ANIMATION SOFTWARE RESEARCH

TENNESSEE DEPARTMENT OF THE TREASURY

INFORMATION SYSTEMS DIVISION - SECURITY

BY CORY STEPHENSON

DECEMBER 28, 2023

Contents

List of Tables

List of Figures

1 Introduction

1.1 Objectives for Framework Analysis

1. Research the current Cybersecurity Frameworks to be considered to replace the current framework.
2. Develop a pros and cons list evaluating each framework.
3. Research implementation guidelines.
4. Analyze any costs that may be associated with the frameworks.
5. Present findings to Treasury Security leadership by 01/15/2024 with a recommendation of which framework will work best for Treasury and why.

1.2 Objectives for Framework Implementation

In the first quarter of employment, a cybersecurity framework was chosen. In the remaining IPP period, running from approximately 02/01/2024 - 08/31/2024, work to implement the chosen framework within the Treasury department.

1. Document the process of applying the framework to a control and a test.
2. Create a control document and relate it to the Treasury environment.
3. Create a test case that demonstrates adherence to the control.
4. Review the control and test case with Security leadership.
5. Create a schedule for control review and testing the control.

Definition 1: Information technology

Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.[1][1]

[1] FIPS 200 under INFORMATION TECHNOLOGY from 40 U.S.C., Sec.1401

Definition 2: Information security

Information security refers to the protection of information and data assets from unauthorized access, use, disclosure, alteration, or destruction. It involves implementing security measures, policies, procedures, and controls to ensure information confidentiality, integrity, and availability. Information security focuses on protecting all forms of information, regardless of the technology or system used to store or transmit it.[2]

Definition 3: Information systems security

Information systems security, on the other hand, specifically focuses on protecting computer systems and the associated infrastructure that store, process, transmit, and manage information. It encompasses the security measures, policies, and controls implemented to safeguard computer hardware, networks, and databases from unauthorized access, attacks, and disruptions. Information systems security aims to ensure the availability, integrity, and confidentiality of information processed by computer systems.[2]

Definition 4: Information assurance

Information assurance, is a new term in the computer security field that arose over time. Information assurance is a broader concept encompassing the management and protection of information assets, including information security and information systems security. It emphasizes the holistic approach of ensuring confidentiality, integrity, availability, and non-repudiation of information. Information assurance goes beyond technical controls and includes integrating people, processes, and technology to address risks related to information.[2]

Definition 5: Cybersecurity

"Cybersecurity is a term that has gained significant prominence in recent years and is often used interchangeably with information security. Cybersecurity specifically focuses on protecting computer systems, networks, and digital information from cyber threats, which include unauthorized access, cyber-attacks, data breaches, and other malicious activitiesconducted through digital means. Cybersecurity involves a combination of technical, operational, and managerial measures to identify, protect, detect, respond to, and recover from cyber incidents.[2]"

1.3 Treasury's Current Framework Status

> The ISO 2700 series framework was implemented 15 plus years ago as part of a security project. Unfortunately, after the project was complete and a few years had passed, the framework was not being maintained. Treasury is interested in implementing a new framework. We are currently looking between the National Institute of Standards and Technology (NIST) 800-53 and the Center for Internet Security (CIS) Critical Security Controls. We want you to research each framework and help us decide on which will be best for Treasury.
>
> —Andrew Sprague, Security Manager

> Treasury IS Security will be revitalizing the ISO 27001/2 security framework and possibly moving to NIST standards in the FY 2024 year.
>
> —Comprehensive Cybersecurity Framework

1. Alignment with Standards

Treasury is using the ISO 27001/2 framework to identify and test alignment with policies and procedures. ISO Sorts are performed each month to test separate sections of the plan.

—Comprehensive Cybersecurity Framework

2 Frameworks

I borrowed the descriptions of the following frameworks from https://www.controlmap.io/compliance-frameworks.

SOC 2 Type I & II

The American Institute of Certified Public Accountants (AICPA) created the SOC 2 framework to help organizations safeguard customer data from unauthorized access and other security risks. The framework delineates five Trust Services Criteria: security, availability, processing integrity, confidentiality, and privacy. Each criterion is intended to ensure that customer data remains secure at all times.

ISO 27001

ISO/IEC 27001:2013 (ISO 27001) is an international standard that defines the requirements for an effective information security management system (ISMS). It provides a framework to help organizations protect and manage their data assets. This includes financial data, employee records, intellectual property, and third-party managed information and ensures confidentiality, integrity, and availability.

ISO 27001 (2022)

ISO 27001 is the internationally recognized standard for implementing and managing an Information Security Management System (ISMS). This standard can be used to pass an audit, guaranteeing that a business's information security protocols are up-to-date. On October 25, ISO 27001:2022 was released, replacing the previous version established in 2013.

NIST CSF

The National Institute of Standards and Technology (NIST) Cybersecurity Framework is a comprehensive set of standards, guidelines, and best practices created to help organizations manage their cybersecurity risk. This framework was developed with flexibility in mind, in order to be implemented alongside existing security processes in any industry.

CMMC

The U.S. Department of Defense's Cybersecurity Maturity Model Certification (CMMC) was introduced as a means to ensure that all defense contractors comply with relevant security protocols in order to protect sensitive defense information. Companies responsible for handling Controlled Unclassified Information (CUI) or Federal Contract Information (FCI) must meet the CMMC requirements to remain compliant.

HIPPA

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal standard mandated by the Department of Health and Human Services. HIPAA compliance is regulated by the Office for Civil Rights in order to protect protected health information (PHI). HIPAA outlines the permissible use and disclosure of PHI as set forth by HHS guidelines.

GDPR

GDPR is a revolutionary set of data protection regulations designed to give people full control over information associated with them and limit the ways organizations can use personal data. Comprised of 99 distinct articles, it stands as one of the world's most comprehensive sets of privacy laws.

FedRAMP

FedRAMP® was launched in 2011 to provide a cost-effective and risk-focused model for the federal government's use of cloud technology. FedRAMP allows agencies to adopt modern cloud services with increased attention to security and the protection of federal data. This program is essential for government operations as it ensures that cloud technologies are implemented securely and efficiently.

CSA CCM

The CSA Cloud Controls Matrix (CCM) is a cybersecurity control framework that provides guidance on cloud implementation and security controls. It's a spreadsheet which contains 16 domains covering all aspects of cloud technology, in addition to 133 control objectives. The CCM includes comprehensive guidance on the security controls necessary for all actors within a cloud supply chain.

COBIT 2019

COBIT® 2019 (Control Objectives for Information and Related Technologies) is the most recent evolution of ISACA's globally recognized and utilized COBIT framework. This broad and comprehensive framework was developed to support understanding, designing, and implementing the management and governance of enterprise IT.

CCPA

The Consumer Privacy Act of 2018 (CCPA) legislation grants Californian consumers greater control over the personal information businesses collect from them. As a result, the CCPA provides clear and comprehensive directions to organizations on how they can comply with the law. Businesses governed by the CCPA have a set of legal obligations, such as handling consumer rights requests and providing customers with necessary notices related to their privacy policies.

CIS Controls

The CIS Critical Security Controls (CIS Controls) are a globally implemented set of best practices used to boost an organization's cybersecurity. Thousands of professionals worldwide use the CIS Controls today, and they are continually updated through a collaborative consensus-based approach. The CIS Controls prioritize and simplify the steps necessary to form a strong cybersecurity defense.

NIST 800-171

NIST Special Publication 800-171 (NIST 800-171) is a federal standard that establishes procedures for how defense contractors and subcontractors manage "controlled, unclassified information," or CUI. CUI consists of personal data, intellectual property, equipment specs, logistical plans and other confidential defense-related information. Compliance with this standard is vital in protecting valuable information.

NIST Privacy Framework v1.0

NIST created the Privacy Framework as a collaborative tool to help organizations protect individuals' privacy while also creating innovative products and services. The intent is to allow organizations to better identify and manage potential privacy-related risks. This voluntary framework is intended to be a useful resource in navigating the ever-evolving technological landscape.

