# INFORMATION SECURITY FRAMEWORKS

## AND CONTROLS CATALOGS

Prepared by Dave Zaras

July 17th, 2018

impactmakers
Better Business. Better Community.

## TABLE OF CONTENTS

## WHY DID WE CREATE THIS WHITEPAPER?

There are many organizations that do not yet have a robust information security program. They may have security practices in place but they're most likely not sure if those practices establish a comprehensive security program. In short, organizations are asking themselves "do we have everything, or at least the most important things, covered from an information security perspective?" To answer this question, organizational leadership can turn to a myriad of information security frameworks and controls libraries (e.g., ISO/IEC 27000, NIST SP 800-53, COBIT, HITRUST, CIS Critical Security Controls, etc.), but it can be daunting to understand which one is the right one to use.

There are some pros and cons of each framework and controls library and this whitepaper will give you some insight into selecting the right one(s).

## WHO IS THIS WHITEPAPER FOR?

Anyone who is interested in building a comprehensive information security program will benefit from this whitepaper, particularly if your organization does not already have a robust information security program and knows that it wants one.

## WHAT IS AN INFORMATION SECURITY FRAMEWORK ANYWAY?

A framework is the basic supporting structure for a concept or system. An information security framework provides the foundation to establish a comprehensive information security program that outlines the governance process and how risks will be managed through the employment of security controls. Well-established information security frameworks have gone through much of the trouble to define the elements that should be contained in an information security program.

An information security framework by itself, without modification by the organization which plans to use it, is rarely adequate without adaptation. Organizations that choose to use published information security frameworks must tailor them to suit their risk profile and compliance requirements. For example, a global bank with countless threat actors (i.e., "hackers") and regulations it needs to comply with (e.g., Sarbanes Oxley, GDPR, FFIEC, etc.) will need a significantly more robust information security program than, say, a small manufacturer of machine parts that only has sensitive data regarding employees. Both will benefit from starting with an information security framework to build their program and both will need to add and delete components from that framework to make their program "right sized".

**Information security frameworks have the following benefits:**

- Frameworks provide a comprehensive foundation for a robust information security program that includes governance and risk management
- Framework contributors and reviewers have thought through the most important information security challenges organizations may face
- Frameworks are recognized and accepted by many regulators, oversight organizations, and customers who demand effective security controls to protect themselves
- Some frameworks, such as ISO/IEC 27000 and HITRUST, provide the opportunity for certification which provides additional validation to customers and partners that the organization is meeting information security expectations

Note that some larger organizations adopt multiple information security frameworks to meet the various needs of their business units, regulators, partners, and customers, particularly if they are in multiple countries. With that said, smaller organizations should focus on getting a single security framework in place before attempting to tackle the complexity of using multiple frameworks.

## AND WHAT ABOUT SECURITY CONTROLS LIBRARIES?

Security controls are used to mitigate risks. That is, the employment of security controls is performed to lessen the likelihood and / or impact of a negative event from happening.

Several information security frameworks provide corresponding security controls libraries (e.g. ISO/IEC 27001 with ISO/IEC 27002 and the NIST Risk Management Framework with NIST SP 800-53). Additionally, there are standalone security controls libraries (e.g., CIS Critical Security Controls) that are provided without a corresponding framework, though many organizations adapt the structure of the controls library to become their information security framework.

Security controls libraries outline the specific actions that organizations can take to reduce risks. Whereas the framework will identify the high-level areas that a program should focus on, the controls library will offer specific guidance on how an organization can achieve risk reduction through the use of information security and, in some cases, privacy controls.

A mature or maturing organization, or wants to mature, will require a significant number of security controls that are detailed in formal, written standards and procedures. Likewise, organizations that operate in a highly-regulated environment will need to be clear on how they intend to secure the organization’s assets to meet regulations.

To be clear, implementing a robust set of information security controls will not necessarily prevent an organization from suffering a security incident, such as a data breach, but it is likely to lessen the chances to experience an incident and to lower the impact should it occur. Adopting a security framework and controls library will help demonstrate that the management of the organization was exercising due care to protect the data and systems entrusted to them.

## LET’S DIVE IN

### INFORMATION SECURITY FRAMEWORKS

An information security framework provides the basic structure for an information security program. In some parlance, the information security program is also called the information security management system (ISMS).

Keys to a successful security program include defining how the program will be governed, how risks will be identified and treated, roles and responsibilities for everyone who has a task to perform with regards to information security, and what security and privacy controls will be applied to maintain an acceptable level of risk.

Common information security frameworks include ISO/IEC 27001, the National Institute for Standards and Technology (NIST) Cybersecurity Framework (CSF), the NIST Risk Management Framework (RMF), and the HITRUST Cybersecurity Framework. Additionally, ISACA’s COBIT is an Information Technology framework that includes information security as a component.

## ISO/IEC 27001

The International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) publishes the 27000 family of standards to help organizations keep their information assets secure. It is important to note that these are standards, not just guidelines, suggestions, or recommendations like many other frameworks. This means that organizations can work towards adopting the standard and can receive a certification from an authorizing body in their country / region. However, it's not required for an organization to be certified or even on a certification path to adopt this framework and its corresponding controls.

