NAACCR Cybersecurity Framework and Audit Primer

Version 1.0

Author:

David Chesnut, Information Management Services, Inc.

Editors:

Recinda Sherman, North American Association of Central Cancer Registries

Robert McLaughlin, Cancer Registry of Greater California

Bozena M. Morawski, Cancer Data Registry of Idaho

Carolyn Bancroft, Maine Cancer Registry

Lauren Maniscalco, Louisiana Tumor Registry

Castine Clerkin, North American Association of Central Cancer Registries

Steven Friedman, National Cancer Institute, National Institutes of Health

Tabassum Insaf, New York State Cancer Registry

Selina Khatun, Nunavut Cancer Registry

Carmina Ng, Canadian Cancer Registry – Statistics Canada

Anshu Shrestha, Cancer Registry of Greater California

Qianru Wu, Nebraska Cancer Registry

Publication Date[1]: April 17, 2025

[1] These guidelines should be reviewed and updated every 12 months.

Table of Contents

Introduction

Do you know if ALL the sensitive data entrusted to your registry are secure? Would you be able to prove that your registry's data are secure if you were asked to do so?

These two simple questions cut to the crux of why a cybersecurity framework, and the implementation and auditing of the security controls prescribed by the framework are important for central cancer registries and their personnel. A cybersecurity framework and audits of the associated security controls allow a registry to answer these two questions with credibility and confidence.

Having a cybersecurity framework and conducting audits go a long way to demonstrate that a registry satisfies its duties to protect sensitive data with care. When an incident occurs, a cybersecurity framework is instrumental to effective, corrective, and preventive actions. Security incidents do happen, even in registries that have diligently worked to reduce the likelihood of incidents and are prepared to respond. Furthermore, if a cybersecurity framework is not used or audits are not conducted, it does not mean that a registry's data are insecure! However, implementing a cybersecurity framework helps an organization prevent incidents from happening and provides a framework for what should be done when incidents do occur.

Cybersecurity frameworks exist because no one person knows everything that there is to know about security and privacy. Cybersecurity frameworks have been created by knowledgeable professionals with real world experience in addressing the general security and privacy of an organization and the data that they are entrusted to protect.

Does that mean that a cybersecurity framework is a recipe for what must be done and includes all that needs to be done for data to be safe? The answer is yes and no. A cybersecurity framework, like the name implies, is a frame for a cybersecurity program; the framework is NOT the entire program, but the structure upon which to build a comprehensive cybersecurity program. A cybersecurity framework can be thought of as the internal structure of a building, including the foundation and steel I-beams that provide the walls and floor. The framework itself is not the whole building – there are still internal walls, doors, plumbing, electrical, heating, ventilation, air conditioning, and a myriad of other systems that create the entire building. Similarly, a cybersecurity framework provides the foundation and the structure of a cybersecurity program and is not readily apparent at first glance.

An overall cybersecurity program is tailored to meet the needs of a particular organization. Because no two organizations – including cancer registries – are the same, the individual parts and pieces of the framework may look very different from organization to organization. Each cancer registry must comply with different state laws, different parent organizations, and so forth. Therefore, a cybersecurity program created around a core cybersecurity framework will probably look different for each registry. This is okay because the core principles, or the basic framework, should be the same.

In keeping with the building analogy, cybersecurity audits are like building inspections. All buildings are required to have different inspections to ensure that they are safe for people to be in and to ensure that the builders have complied with the local building codes and best practices. A cybersecurity audit does a similar thing for an organization's cybersecurity program. The cybersecurity audit is meant to show that the organization is following standard practices, typically laid out by a cybersecurity framework, for

privacy and security. The audit is also meant to expose areas where the program may not be up to standard so that those issues can be addressed to make the overall cybersecurity program better.

Document Scope

This primer provides high-level information about various cybersecurity frameworks that are available to registries and some industry-standard audits that can be used to check compliance with the standards and guidelines outlined in cybersecurity frameworks. It is a point of departure for the journey on the cybersecurity road to securing data. That journey will never end, but the more we travel principled, reasoned, and rigorous paths, the more we will understand and the more secure the data entrusted to registries will be.