SOC 1 Type 2 Controls

A SOC 1 Type 2 report is an internal controls assessment designed to meet the needs of OneLogin customers' management and their auditors. The independent third-party auditor who issues the SOC 1 reports periodically performs an examination in accordance with SSAE No. 16 and ISAE No. 3402 so that customers, both in the US and abroad, can use them to evaluate how OneLogin's controls affect their own internal financial reporting processes.

PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a vital tool for any organization that handles credit card information. This set of security standards is carefully designed to protect and secure payment accounts during the entirety of the transaction process. Changes in PCI security standards are regularly made with a focus on improving data safety. All companies that accept, process, store, or transmit credit card data should be sure to abide by these standards.

MARS

Minimum Acceptable Risk Standards (MARS) compliance is designed to ensure the availability, confidentiality, and integrity of protected health information (PHI), personally identifiable information (PII), and federal tax information (FTI). Developed by the Centers for Medicare and Medicaid Services (CMS), the standards are based on the National Institute of Standards and Technology (NIST) Special Publication 800-53.

TX-RAMP

TX-RAMP (Texas Department of Information Resources program) is a data security certification requirement for cloud computing services. It provides "a standardized approach for security assessment, authorization, and continuous monitoring of cloud computing services that process the data of a state agency."

ISO/IEC 27018:2019

ISO/IEC 27018 is an important international standard that focuses on protecting the privacy of Personally Identifiable Information (PII). It is part of the larger ISO/IEC 27000 family, and serves as a vital first step for cloud service providers in assessing risk and implementing appropriate security measures for PII. This industry-driven initiative creates a secure foundation for cloud computing services.

SCF

The SCF (Security and Control Framework) presents a broad range of security and privacy controls to streamline the process of creating and sustaining secure processes, systems, and applications. The SCF is designed to maximize cybersecurity protection

at all levels – strategic, operational and tactical. It encourages companies to establish robust, layered protection systems that protect from both cybercriminal threats as well as unsanctioned data access or misuse.

SCF 2022.2

Secure Controls Framework (SCF) provides organizations with a comprehensive approach to cybersecurity and privacy compliance across all operational levels. This framework offers the guidance needed to implement and maintain internal controls in line with business objectives.

ISO 27701

ISO/IEC 27701 enables organizations to put in place policies and standards for the handling of Personally Identifiable Information (PII), thus enhancing their ability to comply with GDPR and other data privacy regulations. This information security standard provides guidelines on how Data Controllers and Data Processors should manage PII, making this a valuable tool for promoting data privacy within organizations.

ISO/IEC 27017:2015

ISO/IEC 27017:2015 offers rigorous guidance in the security elements of cloud computing. It suggests that cloud service providers adhere to the ISO/IEC 27002 and ISO/IEC 27001 standards while implementing specific information security controls. This code of practice provides clear instructions for additional information security control implementation based on the various cloud services being used.

Microsoft DPR

Microsoft Data Protection Regulations (DPR) are annual requirements that Microsoft suppliers enrolled in the SSPA program must abide by. The regulations ensure the appropriate processing of Personal Data and Confidential Data. All Microsoft suppliers are expected to adhere to these regulations in order to remain compliant with Microsoft requirements.

TISAX

TISAX is an industry-standard method for assessing and exchanging information security for enterprises. By utilizing TISAX, companies can not only simplify the process of evaluating their own supplier's level of data security but also determine appropriate ways to handle sensitive customer information. In short, TISAX provides effortless evaluation of data protection.

UK ICO

This framework provides the essential elements of a successful privacy management program. Although it is not comprehensive and does not substitute for compliance with all aspects of data protection regulations, careful evaluation and consideration should be taken for your specific needs. Additionally, other guidance such as GDPR should be consulted when necessary.

Essential Eight (ACSC)

Australian organizations of all sizes must defend themselves against malicious cyber threats. To that end, the Australian Cyber Security Centre (ACSC) offers a baseline

to help protect systems from these threats: the Essential Eight, eight key mitigation strategies defined by ACSC's Strategies to Mitigate Cyber Security Incidents. Adopting this baseline makes it much more difficult for adversaries to gain access and compromise systems.

AESCSF - AEMO

The Australian Energy Sector Cyber Security Framework (AESCSF) is the result of a collaborative effort between government and industry stakeholders, such as the Australian Energy Market Operator (AEMO), Australian Cyber Security Centre (ACSC), Cyber and Infrastructure Security Centre (CISC), as well as multiple energy organizations from Australia. The framework is designed to ensure the highest level of security in the energy sector.

FTC Safeguards Rule

The FTC Safeguards Rule ensures that entities covered by the Rule maintain safeguards to protect the security of customer information. It applies to financial institutions subject to the FTC's jurisdiction that aren't subject to the enforcement authority of another regulator under section 505 of the Gramm-Leach-Bliley Act, 15 U.S.C. § 6805.

UK Cyber Essentials

UK Cyber Essentials is a government-supported program that provides organizations of any size an effective way to guard against commonly occurring cyber attacks. With two levels, Cyber Essentials and Cyber Essentials Plus, businesses can proactively protect themselves from security risks.

Motion Picture Association

The MPA manages security assessments at entertainment vendor facilities on behalf of its member studios. A set of Content Security Best Practices that outlines standard controls to help secure content, production, post-production, marketing, and distribution.

CSA-CCM v4.03

The Cloud Controls Matrix (CCM) and the corresponding Cloud Security Alliance Questionnaire (CAIQ) are a comprehensive set of security controls and practices, based on the CSA best practices. The CCM provides an industry-standard set of cybersecurity frameworks tailored specifically to cloud computing.

Prudential Standard CPS 234

This Prudential Standard is designed to help ensure that APRA-regulated entities have the capability to safeguard themselves against information security incidents (including cyberattacks). They are required to maintain information security that is matching the threat posed by digital vulnerabilities and threats.

PSPF

The Protective Security Policy Framework (PSPF) outlines the Australian Government's protective security policy. The framework provides guidance to all government bodies on how to effectively implement the policy in four key areas: personnel,

physical, governance, and information security. With the PSPF, government organizations are able to ensure effective security measures.

FFIEC Cybersecurity Assessment

In an effort to help financial institutions recognize potential risks and determine their cybersecurity preparedness, the Federal Financial Institutions Examination Council has developed the Cybersecurity Assessment Tool. This tool is based on the ideas within the FFIEC Information Technology Examination Handbook, NIST Cybersecurity Framework, and industry-established best practices.

New Zealand Information Security Manual (NZISM)

The New Zealand Information Security Manual provides essential controls and processes necessary for protecting all New Zealand Government information and systems. In addition, the manual provides supplemental controls that are recommended for optimum security–efforts to exceed the minimum acceptable baseline levels.

2.1 Control Frameworks

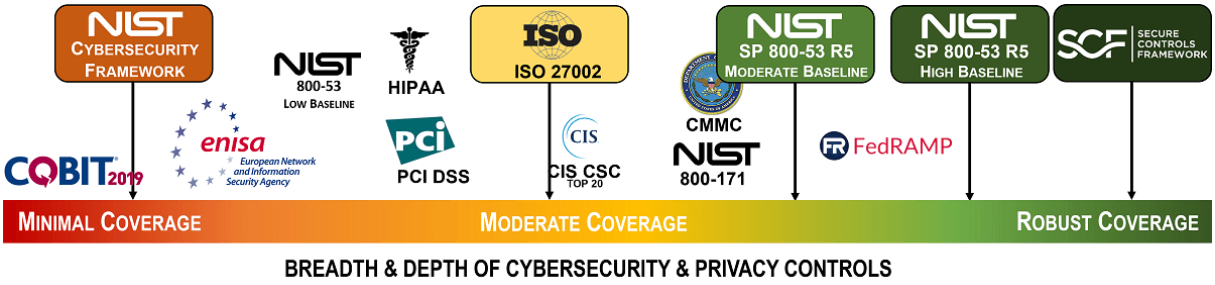

Figure 1: NIST CSF vs ISO 27001/2 vs NIST 800-53 vs SCF

2.1.1 NIST 800-53

Revision 5 of this foundational NIST publication represents a multi-year effort to develop the next generation of security and privacy controls that will be needed to accomplish the above objectives. It includes changes to make the controls more usable by diverse consumer groups (e.g., enterprises conducting mission and business functions; engineering organizations developing information systems, IoT devices, and systems-of-systems; and industry partners building system components, products, and services). The most significant changes to this publication include:

- Making the controls more *outcome-based* by removing the entity responsible for satisfying the control (i.e., information system, organization) from the control statement;
- Integrating information security and privacy controls into a seamless, consolidated control catalog for information systems and organizations;

> - Establishing a new supply chain risk management control family;
> - Separating control selection *processes* from the *controls*, thereby allowing the controls to be used by different communities of interest, including systems engineers, security architects, software developers, enterprise architects, systems security and privacy engineers, and mission or business owners;
> - Removing control baselines and tailoring guidance from the publication and transferring the content to *NIST SP 800-53B, Control Baselines for Information Systems and Organizations*;
> - Clarifying the relationship between requirements and controls and the relationship between security and privacy controls; and
> - Incorporating new, state-of-the-practice controls (e.g., controls to support cyber resiliency, support secure systems design, and strengthen security and privacy governance and accountability) based on the latest threat intelligence and cyber-attack data.
>
> In separating the process of control selection from the controls and removing the control baselines, a significant amount of guidance and other informative material previously contained in SP 800-53 was eliminated. That content will be moved to other NIST publications such as SP 800-37 (Risk Management Framework) and SP 800-53B during the next update cycle. In the near future, NIST also plans to offer the content of SP 800-53, SP 800-53A, and SP 800-53B to a web- based portal to provide its customers interactive, online access to all control, control baseline, overlay, and assessment information.
>
> —[3]

2.1.2 NIST 800-171

> Today, more than at any time in history, the federal government is relying on external service providers to help carry out a wide range of federal missions and business functions using information systems. Many federal contractors process, store, and transmit sensitive federal information to support the delivery of essential products and services to federal agencies (e.g., providing financial services; providing web and electronic mail services; processing security clearances or healthcare data; providing cloud services; and developing communications, satellite, and weapons systems). Federal information is frequently provided to or shared with entities such as state and local governments, colleges and universities, and independent research organizations. The protection of sensitive federal information while residing in *nonfederal systems* and organizations is of paramount importance

> to federal agencies, and can directly impact the ability of the federal government to carry out its designated missions and business operations.
>
> —[4]

> The protection of unclassified federal information in nonfederal systems and organizations is dependent on the federal government providing a process for identifying the different types of information that are used by federal agencies. EO 13556[3] established a governmentwide Controlled Unclassified Information (CUI) Program to standardize the way the executive branch handles unclassified information that requires protection. Only information that requires safeguarding or dissemination controls pursuant to federal law, regulation, or governmentwide policy may be designated as CUI. The CUI Program is designed to address several deficiencies in managing and protecting unclassified information to include inconsistent markings, inadequate safeguarding, and needless restrictions, both by standardizing procedures and by providing common definitions through a CUI Registry NARA CUI. The CUI Registry is the online repository for information, guidance, policy, and requirements on handling CUI, including issuances by the CUI Executive Agent. The CUI Registry identifies approved CUI categories, provides general descriptions for each, identifies the basis for controls, and sets out procedures for the use of CUI including, but not limited to, marking, safeguarding, transporting, disseminating, reusing, and disposing of the information.
>
> —[4]
>
> [3] Executive Order 13556 – Controlled Unclassified Information

> EO 13556 also required that the CUI Program emphasize openness, transparency, and uniformity of governmentwide practices, and that the implementation of the program take place in a manner consistent with applicable policies established by the Office of Management and Budget (OMB) and federal standards and guidelines issued by the National Institute of Standards and Technology (NIST). The federal CUI regulation,developed by the CUI Executive Agent, provides guidance to federal agencies on the designation, safeguarding, dissemination, marking, decontrolling, and disposition of CUI, establishes self-inspection and oversight requirements, and delineates other facets of the program.
>
> The purpose of this publication is to provide federal agencies with recommended security requirements for protecting the confidentiality of CUI: (1) when the CUI is resident in a nonfederal system and organization; (2) when the nonfederal organization is not collecting or maintaining

information on behalf of a federal agency or using or operating a system on behalf of an agency; and (3) where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category listed in the CUI Registry.

The requirements apply to components of nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components. If nonfederal organizations designate specific system components for the processing, storage, or transmission of CUI, those organizations may limit the scope of the security requirements by isolating the designated system components in a separate CUI security domain. Isolation can be achieved by applying architectural and design concepts (e.g., implementing subnetworks with firewalls or other boundary protection devices and using information flow control mechanisms). Security domains may employ physical separation, logical separation, or a combination of both. This approach can provide adequate security for the CUI and avoid increasing the organization's security posture to a level beyond that which it requires for protecting its missions, operations, and assets.

The recommended security requirements in this publication are intended for use by federal agencies in appropriate contractual vehicles or other agreements established between those agencies and nonfederal organizations. In CUI guidance and the CUI Federal Acquisition Regulation (FAR), the CUI Executive Agent will address determining compliance with security requirements.

In accordance with the federal CUI regulation, federal agencies using federal systems to process, store, or transmit CUI, at a minimum, must comply with:

- Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems* (moderate confidentiality);
- Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*;
- NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*; and NIST Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*.

The responsibility of federal agencies to protect CUI does not change when such information is shared with nonfederal partners. Therefore, a similar level of protection is needed when CUI is processed, stored, or transmitted by nonfederal organizations using nonfederal systems. The recommended requirements for safeguarding CUI in nonfederal systems and organizations are derived from the above authoritative federal standards and guidelines to maintain a consistent level of protection. However, recognizing that the scope of the safeguarding requirements in the federal CUI regulation is limited to the security objective of confidentiality (i.e., not directly addressing integrity and availability) and that some of the security requirements expressed in the NIST standards and guidelines are uniquely federal, the requirements in this publication have been tailored for nonfederal entities.

The tailoring criteria described in Chapter Two are not intended to reduce or minimize the federal requirements for the safeguarding of CUI as expressed in the federal CUI regulation. Rather, the intent is to express the requirements in a manner that allows for and facilitates the equivalent safeguarding measures within nonfederal systems and organizations and does not diminish the level of protection of CUI required for moderate confidentiality. Additional or differing requirements, other than the requirements described in this publication, may be applied only when such requirements are based on law, regulation, or governmentwide policy and when indicated in the CUI Registry as CUI-specified or when an agreement establishes requirements to protect CUI Basic at higher than moderate confidentiality. The provision of safeguarding requirements for CUI in a specified category will be addressed by the National Archives and Records Administration (NARA) in its CUI guidance and in the CUI FAR; and reflected as specific requirements in contracts or other agreements. Nonfederal organizations may use the same CUI infrastructure for multiple government contracts or agreements, if the CUI infrastructure meets the safeguarding requirements for the organization's CUI-related contracts and/or agreements including any specific safeguarding required or permitted by the authorizing law, regulation, or governmentwide policy.

This publication serves a diverse group of individuals and organizations in both the public and private sectors including, but not limited to, individuals with:

- System development life cycle responsibilities (e.g., program managers, mission/business owners, information owners/stewards, system designers and developers, system/security engineers, systems

integrators);

- Acquisition or procurement responsibilities (e.g., contracting officers);
- System, security, or risk management and oversight responsibilities (e.g., authorizing officials, chief information officers, chief information security officers, system owners, information security managers); and
- Security assessment and monitoring responsibilities (e.g., auditors, system evaluators, assessors, independent verifiers/validators, analysts).

The above roles and responsibilities can be viewed from two distinct perspectives: the federal perspective as the entity establishing and conveying the security requirements in contractual vehicles or other types of inter-organizational agreements; and the nonfederal perspective as the entity responding to and complying with the security requirements set forth in contracts or agreements.

—[4]

2.1.3 CIS Controls (CSC)

The Center for Internet Security (CIS) Critical Security Controls (CSC) is a set of best practices and guidelines designed to help organizations enhance their cybersecurity defenses and reduce the risk of cyber threats. The CIS CSC provides a prioritized and actionable security control framework that organizations can implement to improve their overall security posture. The CIS CSC consists of 20 specific controls that cover a wide range of cybersecurity areas, including asset management, secure configuration, continuous vulnerability management, and incident response. These controls are based on real-world attack patterns and are regularly updated to address emerging threats and vulnerabilities. The controls are organized into three implementation groups: Basic, Foundational, and Organizational, which represent progressive levels of security maturity and coverage. The CIS CSC is a valuable resource for organizations looking to establish a solid foundation of cybersecurity controls. It provides practical and effective measures that can be implemented to mitigate common security risks and enhance the organization's ability to detect, respond to, and recover from cyber incidents. The controls are designed to be adaptible to various environments. They can be tailored to meet organizations' specific needs and requirements.