The ISO/IEC 27001 standard utilizes the concept of an Information Security Management System (ISMS). According to ISO, an ISMS "is a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process."

### Considerations for ISO/IEC 27001 adoption:

- ISO/IEC 27001 outlines an Information Security Management System (ISMS), which serves as the design for an organization's information security program.
- ISO/IEC 27001 certification is available, but not required. Adoption of security controls from ISO/IEC 27002 (discussed later in this document) would be important for an organization that wishes to be certified.
  - Certification for a small company (~75 people) may run upwards of $100k[1].
- The ISO/IEC 27000 standards have broader acceptance outside the U.S. since it is considered an international standard.
  - Organizations that have subsidiaries outside of the U.S. may be well-served to adopt these standards.
- Between 2015 and 2016, ISO/IEC 27001 certification grew at an annual rate of 20%.
  - For 2016, Japan has the most certifications at 27% of all certifications followed by the UK with 10%, India with 9%, and China with 8%. The United States ranks 7th with only 3% of all certifications.
- The cost to procure the baseline documents is around $350 for ISO/IEC 27001 and ISO/IEC 27002 (or $1,200 for a full suite of ISO 27000 documents).

**WHO SHOULD CONSIDER THIS?**

> Organizations that would like to model their information security program against a well-known and robust standard should consider adopting ISO/IEC 27001. This framework provides the greatest degree of international acceptance and is one of the few standards that can provide a pathway to certification.

## NIST CYBERSECURITY FRAMEWORK (CSF)

The U.S. National Institute for Standards and Technology (NIST)[2] Cybersecurity Framework (CSF) was published in response to U.S. Presidential Executive Order (EO) 13636, *Improving Critical Infrastructure Cybersecurity*. First issued in 2014, the framework is "voluntary guidance, based on existing standards, guidelines, and practices… to better manage and reduce cybersecurity risk… it was designed to foster risk and cybersecurity management communications amongst both internal and external organizational stakeholders."[3]

[1] https://www.pivotpointsecurity.com/blog/two-factors-driving-iso-27001-costs/

[2] NIST publishes several documents on information security known as the "Special Publication 800-series". These documents are provided to everyone at no cost and are considered to be guidance, not standards, unless the adopting organization is a U.S. federal entity.

[3] https://www.nist.gov/cyberframework/cybersecurity-framework-faqs-framework-basics

While this framework was intended for critical infrastructure organizations[4], it's in no way limited to those organizations and has been widely adopted by many non-critical infrastructure organizations, both large and small. Some of the key goals of the CSF allow organizations to: describe their current security posture, identify their desired target state, assess progress towards a future state, and provide a framework to communicate all these items to stakeholders.

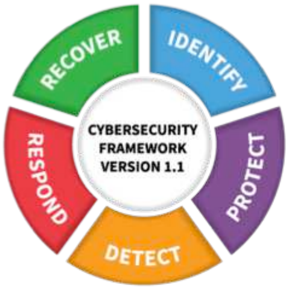
**The NIST CSF consists of three components:**

1. The Core is a description of the desired security outcomes. We find that this is the section most people think of when they are speaking of the CSF.
2. Profiles describe an individual organization's unique requirements, objectives, risk appetite, and resources.
3. Implementation Tiers indicate how an organization manages cybersecurity risks. It's important to recognize that implementation tiers are not a maturity model as there's no expectation that organizations progress through various tiers.

The CSF Core, as the central portion of the document, describes at a high level the five key functions, 23 categories, and 108 subcategories that provide a set of activities to achieve specific cybersecurity outcomes. That is, the group that created the framework identified the key cybersecurity outcomes that help organizations manage risk.

The NIST CSF is not a controls library like ISO/IEC 27002 and NIST SP 800-53, both discussed later in this document, in that it does not offer specific guidance on how to achieve the listed activities. In fact, the CSF uses informative references that map to specific security controls found in controls libraries like ISO/IEC 27002, NIST SP 800-53, and CIS CSC (also described further on in this document).

The NIST CSF should not be confused with other documents published by NIST, particularly the NIST SP 800-53 controls library, *Security and Privacy Controls for Federal Information Systems and Organizations*. We see a lot of confusion on this point and it's an important distinction because they are not one in the same, though the NIST CSF does have a mapping to the NIST SP 800-53 controls.



*Credit: N. Hanacek/NIST*

**Considerations for NIST CSF adoption include the following:**

- One of the most valuable characteristics of the NIST CSF is that it is relatively agnostic when it comes to adoption of security controls. That is, most major controls catalogs are mapped to the CSF giving organizations flexibility in choosing the controls catalog that best suits them.
- While considered “voluntary guidance”, Impact Makers has seen regulators turn to the CSF as an example of what constitutes a minimum baseline for “good security”.

[4] Critical Infrastructure is defined by the Department of Homeland Security and includes industries like financial, communications, manufacturing, energy, healthcare, and utilities. https://www.dhs.gov/critical-infrastructure-sectors

- There is a belief by many information security professionals that this will eventually become a de facto standard in the U.S. for what constitutes a minimum baseline for information security programs.
- Impact Makers has observed a number of organizations, that already adopted a separate information security framework, adopt the NIST CSF either as a supplemental framework or as their primary framework.
- While there is no official certification for the NIST CSF, it's frequently used as baseline for a security program assessment.
- There is no cost for an organization to procure and utilize the NIST CSF documents.

