CTSC
CENTER FOR TRUSTWORTHY SCIENTIFIC CYBERINFRASTRUCTURE

Guide to Developing Cybersecurity Programs for NSF Science and Engineering Projects

Version 1
August 2014

trustedci.org/guide
please direct comments and feedback to info@trustedci.org

About CTSC

The mission of the Center for Trustworthy Scientific Cyberinfrastructure (CTSC, trustedci.org) is to improve the cybersecurity of NSF science and engineering projects, while allowing those projects to focus on their science endeavors. This mission is accomplished through one-on-one engagements with projects to solve their specific problems, broad education, outreach and training to raise the practice-of-security across the community, and looking for opportunities for improvement to bring in research to raise the state-of-practice.

Contributors

Jim Marsteller, Craig Jackson, Susan Sons, Jared Allar, Terry Fleury, Patrick Duda

Acknowledgments

We acknowledge and thank the following collaborators and colleagues. Very special thanks goes to Bret Goodrich of DKIST for inspiring this effort, for his direct and incredibly valuable advice, and for his encouragement. Special thanks to Mark Krenz and Von Welch for their assistance. Many thanks to the following additional resources: Jim Basney, Steve Berukoff, Bob Cowles, Ardoth Hassler, Drew Simshaw, Abe Singer, Adam Slagell, and Betsy Thomas.

This document is a product of the Center for Trustworthy Scientific Cyberinfrastructure (CTSC). CTSC is supported by the National Science Foundation under Grant Number OCI-1234408. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

Disclaimer

This document and its contents are not meant to supersede or be a substitute for any obligatory requirement or framework (legally binding or otherwise). Nor does this document contain legal advice. We strongly urge readers, including science projects within the target audience, to ensure they are aware of all requirements, and communicate readily with stakeholders around information security.

Using & Citing this Work

Guide to Developing Cybersecurity Programs for NSF Science and Engineering Projects, v1, Center for Trustworthy Scientific Cyberinfrastructure, August 2014.

This work is available on the web at the following URL: http://trustedci.org/guide

---

[1] http://creativecommons.org/licenses/by/3.0/deed.en_US

Table of Contents

Introduction

Overview & Purpose

Through funding from the National Science Foundation, the Center for Trustworthy Scientific Cyberinfrastructure (CTSC) is committed to improve the cybersecurity of NSF science and engineering projects, while allowing those projects to focus on their science endeavors.

The purpose of this document is to offer a streamlined approach to developing a cybersecurity program for NSF funded projects including Large Facility (LFs), Major Research Equipment and Facilities Construction (MREFCs), and Cyberinfrastructure (CI) projects. This guide was developed for projects of considerable size but smaller projects will also benefit from following the concepts contained within this document. For smaller projects or those with fewer resources, some concessions will need to be made but the overall cybersecurity planning guidance can be applied to projects big and small. This guide has been developed to address the cybersecurity requirements outlined in the NSF Cooperative Agreements: CA-FATC LF Article 56 or CA-FATC FFRDC Article 59[2], as well as the increasing trend for information security planning at the grant proposal stage. We will review these requirements in more detail in the "Building a Cybersecurity Plan" section of this guide.

The development of this guide was influenced by a variety of commonly available publications related to risk mitigation and cybersecurity planning including the following.

- NIST Special Publications 800 Series[3]
- NIST Federal Information Processing Standards (FIPS) Publications[4]
- NIST's Framework for Improving Critical Infrastructure Cybersecurity[5]
- NRECA / Cooperative Research Network Smart Grid Demonstration Project "Guide to Developing a Cyber Security and Risk Mitigation Plan"[6]

This document is tailored for an NSF-funded project serving the scientific community and includes guidance on cybersecurity challenges faced by those projects (regarding, *e.g.*, scientific data, instruments, the distributed nature of science communities). Aspects related to that tailoring are based on the experience of the authors working in cybersecurity for a number of NSF and other federally funded science projects.

Using This Guide

Section 1 of this document is intended to provide a step-by-step process for developing a risk-based operational cybersecurity program to a reader who has a moderate to advanced understanding of information technology, but who may be relatively new to information security. Thus, this reader

---

[2] http://www.nsf.gov/pubs/policydocs/cafatc/cafatc_lf212.pdf
[3] http://csrc.nist.gov/publications/PubsSPs.html
[4] http://csrc.nist.gov/publications/PubsFIPS.html
[5] http://www.nist.gov/cyberframework/
[6] https://groups.cooperative.com/smartgriddemo/public/CyberSecurity/Documents/CyberSecurityGuideforanElectricCooperativeV11-2.pdf

may be a project's principal investigator and/or an IT specialist working for the project. For areas that are outside the readers' knowledge, consultation with other members of the project and other sources of cybersecurity-relevant expertise (e.g., campus information security office) should be considered. Regardless, selecting key members of the project and including them in the planning process is recommended. The effort needed to complete each section of the guide will vary on the complexity of the project environment and resources available for the planning process.