—[2]

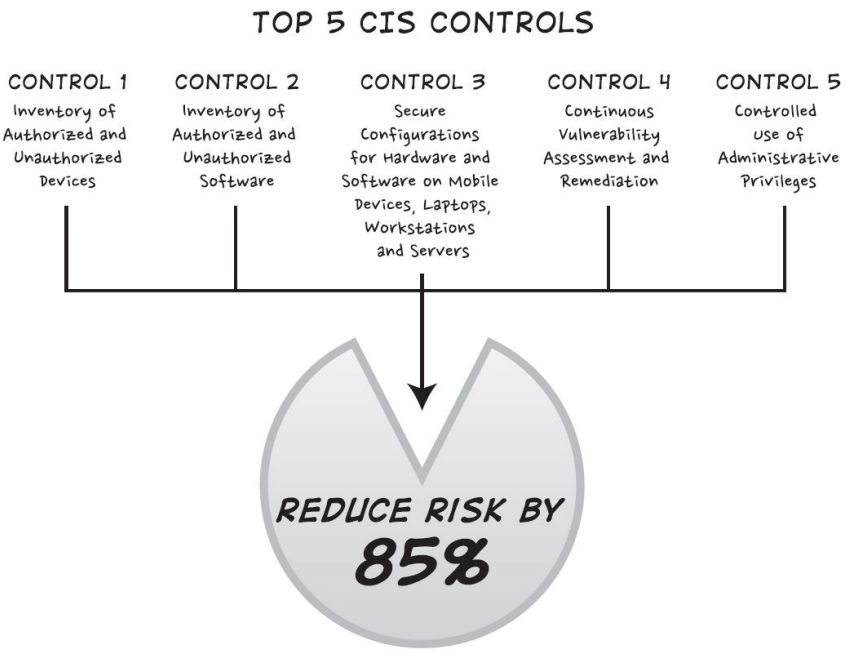

Figure 2: The "Top 5 CIS Controls" can stop 85 percent of cyberattacks.

> In cybersecurity, there are five controls that stop 85 percent of all attacks.[4]
>
> If these five controls stop 85 percent of attacks, does it make sense to spend time on anything else until you've mastered them? Until these five controls are in place, does it make sense to focus on anything else?
>
> One-hundred-item frameworks overcomplicate simple solutions, and often these five crucial controls are glossed over or ignored.
>
> —[5]

[4] "The 20 CIS Controls & Resources," Center for Internet Security, accessed October 20,2020, https://www.cisecurity.org/controls/cis-controls-list/.

Along with the excerpt shown above, Figure 2 can be found on page 41 of Christian Espinosa's book (listed in the bibliography as entry 5). The source file (.jpg) was downloaded from the book's companion site, https://christianespinosa.com/resources/tspitr/. Since the book's time of publication (February of 2021), the number of CIS controls has been reduced to 18.

2.1.4 Resources

- NIST SP 800-53 Revision 5
- NIST SP 800-53A Revision 5
- NIST SP 800-171 Revision 2
- The 18 CIS Critical Security Controls
- CIS CSC Implementation Group 1
- CIS CSC Implementation Group 2
- CIS CSC Implementation Group 3
- Mapping and Compliance
- CIS Critical Security Controls Navigator

2.2 Program Frameworks

2.2.1 ISO 27001

ISO/IEC Standards

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) have created two standards that companies can use to implement information security controls. The two standards work together: one guides information security governance, whereas the other reviews how to implement security control. The standards are:

- ISO/IEC 27001:2013, "Information Technology—Security Techniques—Information Security Management Systems—Requirements"
- ISO/IEC 27002:2013, "Information Technology—Security Techniques—Code of Practice for Information Security Controls"

ISO/IEC 27001 provides a framework for creating an information security management system. It uses a risk-based approach to review how information security is managed within an organization, and reviews the processes that management teams must consider to operate monitor, review, and maintain IT systems.

ISO/IEC 27002 lists information security safeguards. Unlike COBIT and GAIT, ISO/IEC 27002 does describe specific controls. It has 14 major sections, with each section reviewing a different category of information security controls. The standard explains why organizations should use the listed controls. It also explains how to use the controls. The 14 sections are:

- Information security policy
- Information security organization
- Human resources security
- Asset management
- Asset control
- Cryptography
- Physical and environmental security
- Operations security
- Communications security
- Information system acquisition, development, and maintenance
- Supplier relationships
- Information security incident management
- Information security business continuity management
- Compliance

The ISO/IEC standards are specific to information security. Companies can use these standards to make sure that their information security practices provide reasonable assurance that ICFR are effective.[6]

2.2.2 Combining ISO 27001 with the NIST Cybersecurity Framework (CSF)

> Organizations can leverage the ISO/IEC 27001 and 27002 frameworks to enhance their cybersecurity posture when used in conjunction with the NIST Cybersecurity Framework. The NIST Cybersecurity Framework provides a flexible and risk-based approach to managing and mitigating cyber risks, while ISO/IEC 27001 and 27002 offer detailed controls and implementation guidance. By aligning the two frameworks, organizations can benefit from the comprehensive control framework of ISO/IEC 27001 and 27002 while leveraging the risk management and organizational framework provided by the NIST Cybersecurity Framework.
>
> —[2]

2.3 Risk Frameworks

2.3.1 ISO 27005

2.3.2 NIST 800-39

2.3.3 NIST 800-37

2.3.4 NIST 800-30

2.3.5 FAIR

2.4 Honorable Mentions

- Secure Controls Framework
- Unified Compliance Framework

2.5 Selecting Appropriate Framework(s)

I took a LinkedIn Learning course in October of 2023, entitled Security Frameworks Fundamentals. The instructor (Mandy Huth) provided a number of key considerations whenever you are selecting appropriate frameworks for your organization:

1. Do you have any regulatory or compliance requirements?
2. What is your organizations risk management approach?
3. Does it need a risk management program as well?
4. Are there any industry-specific requirements that apply to your organization?
5. What is the current status of your current security controls and practices?
6. What resources and budget does your company have?
7. What are your organizations goals and objectives for its security program?
8. What is the focus of the current/desired framework: risk management, compliance, or cyberthreats
9. Who are the key stakeholders that may be impacted by implementing the controls?

