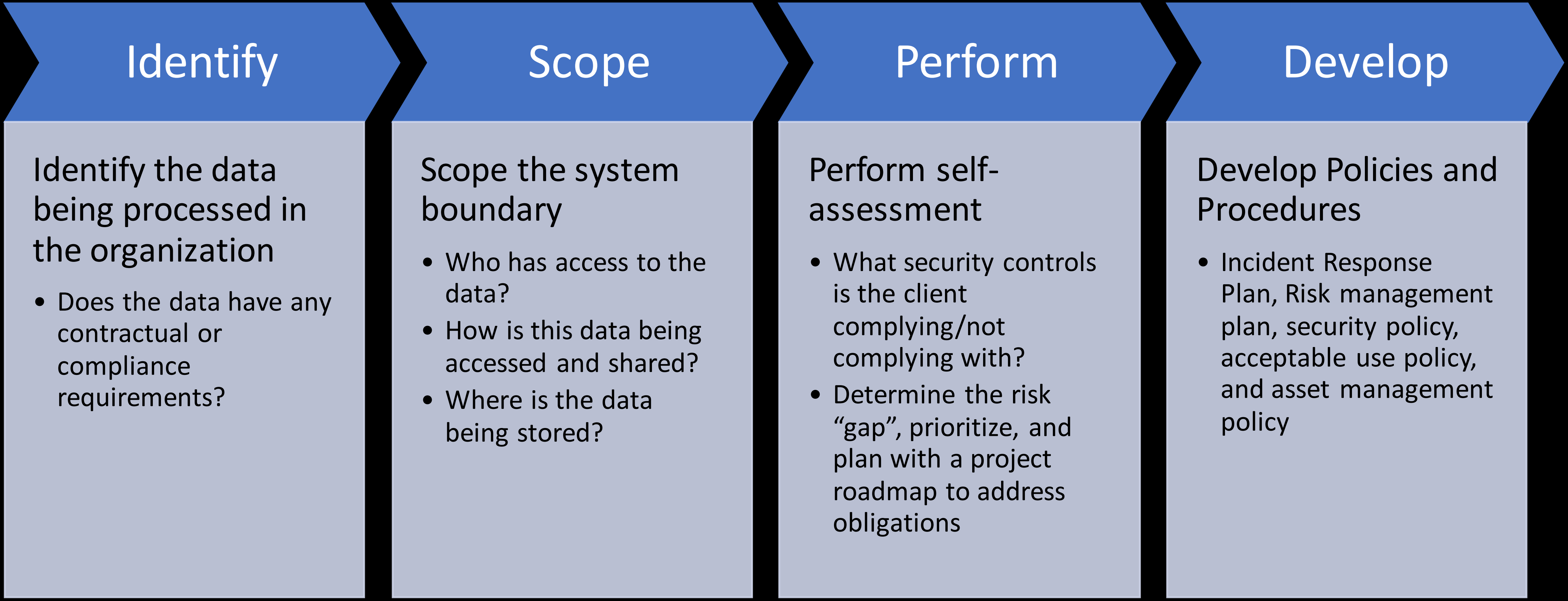
A written IT policy serves as written documentation of the organizations commitment to meet its cybersecurity objectives.

Serves as a basic communications tool to survey the expectations of management and the IT team

Saves time with producing decisions that others have made before. IT will have the information and support they need to carry out management's objectives.

IT Policy serves as the window for executives to view their present cybersecurity hygiene.

Cybersecurity Program – Next Steps



Identify

Identify the data being processed in the organization

- Does the data have any contractual or compliance requirements?

Scope

Scope the system boundary

- Who has access to the data?
- How is this data being accessed and shared?
- Where is the data being stored?

Perform

Perform self-assessment

- What security controls is the client complying/not complying with?
- Determine the risk “gap”, prioritize, and plan with a project roadmap to address obligations

Develop

Develop Policies and Procedures

- Incident Response Plan, Risk management plan, security policy, acceptable use policy, and asset management policy