Because registry personnel may be asked to participate in the creation, implementation, and review of activities prescribed by a framework and/or an audit, registry personnel should understand:

1. what cybersecurity frameworks are; and
2. the role and functions of audits in an organization's cybersecurity program.

The overall goal of a registry is to further scientific understanding of how cancer affects our population. Collection and storage of sensitive data are central to achieving this goal, and these data must be kept secure. Everyone in the registry community must "be on the same page" about the importance of data security; this way, sensitive information will stay private and confidential while remaining the paramount data resource of a registry.

This primer is **NOT** an in-depth study of the many different cybersecurity frameworks that can be put into place, nor does it offer an in-depth study of the different industry standard audits that are available. There are already multiple books, white papers, and articles written on these topics. It is **NOT** a how-to guide for implementing information security and privacy.

It is worth mentioning that not all cybersecurity frameworks listed in this document are freely available. The NIST frameworks and their documentation are freely provided, but commercial frameworks like ISO and SOC must be purchased from their respective organizations for an appropriate cost.

Terms, Definitions, and References

The table below lists some terms and references that are commonly used in the cybersecurity world but may not be familiar to registry personnel. Like cancer data collection, when it comes to security, having a common set of definitions helps everyone. Too often, definitions get lost in translation between the data/system owner, project manager, software developer, and system auditor, so a clear starting point is a must.

Term	Acronym	Definition	Reference(s)
Cybersecurity Framework	N/A	A defined set of structured guidelines to help organizations manage and mitigate security and privacy risk.	
Cybersecurity Program	N/A	The implementation of process, procedures, and guidelines in a structured way to mitigate cybersecurity risks within an organization.	
National Institute of Standards and Technology	NIST	Mission statement: To promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.	https://csrc.nist.gov/
Federal Information Security Management Act	FISMA	FISMA 2002, part of the E-Government Act (Public Law 107-347), was passed in December 2002. FISMA 2002 requires each U.S. federal agency to develop, document, and implement an agency-wide program to provide information security for the information and systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other sources.	https://csrc.nist.gov/Projects/risk-management/fisma-background
Federal Risk and Authorization Management Program	FedRAMP®	FedRAMP was established in 2011 to provide a cost-effective, risk-based approach for the adoption and use of cloud services by the U.S. federal government.	https://www.fedramp.gov/program-basics/

Term	Acronym	Definition	Reference(s)
Cybersecurity & Infrastructure Security Agency	CISA	U.S. government agency that has taken the operational lead for federal cybersecurity and national coordination for critical infrastructure and security resilience. CISA's mission is to lead the national effort to understand, manage, and reduce risk to cyber and physical infrastructure.	https://cisa.gov/
Canadian Centre for Cyber Security	N/A	The Canadian Centre for Cyber Security (the Cyber Centre) is part of the Communications Security Establishment in Canada. It is the single unified source of expert advice, guidance, services, and support on cybersecurity for Canadians.	https://www.cyber.gc.ca/
American Institute of Certified Public Accountants	AICPA	Authors and regulators of the Service and Organization Controls (SOC) controls.	https://www.aicpa-cima.com/home
System and Organization Controls	SOC	Security controls, called "principles," developed by the AICPA. There are different sets of SOC principles depending on what is being protected or audited. SOC is currently the U.S. industry standard.	https://www.aicpa-cima.com/resources/landing/system-and-organization-controls-soc-suite-of-services
SOC 2	SOC 2	Set of "trust service principles" developed by AICPA that are used for securing data. The principles include security, availability, processing integrity, confidentiality, and privacy. Depending on the system, some or all of the principles are included in an audit.	https://www.aicpa-cima.com/topic/audit-assurance/audit-and-assurance-greater-than-soc-2
International Standards Organization	ISO	The ISO 27000 series of documents is currently the industry standard for data security in most places outside of the U.S. However, many U.S. organizations also use and adhere to these standards.	https://www.iso.org
Center for Internet Security	CIS	Organization known and accepted by the industry for providing secure system baseline configuration.	https://www.cisecurity.org