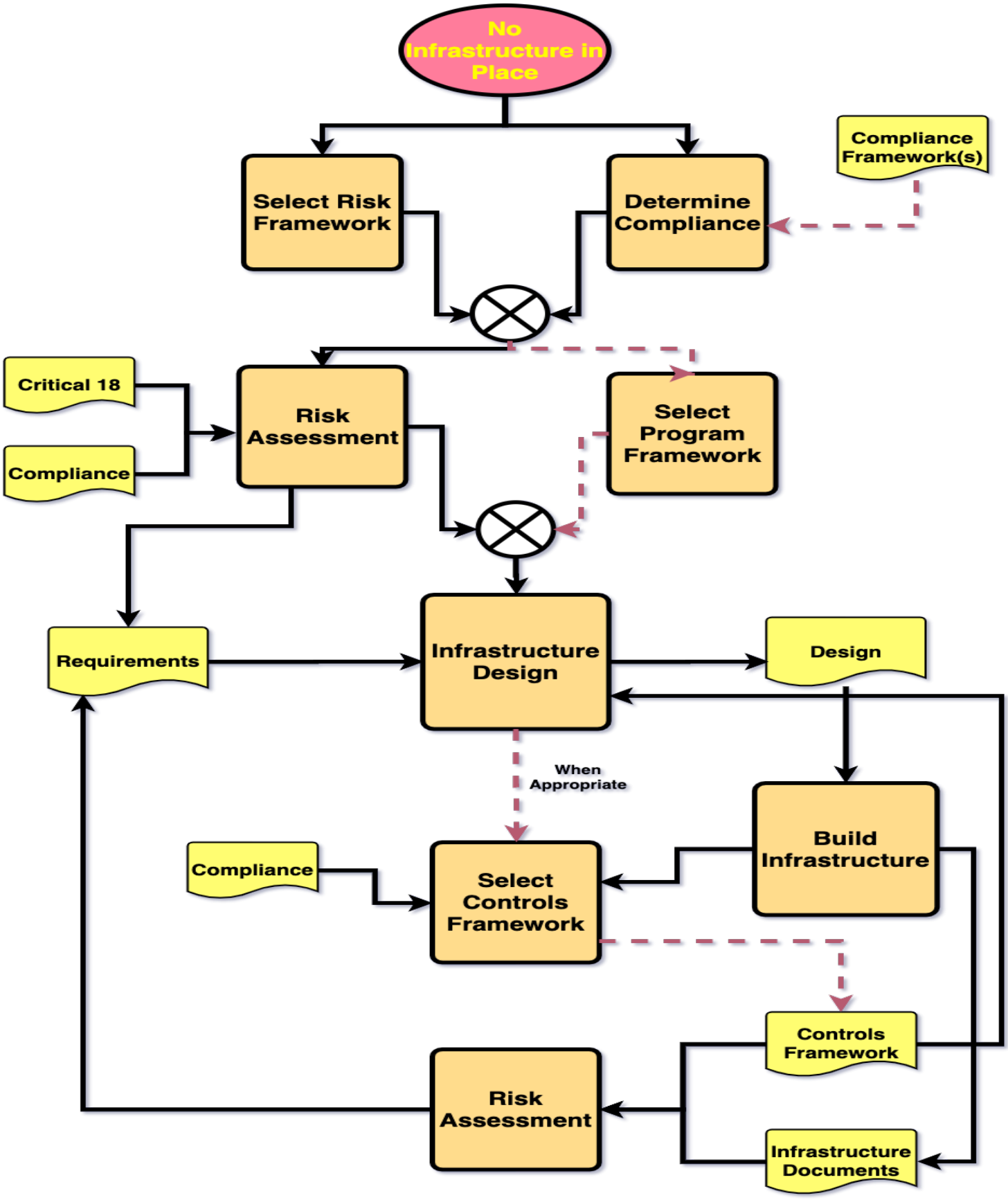

Figure 3: Frameworks Selection Process

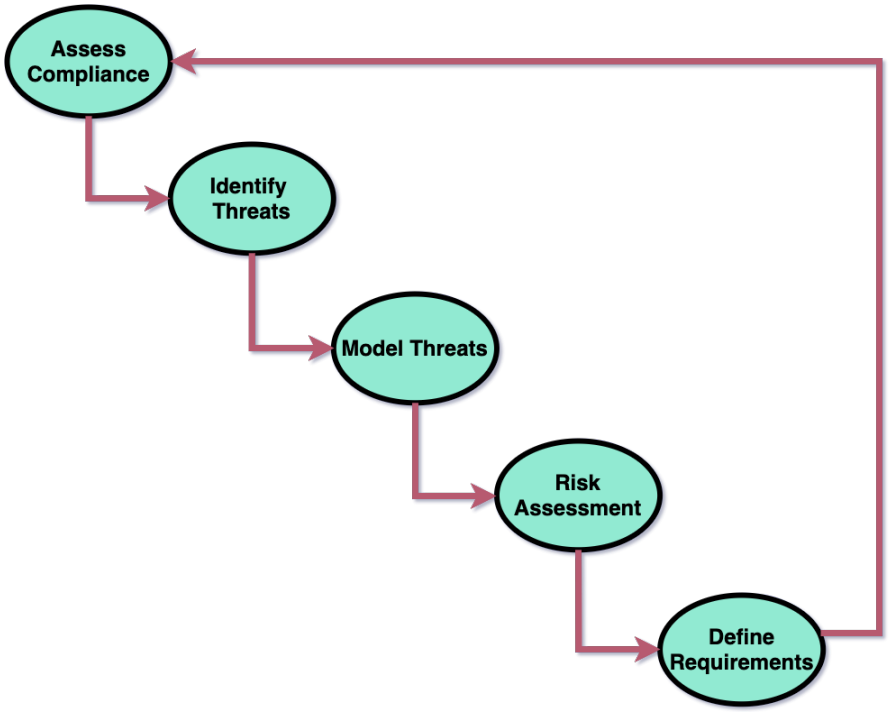

Figure 4: Requirements Definition Process

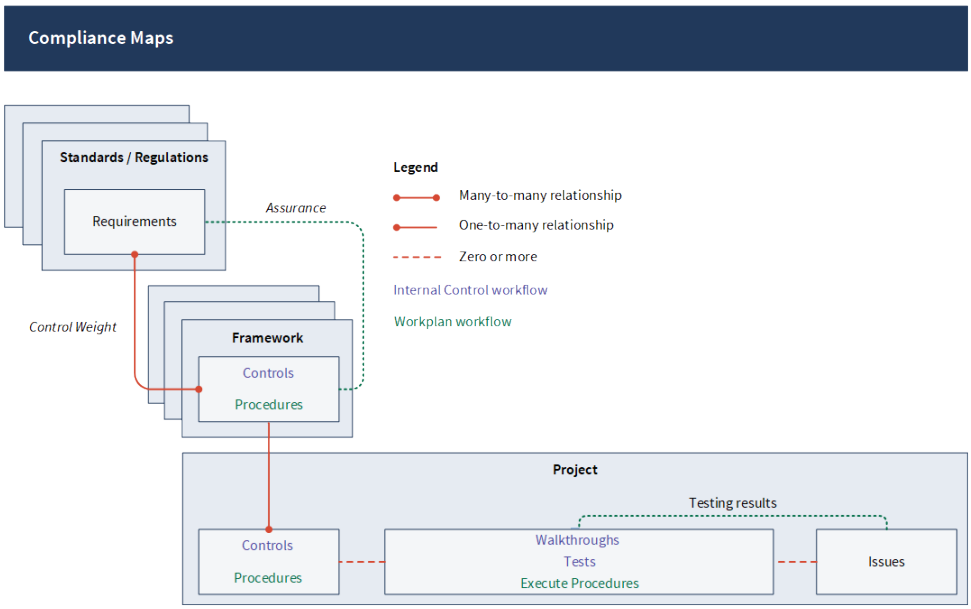

Figure 5: Compliance Maps Entity Relationship Diagram (ERD)

> The processes for selecting a framework for a new or established business can differ based on the security program's maturity. Figure 3 shows the complete process. An organization starts its process at the appropriate point. In the real world, an organization might find itself anywhere on this model. The red dashed arrows are paths needed only initially or when business conditions radically change.
>
> The first two steps can take place at the same time. They include selecting a risk framework and determining compliance. Determining compliance may also require adopting a compliance framework. For example, entities covered under the HIPAA need to understand the necessary standards before finalizing network and system requirements.
>
> The team needs a risk framework to guide the initial and future risk assessments. Each risk assessment includes compliance requirements.
>
> The initial risk assessment uses the compliance requirements and the modeling of probable threats to perform a risk assessment. This process is shown in Figure 2. If the organization has not yet selected a control framework, it should use the CIS 18 critical controls as a baseline until it adopts a more comprehensive framework.[5]
>
> — Tom Olzak
> Cybersecurity Researcher, Author & Educator
> July 29, 2021

[5] https://www.spiceworks.com/it-security/cyber-risk-management/articles/best-security-framework/

Figure 2 is featured in the video Select System Controls Based Upon Requirements. I would also like to direct your attention to this document. The taxonomy found therein is the final result of a research project conducted by Enclave Security.