**WHO SHOULD CONSIDER THIS?**

Impact Makers feels that organizations that have not already adopted a security framework should consider the NIST CSF as their starting point. In fact, when we're evaluating an organization to determine the current and future state of their information security program, this is the framework we most commonly use to assist with the assessment.

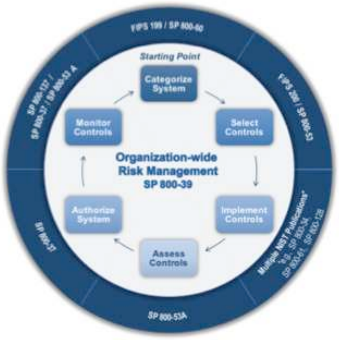
## NIST RISK MANAGEMENT FRAMEWORK

As mentioned above in the NIST CSF section, we commonly see people confuse the NIST Cybersecurity Framework with the NIST SP 800-53 controls library. While both documents are published by NIST, SP 800-53 is a distinct component of the NIST Risk Management Framework (RMF) which is further described in NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*. NIST SP 800-39, *Managing Information Security Risk*, provides additional context. The NIST RMF follows a risk-based view of managing an information security program.

**The RMF is a six-step process cycle that has the following steps and associated documents in parenthesis:**

- Step 1: Categorize (NIST SP 800-60)
- Step 2: Select Controls (NIST SP 800-53)
- Step 3: Implement Controls (NIST SP 800-34, 800-61, 800-128)
- Step 4: Assess Controls (NIST SP 800-34A)
- Step 5: Authorize System (NIST SP 800-37)
- Step 6: Monitor Controls (NIST SP 800-137, 800-37, 800-53A)

As you can imagine, it could be a significant undertaking for a small organization to adopt this type of framework. To help, NIST publishes quick start guides[5] for steps 1 (categorize), 2 (select), and 6 (monitor).



*Credit: NIST*

[5] The NIST Quick Start guides are available here: https://csrc.nist.gov/Projects/Risk-Management/Risk-Management-Framework-Quick-Start-Guides

The NIST RMF should be considered for larger organizations that seek to have a robust information security risk management process. Organizations that are highly regulated and /or perform U.S. government contracting may also be candidates to adopt the NIST RMF. We do not recommend using this approach for organizations that are just starting to build their information security and / or risk management programs, unless they use a partner who is familiar with the framework and can tailor it to their environment.

It's important to note that in practice, and contrary to the intended purpose, we've seen organizations adopt the NIST SP 800-53 controls library as their information security framework. Essentially, organizations structure their information security program around the 18 control families described in the document by creating a policy, standard, and procedures for each family. You can see the control families in the NIST SP 800-53 controls library section below.

**Considerations for adopting the NIST RMF include the following:**

- The NIST RMF provides a robust framework to identify, assess, control, and monitor risks that are essential to any information security program.
- The comprehensive nature of the RMF may make it more suitable for organizations that already have some form of risk awareness across their organization. That is, it may be difficult to implement a framework of this nature if the organization does not already speak the language of risk and have staff who are skilled in implementing a program.
- Organizations that seek to implement the NIST RMF should consider engaging a partner who has implementation experience, such as Impact Makers.
- There is no cost to organizations to download and use the NIST RMF. Although it was designed initially for federal systems, it has good applicability to other industries.

**WHO SHOULD CONSIDER THIS?**

> Impact Makers views the NIST RMF as an extremely robust risk management framework for organizations ready to implement a strong risk management program. We do offer the caveat that this framework should not be approached lightly and it could take external expertise to assist with implementation.

## HITRUST CSF

HITRUST

*Credit: HITRUST Alliance*

The HITRUST Alliance was founded in 2007 and is an independent not-for-profit organization based in the United States HITRUST partners with both the private and public sectors to develop and maintain a risk and compliance management framework. They seek to combine all the requirements of heavily regulated industries into a single framework. Historically, they have focused on the healthcare industry but are also making inroads into the financial services industry through the inclusion of major financial services regulations.

HITRUST offers the HITRUST CSF, which is a certifiable framework that provides organizations an approach to a compliance and risk framework.

The HITRUST CSF is based on the ISO/IEC 27001 and 27002 standards, but also has coverage for 37 major information security standards, regulations, and requirements. A full listing is in Appendix C: HITRUST CSF 9.1 Standards, Regulations, and Frameworks.

The HITRUST CSF is organized by 14 Control Categories, containing 46 Control Objectives and 149 Control Specifications based on ISO/IEC 27001:2005 and 27002:2005. Each Control Specification consists of as many as three implementation levels applied to healthcare organizations according to specific organizational, system, and regulatory factors.