Term	Acronym	Definition	Reference(s)
Security Control	N/A	A safeguard or countermeasure prescribed for an information system, or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.	https://csrc.nist.gov/glossary/term/security_control
Privacy Control	N/A	Administrative, technical, and physical safeguards employed within an agency to ensure compliance with applicable privacy requirements and manage privacy risks.	https://csrc.nist.gov/glossary/term/privacy_control
Security Audit/ Audit	N/A	A comprehensive overview of an organization's IT security control implementation and general security posture. **In this document usually referred to as an Audit.	
Audit Finding/ Finding	N/A	A Finding is a comment by an auditor on the effectiveness or design of a Security or Privacy control. A typical Finding will detail a risk to the system or organization that the auditor uncovered during their audit activities. A Finding will document: - the condition that caused the risk; - the criteria being used to evaluate; - the effect the exposed risk might have on the system or organization; and - any recommendations for addressing the risk. A Finding can range from minor issues, like system documentation not being updated in the past year, to critical issues, like sensitive data being stored unencrypted on thumb drives and left out on employees' desks. The level of the Finding and why it matters is typically detailed by the auditor in a report.	
Vulnerability	N/A	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.[5]	https://csrc.nist.gov/glossary/term/vulnerability

Term	Acronym	Definition	Reference(s)
Compensating Control	N/A	Management, operational, and/or technical control (i.e., safeguard or countermeasure) employed by an organization in lieu of a recommended security control in the low, moderate, or high baselines that provides equivalent or comparable protection for an information system.	https://csrc.nist.gov/glossary/term/compensating_controls
Gap Analysis/ Gap Assessment	N/A	Process of comparing the current set of security controls for a system against a set of expected security controls. This is not a formal audit and does not usually generate a formal audit report. It is typically used in preparation for a formal audit.	
Third Party Assessment Organization	3PAO	Company that is independent from the company, service, or system being audited. In the U.S. federal space (FedRAMP), a 3PAO must be an assessment organization that is certified by the FedRAMP program to assess FedRAMP systems.	
System Security Plan	SSP	Formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements. This is typically a term used by the U.S. Government.	https://csrc.nist.gov/glossary/term/system_security_plan
System Assessment Report	SAR	Document that provides a disciplined and structured approach for documenting the findings of the assessor and the recommendations for correcting any identified vulnerabilities in the security controls.	https://csrc.nist.gov/glossary/term/security_assessment_report
Plan of Action and Milestones	POA&M	Document containing plans for fixing or implementing security controls to address vulnerabilities in the existing system.	

Data Security & Data Privacy

This section on data security and data privacy is provided because many of the terms used in cybersecurity frameworks directly reference security alone. However, terms like "Security Control," "System Security Plan (SSP)," "Security Assessment Report (SAR)," encompass both security and privacy. In many instances, especially at a registry, privacy motivates security measures and privacy interests have relevance in security measures in more ways than one might think.

Data security and data privacy are often used to refer to the same thing: the protection of data. While they have similar goals – the protection of data – privacy and security are not the same thing. Data security can be defined in terms of the confidentiality, integrity, and the availability of the data. It encompasses providing data on a need-to-know basis (confidentiality); keeping data safe from inappropriate alteration (integrity); and having data available when it is needed (availability). However, data security does not deal with the legal rights of individuals to have their data protected. That is where data privacy comes in. Data privacy, sometimes called information privacy, is the legal right an individual has to have some control over and knowledge about how their personal information is collected, used, and protected. This legal right is given to them by the governments that represent them. In the U.S., basic privacy rights are granted by the Privacy Act of 1974 and the Health Insurance Portability and Accountability Act of 1996. There are other U.S. federal and state laws (as well as regulations) that govern information privacy rights. For Canada, the main privacy laws are the Privacy Act and the Personal Information Protection and Electronic Documents Act.