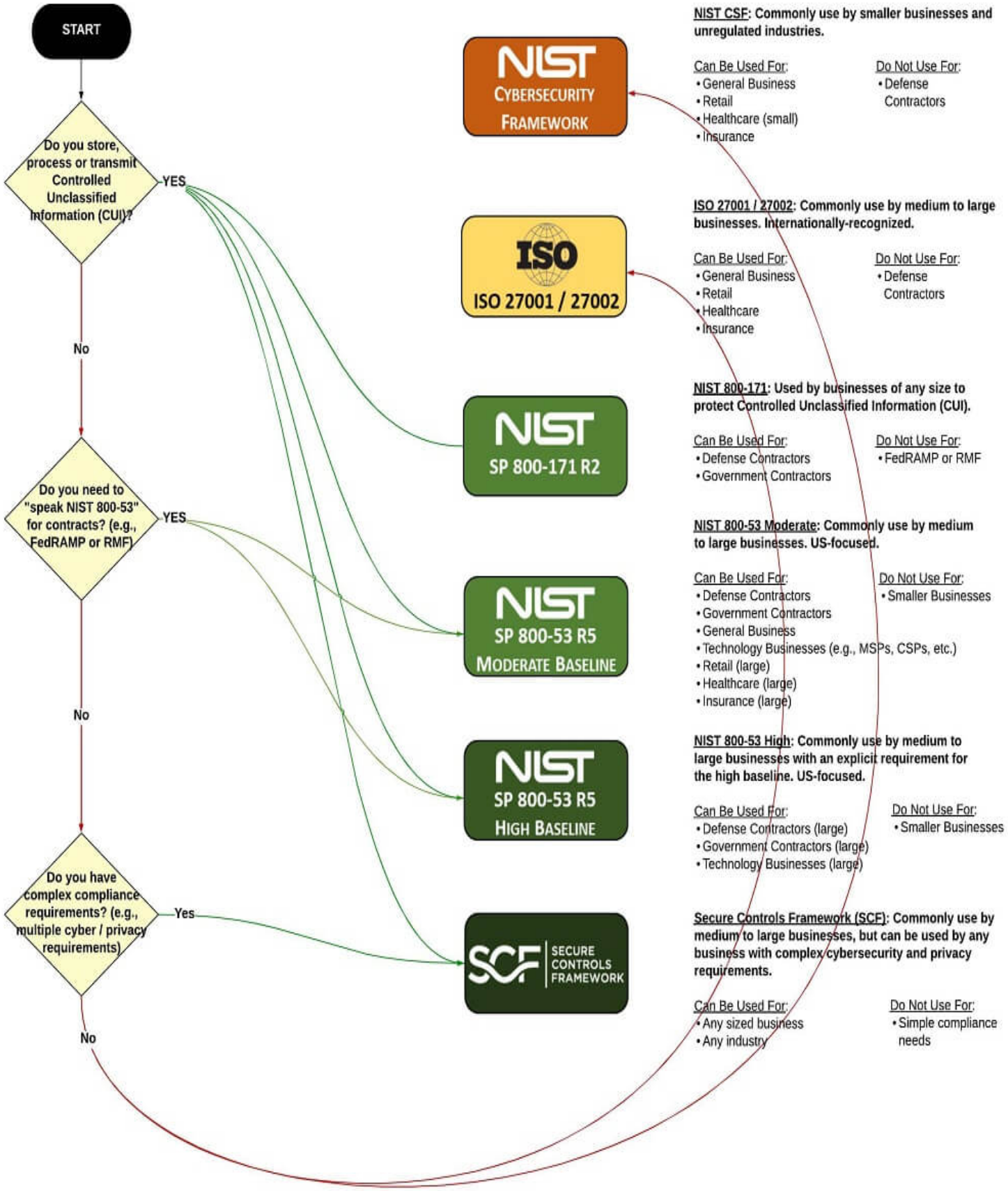

Figure 6: Frameworks Selection Flowchart

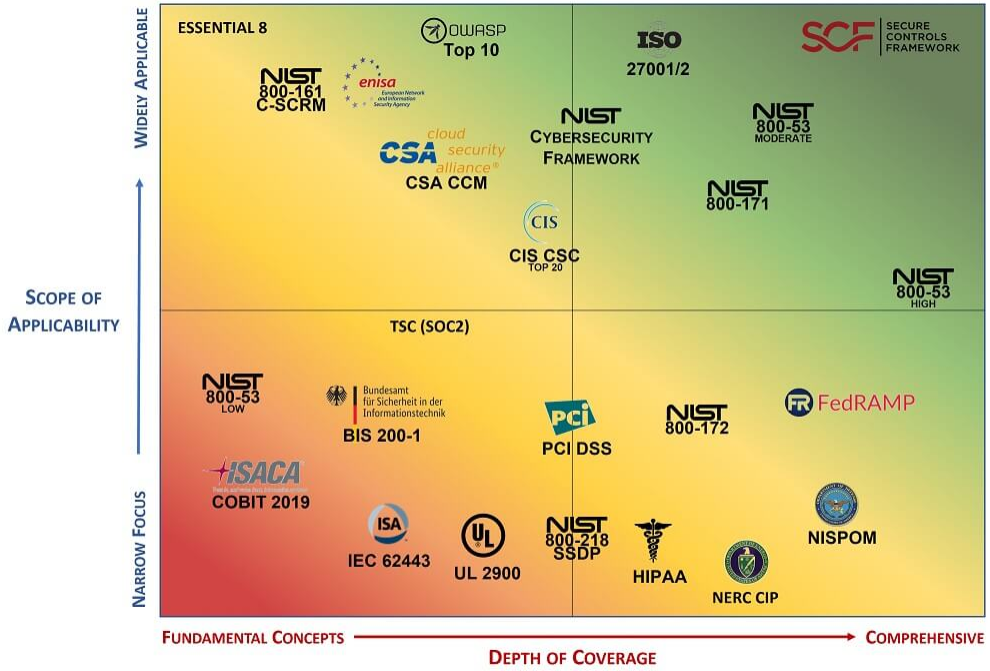

Figure 7: Perceptual Heatmap

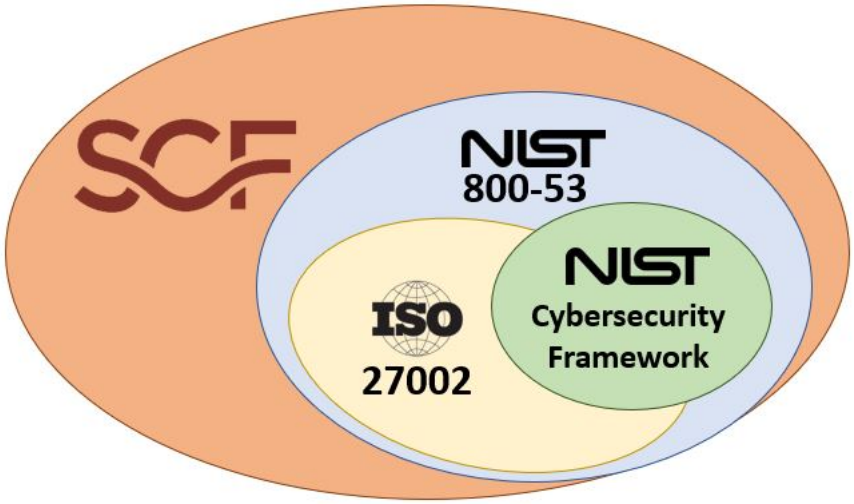

Figure 8: Venn Diagram

Figure 9: Compliance Forge Graphics

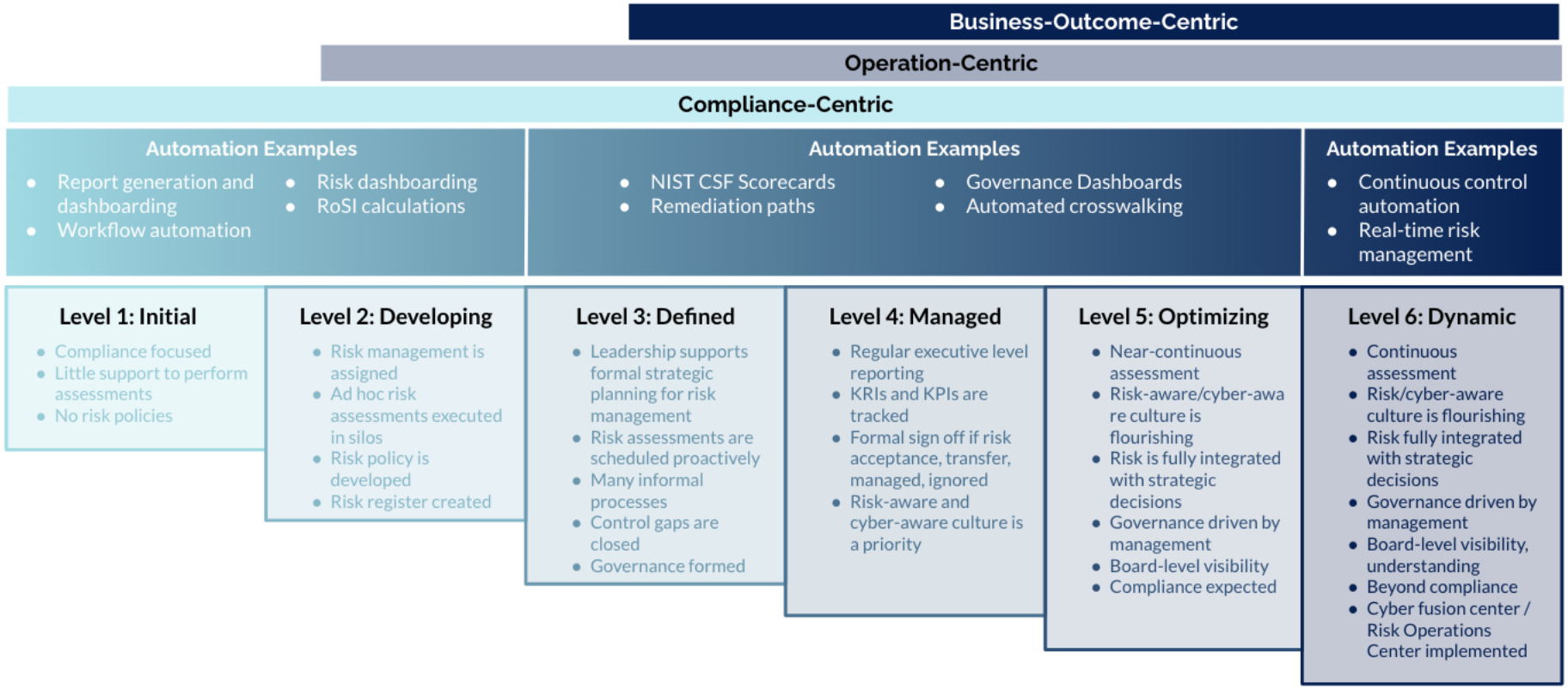

Figure 10: The Six Stages of Cyber Security Risk and Compliance Automation

	NIST SP 800-53 (tenfold)	NIST SP 800-171 (tenfold)	CIS Controls (CSC)
Audience	Federal agencies, (sub)contractors and local governments with access to federal information systems[7]	Non-federal entities who store or process controlled unclassified information (CUI) in their own network[7]	Organizations of all sizes and global enterprises[8]
Controls	20 control families, over 1,000 controls and control enhancements[7]	14 control families, 110 security requirements[7]	18 controls, total of 153 Safeguards[9]
Levels	Three control baselines for low, moderate and high impact systems[7]	Moderate baseline as standard, optional enhanced controls in SP 800-172[7]	Three implementation groups based on risk profile and available resources[9]

Table 1: Control Framework Comparison Table

	ISO 27001	NIST Cybersecurity Framework (tenfold)
Audience	IT service providers, financial organizations, healthcare organizations[10]	Voluntary guidance for private and public organizations, mandatory for federal agencies[7]
Controls	There are 93 controls in all in the latest 2022 revision.[10]	5 core functions, 108 security targets[7]
Levels	• Confidential (only senior management have access) • Restricted (most employees have access) • Internal (all employees have access) • Public information (everyone has access) [11]	Four implementation tiers measuring organizational risk management[7]

Table 2: Program Framework Comparison Table

	ISO 27001	NIST Cybersecurity Framework (tenfold)
Audience	IT service providers, financial organizations, healthcare organizations[10]	Voluntary guidance for private and public organizations, mandatory for federal agencies[7]
Controls	There are 93 controls in all in the latest 2022 revision.[10]	5 core functions, 108 security targets[7]
Levels	• Confidential (only senior management have access) • Restricted (most employees have access) • Internal (all employees have access) • Public information (everyone has access) [11]	Four implementation tiers measuring organizational risk management[7]

Table 3: Risk Framework Comparison Table

Framework	Strengths	Weaknesses
NIST CSF	✓ Superior and unbiased cybersecurity ✓ Enable long-term cybersecurity and risk management ✓ Conciliate the interests of business and technical stakeholders ✓ Framework flexibility and adaptability ✓ Designed to meet future compliance and regulation requirements	• Doesn't help to measure risk • Show directional improvement but can't show the ROI of improvement • Companies are not given guidance on where to rank on the scale
FAIR	✓ Leverages analytics to determine risk and risk rating ✓ A solid taxonomy and technology standard ✓ Integrates and enhances existing risk management frameworks	• It is not a method for performing organisational or individual tasks • In spite of the lack of real measurements and assessment methodologies, technical standards describe risk and relationships • Requires a tightly defined taxonomy to function

Figure 11: NIST CSF vs. FAIR

	NIST CSF	**ISO 27001**
STRUCTURE	Core divided into 5 functions, 22 categories and 98 subcategories, 4 implementation tiers	11 sections (0-3 being non-mandatory, 4-10 being mandatory), Annex A