**Considerations for using the HITRUST CSF include the following:**

- The historical focus has been in the healthcare space with only a more recent focus on financial services and healthcare payers. Organizations in other verticals may find that the framework does not work as well for them.
    - According to HITRUST, 81% of hospitals and 80% of health plans have adopted the CSF in some manner.
- While the HITRUST CSF is U.S.-focused, international healthcare organizations that provide services to U.S.-based organizations may benefit from this framework. There currently isn't a CSF version for non-U.S. healthcare providers.
- Qualified organizations can download and use the HITRUST CSF at no cost.
- Since the CSF is so comprehensive, it can take the better part of a year to complete the validation.
- While the CSF is comprehensive, it is not all-inclusive and organizations will still need to modify the framework to suit their needs.
- While there is coverage for PCI and SOC2, becoming HITRUST certified does not necessarily mean that an organization will have met all the requirements for either of those.
    - In the case of the SOC 2 report, an American Institute of CPAs (AICPA) firm may perform the SOC 2 examination using the HITRUST framework to achieve both a HITRUST certification and generate a SOC 2 report.
- HITRUST offers a governance, risk, and compliance (GRC) tool in the cloud, called "MyCSF". Costs for this tool range from $10k for an organization with less than 25 employees to an unlimited user solution for $75k.

WHO SHOULD CONSIDER THIS?

Organizations that are involved in healthcare delivery and payments would be well-suited to evaluate HITRUST for adoption since it covers many of the unique regulations of healthcare.

## COBIT

Now in its fifth iteration, COBIT 5 describes best practices for the management of information technology. Unlike the previously mentioned frameworks (ISO/IEC 27001, NIST CSF, and HITRUST), it is not specific to information security, though it does contain many information security controls.

**Considerations for using COBIT include the following:**

- Valuable for publicly-held companies that need to meet the requirements in the Sarbanes-Oxley Act, specifically Section 404, which requires assessment of the effectiveness of internal controls for financial reporting.
- The COBIT 5 publication is available in digital form at no cost to ISACA members and $165 for non-members. A companion guide, "COBIT 5 for Information Security", is $50 for ISACA members and $90 for non-members.

Impact Makers has not observed the broad adoption of COBIT specifically for information security. Where we have seen it adopted, it's been used in conjunction with other information security-specific frameworks. Organizations that are interested in the broad governance of all of Information Technology may be well-suited to adopt the COBIT framework.

**WHO SHOULD CONSIDER THIS?**

> Organizations that have a desire to apply governance not only to information security, but to all of IT, should consider the COBIT framework.

## INFORMATION SECURITY CONTROLS LIBRARIES

An information security controls library is a list of common security controls, typically organized around a family or category. Think of a controls library as a menu of choices for what organizations should consider putting in place to protect its data and systems. The expectation with any security controls library is that an organization tailors it to meet its specific needs and risk profile.

Two of the most common and comprehensive information security controls libraries are documented by ISO/IEC 27002 and NIST SP 800-53. These documents, by themselves, do not describe how to build an information security program, establish governance of that program, or how to identify and treat risks. They are simply listings of common information security and privacy controls that are considered best practices.

Controls are offered as libraries since not all controls are appropriate for all organizations or systems within that organization. It's important to note that a particular control may be applicable for a system that contains confidential data, but the same control may be overkill for a system that is publicly accessible. Some controls libraries identify controls that are appropriate for different criticalities of systems; that is, controls that are appropriate for extremely critical systems versus controls that are appropriate for less critical systems.

While an information security controls library provides a good starting point for an organization to build its policies, standards, and procedures, it is highly unlikely that the controls library will contain every conceivable control that the organization will need. This is driven in part by the unique regulatory environment in which each organization operates. There are various federal, state, and industry regulations around privacy and security that an organization will need to account for and, as a result, design unique information security controls that are not found in existing libraries.

To provide a sense of the level of detail included in each controls library, a sample, focusing on data backups, is provided in Appendix B: Sample Controls Statements and Guidance for each library.

ISO/IEC27002 and NIST SP 800 53 are considered to contain the most comprehensive lists of security controls and also offer guidance on how to accomplish each control statement.

Organizations are not restricted to using a single controls library to identify all the controls in its security program. In fact, more organizations (44%) pull from multiple libraries and frameworks than use a single controls library / framework (40%), as reported by a 2016 Dimensional Research survey[6]. With that said, if you are just starting to build or formalize your information security program, it's probably best that you start with a single controls library.

**Both controls libraries (ISO/IEC 27002 and NIST SP 800-53):**

- Help align security programs to best practices, allowing organizations to build comprehensive policies, standards, and procedures based on its requirements and risk appetite, which defines the maximum amount of risk an organization is willing to accept in the pursuit of its objectives
- Permit regulators and auditors to quickly understand the design of the information security program
- Provide a comprehensive list of information security controls along with guidance on how to implement the controls
- Map to the NIST Cybersecurity Framework (CSF)
- Require significant work to customize the controls statements to meet the organization's specific requirements and risk tolerance
- Do not specify the scope of the controls by themselves; controls could cover the entire organization of just a particular service offering or system
- Do not make specific provisions to meet PCI compliance (in some cases, PCI requirements are more prescriptive than controls listed in either framework)
- May not take into account specific privacy requirements, including state and federal regulations (e.g. Gramm-Leach-Bliley Act (GLBA), and the Health Insurance Portability and Accountability Act of 1996 (HIPAA))
- Do not take into account specific U.S. state privacy and / or cybersecurity provisions (e.g. Commonwealth of Massachusetts 201 CMR 17.00, New York State Department of Financial Services 23 NYCRR 500, etc.), though it is likely that many requirements are found in the controls frameworks