For U.S. central cancer registries, these are not the only laws that govern data privacy. For example, section 301 of the U.S. Public Health Services Act [42 U.S.C 241] authorizes the National Program of Cancer Registries to collect cancer data on individuals for the public good; this involves individual-level, private, and confidential medical information and individual identifiers.

In Canada, the government statistics office, Statistics Canada, is tasked with the collection of cancer data for the public welfare. The laws of these Canadian jurisdictions include statements about how the individual's data must remain confidential and only be used for intended, authorized purposes. These are the key tenets of data privacy: the idea and the expectation of an individual that the data collected about them is kept confidential, that only people that need access to it have that access, and that it is only used for the purpose it was collected for.

How does this fit into a discussion about auditing and cybersecurity frameworks? In a nutshell, data privacy depends on good data security. However, having good data security does not necessarily mean there is also good data privacy. Good data privacy means that in addition to keeping data confidential, the data that are collected are only used for the purpose for which the data are intended to be used. It also means that if an employee or researcher does not need a particular piece of private information or is not authorized or permitted to access or use that information, the information is not provided. Well-structured cybersecurity programs take all of this into account. The cybersecurity framework and the associated audit review enable registries to evaluate whether appropriate security controls have been implemented to address both security and privacy considerations within the registry's overall cybersecurity program. An example of where privacy comes into play is the NAACCR Data Release Guidelines, which "outline the steps that a [central cancer] registry can responsibly take prior to, during, and after data release to ensure patient confidentiality while […] supporting the utility of cancer data."

Many of the newer cybersecurity frameworks take both privacy and security into account in their requirements for creating a healthy program. Both the NIST RMF and NIST CSF combine privacy and security into their control definitions. Other frameworks such as SOC and ISO have separate sets of privacy controls that should be addressed to protect the privacy of individuals. Below is an example of a simple cybersecurity control and an explanation of where both data privacy and data security overlap.

Control: Web page logging

> The system must log all access to the web page.

Security context:

> All access should be monitored and logged so that errors can be identified, and anomalous activity such as web server break-in attempts can be identified and mitigated.

Privacy context:

> Access to a web page can be tracked using log files with information such as IP address, browser identity, and other fields that may be logged for "security reasons." However, this data should be kept private since it could be used to track or identify a person. Because of the possibility of identifying someone, the data should only be used by persons that "need" to use it for legitimate security purposes; this is commonly referred to as "role-based access and permissions."

The above is a simplified example that illustrates the reason all websites should have a privacy policy that clearly states what data they collect, what it is used for, and how it is protected.

Laws & Standards

The following is a non-exhaustive list of laws and standards that may be applicable to different registries. The common thread between all of them is that they deal with either data security, data privacy, or both in some way.

Laws

Below are some laws that may or may not be applicable to your registry, depending on a variety of circumstances. An individual registry or their parent organization is ultimately responsible for ensuring that they are aware of and follow all applicable laws.

United States

- **Federal Information Security Modernization Act (FISMA) (P.L. 113-283, 44 USC 35), December 2014**
- **Privacy Act of 1974 as amended (P.L. 93-579, 5 USC 552a), December 1974**
- **Health Insurance Portability and Accountability Act of 1996 (HIPAA)**
- **Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009**

Canada

- **Privacy Act**
- **Statistics Act**

- **Personal Information Protection and Electronic Documents Act (PIPEDA)**

U.S. State Laws

Individual U.S. states have started to enact different privacy laws. If you are not familiar with the privacy laws applicable to your registry, consider contacting your in-house legal counsel or other regulatory staff to determine how the registry may be affected. Also, many U.S. states have their own central cancer registry statute where cancer data is commonly defined as confidential. These laws and any associated administrative rules will affect the security and privacy policies that the registry will be governed by.

Standards

The following are standards that are recognized to meet many of the requirements of the above-mentioned laws. Standards and security frameworks are often entangled, as many of the standards use references to underlying frameworks of security and privacy controls.