CERTIFIABLE	No	Yes
MANDATORY DOCUMETS	Not specified	Scope of the ISMS, Information security policy and objectives, Risk assessment and risk treatment methodology, Statement of Applicability, Risk treatment plan, Risk assessment report, Security roles and responsibilities, Inventory of assets, Access control policy document [10]
BASIS	Risk Management based	Risk Management based
MECHANISM	Optional, self-certification	Non-voluntary, independent audit based.
SCOPE	Optional guidelines, best-practices and standards for implementing and improving cyber-security programs	Information security standard that describes how to implement an ISMS (Information Security Management System)
TECHNOLOGY NEUTRALITY	Yes	Yes

Figure 12: NIST CSF vs. ISO 27001

Figure 13: Compliance Forge Graphics

Category	Cost Range Tier 1 Max Cyber Budget: $50,000			Cost Range Tier 2 Max Cyber Budget: $500,000			Cost Range Tier 3 Max Cyber Budget: $5,000,000		
	No-Cost	Low	High	No-Cost	Low	High	No-Cost	Low	High
Asset Management	$0	$556	$2,044	$0	$690	$3,896	$0	$790	$18,414
Data Management	$0	$1,148	$14,566	$0	$11,192	$41,918	$0	$87,027	$387,867
Secure Configurations	$0	$968	$9,008	$0	$4,710	$47,494	$0	$18,138	$269,263
Account and Access Control Mgmt.	$0	$1,579	$4,025	$0	$7,063	$39,240	$0	$29,412	$388,728
Vulnerability Management	$0	$345	$1,969	$0	$845	$7,200	$0	$5,285	$64,746
Log Management	$0	$88	$2,520	$0	$632	$10,866	$0	$3,543	$54,000
Malware Defense	$0	$452	$1,399	$0	$5,591	$10,799	$0	$44,870	$107,898
Data Recovery	$0	$650	$2,143	$0	$2,925	$11,888	$0	$28,275	$118,701
Security Training	$0	$120	$450	$0	$1,440	$3,660	$0	$3,420	$36,570
Incident Response	$0	$0	$0	$0	$0	$0	$0	$0	$0
TOTAL	**$0**	**$5,906**	**$38,124**	**$0**	**$35,088**	**$176,961**	**$0**	**$220,760**	**$1,446,187**

Audit preparation costs	**$3-40k**
ISO 27001 + 27002 standard requirements	$350
ISO 27001 consultant (optional)	$38k
Gap analysis (optional)	$5.7k
Pen test/vulnerability assessment	$2-8k
Implementation costs	**From $1k annually**
Security training	$1k annually
New tools and software	varies
Productivity costs	varies
Certification audit costs	**$10-50k**
Internal audit	$5-7.5k
Stage 1 + 2 certification audit	$10-50k
Surveillance audit	$10-30k
Total cost of ISO 27001 certification	**$15-$90k**

> Often times, when a security professional enters a new environment to build and manage a team, they are dealing with an organization that is relatively immature from an IT and security perspective, Kim said. In those cases, they want to determine the basic set of controls to implement.
>
> Cybersecurity professionals use control frameworks to do the following, according to Kim:
>
> - Assess the state of the overall security program
> - Build a comprehensive security program
> - Measure maturity and conduct industry comparisons
> - Simplify communications with business leaders
>
> NIST SP 800-53 is a comprehensive control catalog of security and privacy controls, in which control can be implemented based on priority or secure control baselines (low impact, moderate impact, or high impact). CIS Controls, meanwhile, have published the top 20 critical security control, which the US Department of State uses, Kim said.[12]
>
> — Alison DeNisco Rayome
> Managing Editor of ZDNET Commerce
> March 7, 2019

3 References

[1] information technology (IT) - Glossary | CSRC. https://csrc.nist.gov/glossary/term/information_technology, December 2023. [Online; accessed December 8th, 2023].