## ISO/IEC 27002

It's important to understand the relationship between ISO/IEC 27001 and ISO/IEC 27002. As mentioned above, ISO/IEC 27001 is a standard, focused on the design of the information security management system (ISMS). ISO/IEC 27002 consists of best practice controls that map to the objectives in ISO/IEC 27001. Therefore, unlike ISO/IEC 27001, ISO/IEC 27002 by itself is not a certifiable standard. The controls in ISO/IEC 27002 are subject to the organization's needs and are not considered mandatory, though many regulators and auditors will look for fundamental controls to be in place.

[6] "Trends in Security Framework Adoption", Dimensional Research, 2016

Annex A of ISO/IEC 27001 contains an overview of 114 security controls or objectives. The annex provides high-level organizational objectives for each control, but does not state how they should be met or implemented.

ISO 27001 offers guidance on how to govern an information security management system and identify which controls to implement.

ISO 27002 has the same structure as Annex A of ISO 27001, but gives a more detailed explanation on how to implement it. The controls are organized into 14 sections covering topics such as physical security, personnel security, and operational security.

| ID | FAMILY | ID | FAMILY |
|---|---|---|---|
| 5. | Information Security Policies | 12. | Operation Security |
| 6. | Organization of Information Security | 13. | Communication Security |
| 7. | Human Resource Security | 14. | System Acquisition, Development & Maintenance |
| 8. | Asset Management | 15. | Supplier Relationships |
| 9. | Access Control | 16. | Information Security Incident Management |
| 10. | Cryptography | 17. | Information Security Aspects of Business Continuity Management |
| 11. | Physical and Environmental Security | 18. | Compliance |

*Table 1: ISO/IEC 27002 Control Families*

ISO/IEC 27002 provides implementation guidance for controls. For example, a control may state "Backup copies of information, software, and system images should be taken and tested regularly in accordance with an agreed backup policy." The implementation guidance builds on that statement to specify things such as ensuring that backup procedures are in place, restoration capabilities are regularly tested, backup media is physically and electronically protected, and media is stored an appropriate distance away from the primary data to mitigate the impact of disasters.

**Considerations for ISO/IEC 27002 adoption include the following:**

- Organizations can't be certified against ISO/IEC 27002, but can for ISO/IEC 27001. Adoption of the security controls described in ISO/IEC 27002 would be important for an organization wishing to be certified for ISO/IEC 27001
  - Certification for small company (~75 people) may run upwards of $100k[7]
- The ISO/IEC 27000 standards have broader acceptance outside the U.S. since it is considered an international standard
  - U.S.-based organizations that have subsidiaries outside of the U.S. may be well-served to adopt these standards
  - The ISO/IEC 27000 standards form the baseline for the HITRUST CSF

[7] https://www.pivotpointsecurity.com/blog/two-factors-driving-iso-27001-costs/

- The cost to procure the baseline documents is about $350 for both ISO/IEC 27001 and ISO/IEC 27002 (or $1,200 for a full suite of ISO 27000 documents)
  - Other key documents in the ISO/IEC 27000 family include:
    - ISO/IEC 27003 – Information Security Management System Implementation Guidance
    - ISO/IEC 27004 – Information Security Risk Management – Measurement
    - ISO/IEC 27005 – Information Security Risk Management

**WHO SHOULD CONSIDER THIS?**

> Along with NIST SP-800-53, Impact Makers feels that the ISO 27002 controls library is exceptionally comprehensive. Organizations that operate in multiple countries and need to have a robust set of security controls that align to a well-established information security framework should consider ISO/IEC 27001.

### NIST SP 800-53

NIST Special Publication (SP) 800-53 is the document that provides a catalog of security controls for federal information systems. All federal agencies, except those involved in national security, are expected to comply with NIST policies and standards within one year of publication date. While the publication is designed for the U.S. government systems, there is nothing to preclude a private-sector organization from utilizing the document to design its information security controls. In fact, many private-sector organizations do exactly that.

The latest draft revision of NIST SP 800-53, revision 5, includes 20 control families and includes both security and privacy requirements that are consistent with national and international standards and regulations. Requirements and controls from defense, financial, healthcare, intelligence, manufacturing, industrial, and audit communities were used to compile this comprehensive catalog of controls.

| ID | FAMILY | ID | FAMILY |
|---|---|---|---|
| AC | Access Control | MP | Media Protection |
| AT | Awareness and Training | PA | Privacy Authorization |
| AU | Audit and Accountability | PE | Physical and Environmental Protection |
| CA | Security Assessment and Authorization | PL | Planning |
| CM | Configuration Management | PS | Personnel Security |
| CP | Contingency Planning | RA | Risk Assessment |
| IA | Identification and Authentication | SA | System and Services Acquisition |
| IP | Individual Participation | SC | System and Communications Protection |
| IR | Incident Response | SI | System and Information Integrity |
| MA | Maintenance | PM | Program Management |