- **FedRAMP Baselines –** Standards to address FISMA compliance for cloud infrastructure, platforms, and applications. Utilizes the NIST 800-53 set of security controls.
- **FISMA Baselines –** A standard set of NIST 800-53 security controls defined to meet different levels of data protection for government systems.
- **ISO 27000 Series of publications –** International standards on how to implement an information security management program. This includes publications on security foundations (ISO 27001), control implementation (ISO 27002), and risk management (ISO 27005), among others.
- **StateRAMP –** A set of standards organized around the NIST 800-53 set of security controls to help states standardize security practices.

Additional Guidance for Registries

In addition to U.S. state and federal laws and standards, guidance is provided by the U.S. Health and Human Services (HHS) administration in the form of goals and best practices relevant to healthcare organizations. U.S. HHS guidance aligns well with any security and privacy framework listed in the document; however, it has a specific alignment with the NIST cybersecurity framework. Below are some resources and links that may be helpful.

- **HPH Cybersecurity Performance Goals.** Goals to help healthcare organizations prioritize implementation of high-impact cybersecurity practices.
- **Health Care and Public Health (HPH) Sector cybersecurity framework Implementation Guide.** An implementation guide for cybersecurity frameworks, specifically for the HPH sector.

Canadian registries have the following guidance from Statistics Canada. These resources provide guidance, goals and best practices for the registries that align well with cybersecurity frameworks.

- **Statistics Canada's Privacy Framework**
- **Generic Privacy Impact Assessment for Statistics Canada's Statistical Programs**

Common Cybersecurity Frameworks

A cybersecurity framework is, at its core, a list of requirements that must be addressed in some way to achieve a defined, security-related goal. The main goal of all cybersecurity programs is to reduce the risk of an incident occurring that threatens the organization to the level that the organization cannot function effectively.

In order to attain the goal of reducing cybersecurity risk, many organizations adopt a cybersecurity framework. They do this because it is much easier to follow a well-vetted framework than it is to create one's own framework. This section lists some of the common frameworks out there. They share many common attributes and have the same goal: reducing cybersecurity risk. However, some are more in-depth and prescriptive (like NIST), while others are more general (like SOC) and leave the details up to the organization.

NIST Cybersecurity Framework

The NIST cybersecurity framework (CSF) is a cybersecurity risk management framework designed for all organizations wanting to "mature" (or improve) the cybersecurity-focused risk management practices for their organization. This framework focuses on maturity levels and provides best practices to move from the lowest level of organizational maturity "Tier 1: Partial" to the highest "Tier 4: Adaptive." The key feature of this cybersecurity framework is that it overlays well with other security control sets like the NIST 800-53, ISO 27001, and Control Objectives for Information and Related Technologies (COBIT). It also provides direction on the best path forward for improving an organization's risk posture. With this framework, there is not a "pass or fail" approach but more of a growth mentality so that an organization can continually improve.

This is a good framework to adopt if an organization currently does not have any cybersecurity framework in place. It has five core functions: Identify, Protect, Detect, Respond, and Recovery. In each function, there are categories and subcategories of security-related controls that can be implemented within an organization based on risk and other factors. The organization can then measure its level of maturity in the different areas to determine where the organization's resources and its focus should be. The following provides a general overview of the five core functions, what they mean, and how they might impact an organization. These can all be read about in more detail in the NIST cybersecurity framework (CSF).

Identify

> Understand what you have and what risks each have. This includes hardware, software, external services, facilities, and people. Before data can be secured, all the different pieces that may impact that data's security must be identified, and the risks of each understood.

Protect

> Based on what has been identified, what steps will be implemented to protect the data from the identified risks.

Detect

How attacks, compromises, and other incidents will be detected within the organization.

Respond

Once an attack, compromise, or other incident is detected, what response will be enacted. This covers the analysis, mitigation, reporting and communication of the incident.

Recovery

How the organization will recover after the initial response to a detected incident has begun.