[2] Lisa McKinley Kip Boyle, Jason Dion. *Mastering Cyber Resilience*. Akylade Certified. Akylade, jul 2023.

[3] NIST SP 800-53, Revision 5 - CSF Tools — csf.tools. https://csf.tools/reference/nist-sp-800-53/r5/, . [Accessed 20-12-2023].

[4] NIST SP 800-171 Revision 2 - CSF Tools — csf.tools. https://csf.tools/reference/nist-sp-800-171/r2/, . [Accessed 21-12-2023].

[5] Christian Espinosa. *The smartest person in the room the smartest person in the room*. Lioncrest Publishing, February 2021.

[6] Joanna Lyn Grama. *Legal and Privacy Issues in Information Security*. Information Systems Security & Assurance Series. Jones & Bartlett Learning, third edition, 2022.

[7] Joe Köller. NIST 800-53 and NIST 800-171: What‘s the Difference?

https://www.tenfold-security.com/en/nist-800-53-and-171-differences/, October 2023. [Online; accessed December 8th, 2023].

[8] Hatice Özşahan. Top 5 Cybersecurity Frameworks and Standards | Resmo. https://www.resmo.com/blog/top-cybersecurity-frameworks-and-standards, 2023. [Online; accessed December 8th, 2023].

[9] CIS Critical Security Controls Implementation Groups. https://www.cisecurity.org/controls/implementation-groups, November 2021. [Online; accessed December 8th, 2023].

[10] Autodit. ISO 27001: A Comprehensive Guide to Information Security Management. *Medium*, July 2023. [Online; accessed December 8th, 2023].

[11] Luke Irwin. ISO 27001 & Information Classification: Free 4-Step Guide. https://itgovernance.co.uk/blog/what-is-information-classification-and-how-is-it-relevant-to-iso-27001, March 2023. [Online; accessed December 8th, 2023].

[12] Alison DeNisco Rayome. How to choose the right cybersecurity framework. https://www.techrepublic.com/article/how-to-choose-the-right-cybersecurity-framework, March 2019. [Online; accessed December 8th, 2023].

[13] Maahnoor Siddiqui. NIST vs. ISO -What You Need To Know — securityboulevard.com. https://securityboulevard.com/2022/06/nist-vs-iso-what-you-need-to-know/. [Accessed 16-10-2023].

[14] Tom Olzak. How To Pick The Best Security Framework For Your Organization. https://www.spiceworks.com/it-security/cyber-risk-management/articles/best-security-framework/, July 2021. [Online; accessed December 8th, 2023].

[15] ISO 27001 Certification Costs. https://secureframe.com/hub/iso-27001/certification-cost, December 2023. [Online; accessed December 8th, 2023].

[16] Regulatory Compliance Costs & How It Helps Your Bottom Line. https://www.ispartnersllc.com/blog/rising-compliance-costs/, December 2023. [Online; accessed December 8th, 2023].

[17] Matthew K Sharp and Kyriakos Lambros. *The CISO evolution*. John Wiley & Sons, Nashville, TN, April 2022.

[18] Kelly Shortridge and Josiah Dykstra. Opportunity cost and missed chances in optimizing cybersecurity. *Commun. ACM*, 66(7):96–104, July 2023.

[19] Marco Spruit and Wouter de Bruijn. CITS. *Int. J. Inf. Secur. Priv.*, 6(4):94–116, October 2012.

[20] Cameron Delfin. The Six Stages of Cyber Security Risk and Compliance Automation. https://www.cybersaint.io/blog/the-six-stages-of-cyber-risk-and-compliance-automation. [Online; accessed December 15th, 2023].

[21] Calvin Wong. Investigation of information risk management frameworks. 05 2022.

[22] Prameet P. Roy. A high-level comparison between the nist cyber security framework and the iso 27001 information security standard. *2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTEA)*, pages 1–3, 2020. URL https://api.semanticscholar.org/CorpusID:219990502.

[23] Compliance Forge. NIST 800-53 vs ISO 27002 vs NIST CSF. https://complianceforge.com/grc/nist-800-53-vs-iso-27002-vs-nist-csf-vs-scf. [Accessed 20-12-2023].

[24] Scott E. Donaldson, Stanley G. Siegel, Chris K. Williams, and Abdul Aslam. *Mapping Against Cybersecurity Frameworks*, pages 429–447. Apress, Berkeley, CA, 2018. ISBN 978-1-4842-3258-3. doi: 10.1007/978-1-4842-3258-3_13. URL https://doi.org/10.1007/978-1-4842-3258-3_13.

Distinguishing Features	CIS CSC	NIST CSF
Comprehensiveness vs. Prescriptiveness	CIS Controls are renowned for their prescriptive nature, offering meticulous, actionable guidance.	NIST Framework casts a broader net, enabling organizations to tailor cybersecurity measures to their specific requirements.
Implementation Groups vs. Implementation Tiers	CIS deploys Implementation Groups to categorize organizations based on size and cybersecurity maturity.	NIST relies on Implementation Tiers to gauge organizations' cybersecurity readiness.
Specificity vs. Flexibility	CIS Controls are specific, leaving minimal room for interpretation, providing organizations with clear directives.	NIST Framework is flexible, allowing organizations to adapt guidelines to their unique needs.
When to Choose NIST Over CIS	While CIS is a strong contender, there are scenarios where NIST is the preferred choice.	1. **Government Contracts:** Organizations involved in government contracts or the federal supply chain must comply with NIST standards, such as NIST Special Publications 800-171 and 800-53. 2. **Mature Security Postures:** NIST frameworks are well-suited for organizations with mature security policies and a clear understanding of their cybersecurity needs. 3. **Customization:** NIST's flexibility allows for tailoring cybersecurity measures to fit an organization's unique resources and objectives.
When to Choose CIS Over NIST	1. **Practical Implementation:** For organizations seeking actionable, step-by-step guidance for implementing cybersecurity controls, CIS offers a clear advantage. 2. **Cross-Functional Teams:** The common language used in CIS documentation facilitates communication between technical and non-technical teams working on security initiatives. 3. **Framework of Frameworks:** CIS incorporates elements from various frameworks, including NIST, providing a consolidated approach for organizations lacking a comprehensive security policy.	While NIST is a strong contender, there are scenarios where NIST is the preferred choice.
Use Cases of CIS vs. NIST	CIS controls are well-suited for organizations seeking to implement security controls effectively. They are particularly beneficial for those without a comprehensive security policy and unsure about implementation prioritization.	NIST frameworks shine in diagnostics, organization, and planning. They are ideal for mature organizations looking to enhance their existing security policies and cater to specific regulatory requirements.
Cross-Compatibility with Compliance Frameworks	Both CIS and NIST frameworks align with various cybersecurity standards and compliance frameworks, but CIS does a better job of mapping into different standards. This makes CIS a valuable starting point for complying with regulations like PCI DSS, HIPAA, GDPR, and ISO 27001.	
Coverage Comparison	While CIS offers practical recommendations, NIST documentation is more comprehensive. It covers a wide range of cybersecurity standards, including NIST SP 800-53, 800-171, 800-37, and others, making it suitable for organizations aiming for high-level contracts or working with sensitive government data.	

Table 4: CIS CSC vs. NIST CSF Comparison Table