*Table 2: NIST SP 800-53r5 Control Families*

**Considerations for adoption of NIST SP 800-53 include the following:**

- Since NIST SP 800-53 is not a standard, there is no certification available for private sector organizations
- This control library is used by the U.S. federal government, so organizations that need to align with U.S. government standards (e.g. contracting) may be well-served to utilize these controls
- It may be viewed as being U.S.-centric by those outside the U.S.
  - Organizations that operate in multiple countries should discuss the use of NIST documents with their colleagues, compliance teams, and leadership to understand challenges for adoption and acceptance by non-U.S. regulators
- NIST 800-53 is a controls library only and does not formally provide for the design of a security program or ISMS
- All NIST Special Publications are freely available to both the private and public sectors

**WHO SHOULD CONSIDER THIS?**

> Impact Makers views NIST SP 800-53 as the "gold standard" for information security controls frameworks. If you're willing to take the time to understand the NIST Risk Management Framework and want to have a comprehensive set of security controls, this is a great place to start.

## CENTER FOR INTERNET SECURITY CONTROLS (CIS CSC)

This controls library was previously known as the "SANS Top 20 Security Controls". The premise is that if most organizations would focus on the top 20 security controls, they would cover practically all of their information security risk. This premise is extended to state that organizations focused on the first five controls will mitigate the vast majority of their information security risks.

**Considerations for adoption of the CIS CSC include the following:**

- The CIS Controls are available at no charge to organizations
- The CIS Controls are listed as informative references in the NIST CSF Core
- Mappings are available between the CIS Controls and numerous other frameworks, including NIST 800-53 and ISO/IEC 27002
- In a 2016 Data Breach Report[8] from the State of California, the 20 controls were described as "…a minimum level of security – a floor – that any organization that collects or maintains personal information should meet." As the headquarters for a number of Internet companies and the sixth largest global economy, the reference to the CIS Controls carries significant weight.

**WHO SHOULD CONSIDER THIS?**

> Impact Makers feels that smaller organizations that are not planning to adopt a full information security framework and comprehensive controls library should strongly consider the CIS CSC. For organizations that do not currently have an information security program, it is a good place to start in order to address information security risks. While there's a lot of effort to implement some of the controls, it's easy to digest and explain to management and other stakeholders.

[8] https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf

## CONCLUSION

Practically every organization has a need to protect confidential information, whether that information is customer data, intellectual property, or employee data. In order to understand how to best protect that information, organizations should consider the risks regarding the loss of confidentiality, integrity, and availability and build an information security program that's appropriate to protect the information. Information security frameworks form the foundation of a well-run information security program.

There is no right or wrong controls catalog or framework listed in this document. They all have tradeoffs and will almost always require some level of customization to effectively cover all the risks an organization is likely to face. With that said, every organization would be well served by selecting any of the best-practice documents listed in this whitepaper over nothing at all. Additionally, these frameworks and controls catalogs should be well-understood by regulators, offering an advantage over building a framework and selecting controls from scratch. Organizations must understand the limitations of information security frameworks and controls catalogs. They typically take some time to customize to meet the risk needs of the organization. They also don't include specific regulatory or privacy requirements such as PCI or HIPAA, which will need to be considered as an organization builds their information security and privacy program. Partnering with a consulting firm that has experience in implementing information security frameworks and controls will help organizations quickly identify what should and should not be in their information security program.

**TELL US WHAT YOU THINK**

> We already have some ideas for the next version of this document including how ITIL can be leveraged for information security. If you have topic requests for future versions of this document or would like to discuss how to implement an information security framework and/or controls library at your organization, contact us at http://www.impactmakers.com/contact/.

## ABOUT IMPACT MAKERS

Impact Makers is an IT and management consulting firm that helps companies manage transformation across data, cloud, security, and people in the healthcare, financial services, and public sectors. We're committed to creating meaningful change and value for our clients and our community partners, contributing 100% of net profits to the community over the life of the company.

Impact Makers' information security professionals average over 20 years of IT and information security experience and include individuals such as Ron White, a former Chief Security Officer for a shipping and logistics company operating in all 50 states, who was a key contributor and reviewer for this document.

# APPENDIX A: REFERENCES

| CONTROLS LIBRARY / INFORMATION SECURITY FRAMEWORK | ISSUING ORGANIZATION | CURRENT VERSION (as of July 2018) | LINK |
|---|---|---|---|
| NIST SP 800-53 | The National Institute for Standards and Technology (NIST) | Revision 4[9]<br>Revision 5 *(draft)* | http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf<br>https://csrc.nist.gov/CSRC/media//Publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf |
| NIST Cybersecurity Framework | The National Institute for Standards and Technology (NIST) | 1.1 | https://www.nist.gov/cyberframework |
| ISO/IEC 27001 & 27002 | International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) | 2013 | https://webstore.ansi.org/RecordDetail.aspx?sku=ISO%2FIEC+27000+Information+Technology+Security+Techniques+Collection |
| HITRUST CSF | HITRUST Alliance | 9.1 | https://hitrustalliance.net/hitrust-csf/ |
| COBIT | ISACA (previously Information Systems Audit and Control Association, now just the acronym) | 5 | http://www.isaca.org/cobit/pages/default.aspx |
| CIS Controls *(formerly known as the SANS Top 20 Security Controls)* | Center for Internet Security | 7 | https://www.cisecurity.org/controls/ |

[9] Revision 5 is currently in draft and expected to be published in 2018

# APPENDIX B: SAMPLE CONTROLS STATEMENTS & GUIDANCE

**ISO/IEC 27002**

12.3: Backup

**Control**

Backup copies of information, software, and system images should be taken and tested regularly in accordance with an agreed backup policy.