The last overarching principle in the CSF is **Govern**, which encompasses all of the organization's risk management strategies, policies, and procedures that have been established and communicated to everyone. It also includes the ability to monitor or audit how well the program is doing over time so improvements can be made where appropriate.

NIST Risk Management Framework

The NIST Risk Management Framework (RMF) is the risk management framework mandated for U.S. federal systems. This framework is typically only used by the U.S. Federal Government and its contractors that run systems on behalf of the U.S. Federal Government. It is a documentation-heavy framework with many approvals and requirements for federal systems, including the requirement to obtain an Authorization to Operate (ATO), which must be signed by a government official. It utilizes the NIST Special Publication (SP) 800-53 security control catalog and many other NIST-related Special Publication (SP) documents.

The utilization of the NIST SP 800-53 security control catalog with the RMF framework sometimes causes confusion, where the RMF and the control catalog are considered the same thing; however, although the NIST RMF must use the NIST SP 800-53 security controls, they are not the same. The NIST RMF has seven (7) activities: Prepare, Categorize, Select, Implement, Assess, Authorize, and Monitor.

Prepare

Carry out essential activities to help prepare the organization to begin managing its security and privacy risks.

Categorize

Identify risk to security and privacy and use them to determine the level of impact the loss of confidentiality, integrity or availability would have on the organization. This is usually a Low, Moderate or High rating as defined by the NIST FIPS-199 publication.

Select

Select, tailor, and document security and privacy controls from the NIST SP 800-53 control catalog necessary to protect the organization from the risks determined in the Categorize phase.

Implement

Implement the security controls selected in the Select phase of the framework.

Assess

Audit the security and privacy controls detailed in the implementation phase to determine if they are implemented correctly, operating as intended, and producing the desired protections.

Authorize

Have a senior official review the assessment, the documented risks, system need, and the implemented control documentation to determine if the system should remain in operation as it is currently implemented.

Monitor

Routinely review the system to maintain situational awareness about the security and privacy of the system.

Each phase of the RMF has a specific purpose in the life cycle of a system. During the Select and Implement phases, security controls from the NIST SP 800-53 control catalog are selected and then implemented based on the defined security and privacy needs of the system. To help organizations determine the appropriate controls to implement, NIST created guidance in the form of security control baselines. A security baseline is the minimum recommended set of security controls that should be implemented based on the system categorization in the areas of confidentiality, integrity, and availability. NIST has defined 3 default baselines, one for each system categorization of Low, Moderate or High. These control baselines are documented in the NIST publication SP 800-53B.

Once the baseline set of controls has been determined, additional controls can be added based on specific system need. The other RMF steps revolve around this set of security controls and whether or not they have been implemented appropriately in the Assess phase and continue to work as expected during the Monitor phase. Some additional information about the NIST SP 800-53 security control catalog is listed below.

NIST Special Publication (SP) 800-53

The NIST Special Publication (SP) 800-53 is a catalog of security and privacy controls that must be used in the NIST RMF, but can also be used to define security and privacy controls in other frameworks. The catalog contains detailed control definitions, requirements, and implementation guidance for sound security and privacy practices.

In the SP 800-53 document, controls are broken down into groups that are called control families. These control families deal with areas such as Access Control, Audit Logging, Contingency Planning, Configuration Management, Software Acquisition and Supply Chain, among others. By using control families, NIST grouped the controls together by general areas so that they will align with concepts that are common to all security frameworks and industry best practices. This allows these controls to be mapped onto other security frameworks if necessary.

Remember, NIST SP 800-53 does not provide a framework for putting best practices in place for IT risk management – that is the responsibility of the security framework, and the general processes defined there. The NIST SP 800-53 catalog only provides a comprehensive list of security and privacy controls that can be implemented to as part of the overall security framework.

NOTE: The security and privacy controls detailed in the NIST SP 800-53 catalog can also be easily mapped onto the other NIST framework (the NIST CSF) if that is that framework being used.

COBIT

COBIT is an enterprise IT governance framework. By this, we mean that COBIT is not solely focused on cybersecurity, but rather on overall IT governance, which is typically used by large businesses. COBIT will not be leveraged for most central cancer registries. While there are sections and practices outlined in COBIT that focus specifically on cybersecurity risk, the overall framework itself focuses on business/institutional risk as well as cybersecurity risk. Since this is an overarching framework for IT governance, it complements other frameworks on this list and may be used to create an overarching IT framework for an organization.

ISO 27001

The ISO 27001 security framework is an international standard for developing and implementing information security management systems. It is similar to the NIST SP 800-53 security controls in that ISO 27001 provides a comprehensive set of security controls that should be implemented by an organization to lower cybersecurity risk.

This framework also provides a standard certification of compliance for security control implementation. Since this control set was created by the International Organization for Standardization (ISO), it is recognized around the world.

SOC 2

SOC 2 was developed by the American Institute of Certified Public Accountants and Certified Investment Management Analysts (AICPA & CIMA) as a way to demonstrate that organizations are protecting customer data from unauthorized access, security incidents, and other vulnerabilities. It consists of five (5) areas called Trust Service Criteria (TSC): Security; Availability; Processing Integrity; Confidentiality; and Privacy. Each area is broken down into a set of criteria that must be addressed for the organization to be deemed compliant in that area. The organization must determine which TSC is appropriate for the application or organization that is being audited. Only the Security TSC is required for all systems. The other TSC are optional and should be reviewed for relevance before being implemented. This framework differs from the others, as it puts responsibility on the system owner to define the actual security controls used to meet the defined criteria.

As with the ISO 270001 framework, an industry standard certification can be obtained from an accredited auditor stating that the system meets some or all of the TSC.

Other Frameworks

There are other cybersecurity control frameworks and certifications out there. Here are a few more:

- **HITRUST CSF**
- **CIS**
- **PCI DSS**

Making Choices about Frameworks

While there are multiple frameworks available to choose from and each one is a little bit different, they generally share the same set of principles: they all are attempting to protect confidential data and the organization that uses the framework by reducing risk when data are collected, processed, stored, or disseminated. Each framework has its pros and cons, and some frameworks may be more appropriate for a particular organization than others. However, the above frameworks have been proven to be effective in producing positive results in the cybersecurity area; it is much better to follow a vetted cybersecurity framework than to work without a framework or attempt to "do it yourself." Whichever framework you choose (and sometimes you may choose multiple), it will be helpful in protecting the security and privacy of patient data.

Cybersecurity Auditing

Auditing is the comprehensive review and analysis of policies, procedures, practices, infrastructure, and personnel to determine if security practices currently implemented by an organization are adequate to protect the information system from known and unknown threats. This includes a thorough inspection of systems and practices for existing vulnerabilities to see if best practices are being followed and enforced.

There are many different types of audits that can be performed. Below is a list of a few types of audits, some of which may be familiar:

- **Process audits**
- **Compliance audits**
- **Financial audits**
- **HIPAA audits**
- **Control self-assessments**

Each type of audit has a specific purpose and goal. Some audits may be conducted to obtain industry standard certifications or to address industry-specific requirements. Some audits are used internally to improve processes and procedures. Audits can be done by internal and/or external parties, depending on the goals and requirements of the audit.

The following are some general internal audits, reviews, or assessments that should happen at most organizations dealing with securing data:

- **Policy and procedure reviews**
- **User account/permission audit**

- **Data inventory assessment**
- **IT System inventory audit**

Internal vs. External, the Key is Independence

Whether the audit is completed by an internal group within the organization or performed by an external auditing company depends on multiple factors. However, there is one key component that all auditors must have in common: they must be independent of the product or process being audited. This ensures objectivity and the absence of any bias that might otherwise be attributable to a conflict of interest or commitment. For an audit to have credibility, the auditors performing the audit function must be both independent and perceived to be independent of whatever is being audited. Specifically, this means having no direct involvement in the design, implementation, or management of the system or process being audited. For any audit report to have credibility, the auditors creating the report cannot have any appearance or question of impropriety. If an auditor is not independent or does not conduct the audit properly, the audit will not hold a lot of weight and will not be as useful as one done by a truly independent auditor.