**Implementation guidance**

A backup policy should be established to define the organization's requirements for backup of information, software, and systems. The backup policy should define the retention and protection requirements. Adequate backup facilities should be provided to ensure that all essential information and software can be recovered following a disaster or media failure. When designing a backup plan, the following items should be taken into consideration:

**a.** Accurate and complete records of the backup copies and documented restoration procedures should be produced.
**b.** The extent (e.g. full or differential backup) and frequency of backups should reflect the business requirements of the organization, the security requirements of the information involved, and the criticality of the information to the continued operation of the organization.
**c.** The backups should be stored in a remote location, at a sufficient distance to escape any damage from a disaster at the main site.
**d.** Backup information should be given an appropriate level of physical and environmental protection (see Clause 11) consistent with the standards applied at the main site.
**e.** Backup media should be regularly tested to ensure that they can be relied upon for emergency use when necessary; this should be combined with a test of the restoration procedures and checked against the restoration time required. Testing the ability to restore backed-up data should be performed onto dedicated test media, not by overwriting the original media in case the backup or restoration process fails and causes irreparable data damage or loss.
**f.** In situations where confidentiality is of importance, backups should be protected by means of encryption.

Operational procedures should monitor the execution of backups and address failures of scheduled backups to ensure completeness of backups according to the backup policy. Backup arrangements for individual systems and services should be regularly tested to ensure that they meet the requirements of business continuity plans. In the case of critical systems and services, backup arrangements should cover all systems information, applications, and data necessary to recover the complete system in the event of a disaster. The retention period for essential business information should be determined, taking into account any requirement for archive copies to be permanently retained.

**NIST SP 800-53r4**

CP-9 INFORMATION SYSTEM BACKUP

**Control**

The organization:

- **a.** Conducts backups of user-level information contained in the information system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives];
- **b.** Conducts backups of system-level information contained in the information system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives];
- **c.** Conducts backups of information system documentation including security-related documentation [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; and
- **d.** Protects the confidentiality, integrity, and availability of backup information at storage locations.

**Supplemental Guidance:**

System-level information includes, for example, system-state information, operating system and application software, and licenses. User-level information includes any information other than system-level information. Mechanisms employed by organizations to protect the integrity of information system backups include, for example, digital signatures and cryptographic hashes. Protection of system backup information while in transit is beyond the scope of this control. Information system backups reflect the requirements in contingency plans as well as other organizational requirements for backing up information. Related controls: CP-2, CP6, MP-4, MP-5, SC-13.

**NIST CSF**

**Subcategory**

PR.IP-4: Backups of information are conducted, maintained, and tested periodically.

**Informative References**

- COBIT 5 APO13.01
- ISA 62443-2-1:2009 4.3.4.3.9
- ISA 62443-3-3:2013 SR 7.3, SR 7.4
- ISO/IEC 27001:2013 A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3
- NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9

**CIS CONTROLS**

**Control**

CSC 10: Data Recovery Capability

The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.

**Why Is This Control Critical?**

When attackers compromise machines, they often make significant changes to configurations and software. Sometimes attackers also make subtle alterations of data stored on compromised machines, potentially jeopardizing organizational effectiveness with polluted information. When the attackers are discovered, it can be extremely difficult for organizations without a trustworthy data recovery capability to remove all aspects of the attacker's presence on the machine.

**Control Description**

**10.1** Ensure that each system is automatically backed up on at least a weekly basis, and more often for systems storing sensitive information. To help ensure the ability to rapidly restore a system from backup, the operating system, application software, and data on a machine should each be included in the overall backup procedure. These three components of a system do not have to be included in the same backup file or use the same backup software. There should be multiple backups over time, so that in the event of malware infection, restoration can be from a version that is believed to predate the original infection. All backup policies should be compliant with any regulatory or official requirements.

**10.2** Test data on backup media on a regular basis by performing a data restoration process to ensure that the backup is properly working.

**10.3** Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.

**10.4** Ensure that key systems have at least one backup destination that is not continuously addressable through operating system calls. This will mitigate the risk of attacks like CryptoLocker which seek to encrypt or damage data on all addressable data shares, including backup destinations.

**COBIT 5**

**Management Practice**

DSS04.07 Manage backup arrangements. Maintain availability of business-critical information.