Control Self-Assessment

A control self-assessment is just what it sounds like: an assessment of security controls done by internal parties associated with the system being assessed. This type of assessment, while not accepted for official certifications, can be useful to the organization if performed correctly and honestly. This type of assessment can benefit from the possibility that local knowledge, control, and use of systems and security controls implies the best knowledge of those systems and controls. Control self-assessments are typically used to improve operations and processes internally before an industry standard audit is performed on the process. This assessment can also be used to help improve internal processes that benefit the organization, either by making those processes more efficient or by providing feedback on areas that need additional resources or more oversight.

Industry Audits

Cancer registries will typically not have an industry standard audit performed on them. They should, however, ask that audits be performed by vendors on systems the registry uses to collect, store or process registry data. Prior to entering into a relationship with a vendor, a central cancer registry should request a standard audit report from that vendor for the system or service they want to utilize. This will typically be a SOC 2 Type 2 audit listed below. However, if the registry has contracts with the U.S. Federal government, a FISMA or FedRAMP audit may be required to comply with that contract.

Below is a list of common audits that may have been performed by a potential vendor. Of course, there are other types of audits that can also be performed in addition to the ones listed. These are the most common.

FISMA/FedRAMP Audit

FISMA and FedRAMP audits are paired together below because they are focused on the same security control set, NIST SP 800-53. The differences between the two are the expected set of

policies and the expected set of security controls implemented. A FISMA audit can be done by an independent party within the organization if the system owner and authorizing official agree to it. A FedRAMP audit must be performed by a certified Third-Party Assessment Organization (3PAO). This 3PAO must be approved by the FedRAMP Joint Authorization Board (JAB) before it can perform FedRAMP audits for the organization.

Note: FedRAMP audits are reserved for cloud services, either SAAS, PAAS, or IAAS.

SOC 2 Type 1 or Type 2 Audit

A SOC 2 Audit is an audit of the organization's security, availability, processing integrity, confidentiality, and privacy controls against the AICPA's Trust Services Criteria (TSC). A certified AICPA auditor MUST perform this audit. There are two types of SOC 2 audits:

1. **Type 1 audit**: a point-in-time audit that is carried out on a specific date. The auditor only checks that the TSC are fulfilled as of that date.
2. **Type 2 audit**: a time-based audit. It is up to the organization to determine the timeframe that they want to have the auditor review, typically 6 months to 1 year prior to the start of the audit. The auditor will review the selected TSC over that period to ensure that the organization has continually met its commitments.

After an audit has been completed, the auditor will issue an audit report. This audit report will contain the organization's statement about what is provided and how it is secured. The report will also include detailed auditor's findings in the different TSC areas and statements. The report will typically only state if the control was met without exceptions, or it will list the exception/finding if the auditor felt that the control was not addressed or there was a weakness discovered. This audit report is formatted such that it may be given to the organization's clients for review.

ISO 27001 audit

An ISO 27001 audit must be performed by an external third-party auditor that has received their ISO auditing certification. An ISO 27001 audit is completed similarly to other audits, where a set of policies, procedures, and a set of predefined security controls are assessed to determine if they are in place and how well they are performing. The first stage of the audit is a documentation review process for policies and procedures. Once that stage is completed, the security controls are reviewed to ensure that they are performing as described. Once the ISO 27001 audit/accrediting process is completed, an ISO 27001 certification is awarded to the organization.

Summary

While this document does not provide a how-to for implementing a cybersecurity framework or an industry standard audit program, it does provide the general information necessary for where to start. Creating and maintaining a cybersecurity program at a registry or parent organization takes a lot of effort and is never finished. There are always things to do or modify, like process, procedure, or security control implementations. Cybersecurity in general is an ever-changing process – the security posture of an organization must change over time to adapt to the current risks and threats. This is why having a vetted cybersecurity framework as the backbone of any cybersecurity program is beneficial for promoting the security of information handled by the registry.