**Activities**

**1.** Back up systems, applications, data, and documentation according to a defined schedule, considering:

1. Frequency (monthly, weekly, daily, etc.)
2. Mode of backup
   (e.g., disk mirroring for real-time backups vs. DVD-ROM for long-term retention)
3. Type of backup (e.g., full vs. incremental)
4. Type of media
5. Automated online backups
6. Data types (e.g., voice, optical)
7. Creation of logs
8. Critical end-user computing data (e.g., spreadsheets)
9. Physical and logical location of data sources
10. Security and access rights
11. Encryption

**2.** Ensure that systems, applications, data, and documentation maintained or processed by third parties are adequately backed up or otherwise secured. Consider requiring return of backups from third parties, as well as escrow or deposit arrangements.

**3.** Define requirements for on-site and off-site storage of backup data that meet the business requirements. Consider the accessibility required to back up data.
**4.** Roll out BCP awareness and training.
**5.** Periodically test and refresh archived and backup data.

## APPENDIX C: HITRUST CSF 9.1 STANDARDS, REGULATIONS, & FRAMEWORKS

- 16 CFR Part 681 – Identity Theft Red Flags
- 201 CMR 17.00 – State of Massachusetts Data Protection Act: Standards for the Protection of Personal Information of Residents of the Commonwealth
- American Institute of Certified Public Accountants (AICPA) Trust Services Principles and Criteria: Security, Confidentiality and Availability
- California Civil Code § 1798.81.5(b) (mapped to CIS CSC v6): CA Attorney General Interpretation of "Reasonable Security Procedures"
- Center for Internet Security (CIS) Critical Security Controls (CSC) v6: Critical Security Controls for Effective Cyber Defense
- Cloud Security Alliance (CSA) Cloud Controls Matrix Version 1.1
- CMS Information Security ARS 2013 v2: CMS Minimum Security Requirements for High Impact Data
- COBIT 4.1 (with associated mappings to COBIT 5): Deliver and Support Section 5 – Ensure Systems Security
- Department of Homeland Security (DHS) Critical Resilience Review (CRR)
- EU General Data Protection Regulation (GDPR)
- Federal Register 21 CFR Part 11: Electronic Records; Electronic Signatures
- Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable,
- Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements
- Federal Financial Institutions Examination Council (FFIEC) Information Technology (IT) Examination Handbook – Information Security, September, 2016
- Federal Register 21 CFR Part 11: Electronic Records; Electronic Signatures
- Federal Risk and Authorization Management Program (FedRAMP)
- Health Information Trust Alliance (HITRUST) De-Identification (De-ID) Framework: De-identification Controls Assessment (DCA)
- HIPAA – Federal Register 45 CFR Part 164, Subpart C: HIPAA Administrative Simplification: Security Standards for the Protection of Electronic Protected Health Information (Security Rule)
- HIPAA – Federal Register 45 CFR Part 164, Subpart D: HIPAA Administrative Simplification: Notification in the Case of Breach of Unsecured Protected Health Information (Breach Notification Rule)
- HIPAA – Federal Register 45 CFR Part 164, Subpart E: HIPAA Administrative Simplification: Privacy of Individually Identifiable Health Information (Privacy Rule)
- IRS Publication 1075 v2014: Tax Information Security Guidelines for Federal, State and Local Agencies: Safeguards for protecting Federal Tax Returns and Return Information
- ISO/IEC 27001:2005: Information technology – Security techniques – Information security management systems - Requirements
- ISO/IEC 27001:2013: Information technology – Security techniques – Information security management systems - Requirements
- ISO/IEC 27002:2005: Information technology – Security techniques – Code of practice for information security management

- ISO/IEC 27002:2013: Information technology – Security techniques – Code of practice for information security controls
- ISO/IEC 27799:2008: Health informatics – Information security management in health using ISO/IEC 27002
- Joint Commission (formerly the Joint Commission on the Accreditation of Healthcare Organizations, JCAHO)
- MARS-E v2.0: Catalog of Minimum Acceptable Risk Controls for Exchanges Exchange Reference Architecture Supplement
- New York State Department of Financial Services – Title 23 NYCRR Part 500
- NIST Framework for Improving Critical Infrastructure Cybersecurity v1.0: Framework Core – Subcategories
- NIST Special Publication 800–53 Revision 4 (Final), including Appendix J – Privacy Control Catalog: Security Controls for Federal Information Systems and Organizations
- NIST Special Publication 800–66: An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule
- NRS: Chapter 603A – State of Nevada: Security of Personal Information
- Office of Civil Rights (OCR) Audit Protocol April 2016 – HIPAA Security Rule
- Payment Card Industry (PCI) Data Security Standard Version 3.2: Information Management (IM) Standards, Elements of Performance, and Scoring
- Precision Medicine Initiative Data Security Policy Principles and Framework v1.0: Achieving the Principles through a Precision Medicine Initiative Data Security Policy Framework
- Texas Health and Safety Code § 181 – State of Texas: Texas Medical Records Privacy Act
- Title 1 Texas Administrative Code § 390.2 – State of Texas: Standards Relating to the Electronic Exchange of Health Information

## VERSION HISTORY

| VERSION | DATE | SUMMARY OF CHANGES |
|---|---|---|
| 1.0 (initial) | July 25, 2018 | Initial release |
| | | |
| | | |