Section 2 provides introductory information, recommendations, and resources on a variety of special topics in information security. Many covered topics are relevant to any operational cybersecurity program (e.g., access controls), but the content is written and selected with NSF projects in mind and highlights a number of areas of particular relevance or interest.

Throughout the guide, you will find a number of green Getting Started boxes, highlighting templated policies and tools. These templates are provided to help clarify concepts and assist projects in kickstarting their programs. At the same time, we strongly encourage projects to take ownership of the content, and make sure resulting policies meet their needs.

> Getting Started:
>
> These blocks highlight templates for the policies and other documents discussed in this guide. Copying and editing these templates to customize for your project's individual needs is an easy way to get started with needed documentation, or formalize what you may already have documented.

Blue boxes serve to provide brief "Spotlights on Science," highlighting content of special relevance to the science community.

> Spotlight on Science:
>
> Spotlight on Science blocks expand on the topic at hand with tips or other guidance relevant to the needs of science projects.

Cybersecurity planning and program implementation is not a *one-size-fits-all* endeavor. We hope that both the templates and the notes on doing cybersecurity in the science world will aid in addressing your project's specific needs. We strongly encourage the inclusion of all stakeholders and risk owners in any planning process.

1 The Process: Establishing and Maintaining a Program

1.1 Establishing a Cybersecurity Program

1.1.1 What is a "Cybersecurity Program?"

A cybersecurity program is a structured approach to develop, implement, and maintain an organizational environment conducive to appropriate information security and levels of information-related risk. Cybersecurity programs generally include ongoing activities to address relevant policies and procedures, technologies, mitigations, and training and awareness activities. A cybersecurity program is scoped to the key information assets, resources, and lifespan of organizations.

There exists no single authoritative approach or framework to developing and implementing a cybersecurity program, and we suggest projects consider a broad set of core tools (best practices, risk assessment, and program frameworks/maturity models), to inform a range of programmatic processes from establishing a program to evaluating and refining a program.

Cybersecurity Program Processes and Core Tools

These tools and processes are aimed at protecting information assets. *Information assets* (or just "assets"), as we refer to them in this guide, are valuable and/or sensitive organizational information and information systems. A cybersecurity program seeks to protect these assets from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide for the information security objectives of *confidentiality*, *integrity*, and *availability* (i.e., the "CIA" triad).[7] "A

---

[7] *See*, 44 U.S.C. 3542(b), Available:

loss of information security" is synonymous with the "unauthorized access, use, disclosure, disruption, modification, or destruction of information assets."

Of course, there are a variety of ways to characterize the elements or components of a comprehensive cybersecurity program. Science projects may have security requirements handed down directly from a funding organization or other stakeholders of the system, or may fall under legal or regulatory regimes that dictate all or some of these components. NSF has the following highlighted security requirements for Large Facilities and FFRDCs, and has increasingly been including information security planning requirements at the grant writing stage.

> CA-FATC LF Article 56 and CA-FATC FFRDC Article 59[8]
>
> Security for all information technology (IT) systems employed in the performance of this award, including equipment and information, is the awardee's responsibility. Within a time mutually agreed upon by the awardee and the cognizant NSF Program Officer, the awardee shall provide a written Summary of the policies, procedures, and practices employed by the awardee's organization as part of the organization's IT security program, in place or planned, to protect research and education activities in support of the award.
>
> The Summary shall describe the information security program appropriate for the project including, but not limited to: roles and responsibilities, risk assessment, technical safeguards, administrative safeguards, physical safeguards, policies and procedures, awareness and training, and notification procedures in the event of a cyber-security breach. The Summary shall include the institution's evaluation criteria that will measure the successful implementation of the IT Security Program. In addition, the Summary shall address appropriate security measures required of all subawardees, subcontractors, researchers and others who will have access to the systems employed in support of this award.
>
> The Summary will be the basis of a dialogue which NSF will have with the awardee, directly or through community meetings. Discussions will address a number of topics, such as, but not limited to, evolving security concerns and concomitant cyber-security policy and procedures within the government and at awardees' institutions, available education and training activities in cyber-security, and coordination activities among NSF awardees.

1.1.2 Utilizing a Risk-Based Approach to Information Security

Risk management refers to a coordinated set of activities and methods that are used to direct an organization and to understand and respond to adverse events that can affect its ability to achieve its objectives.[9] As such, a risk management approach provides a disciplined and structured process that integrates information security and broader risk management activities.[10]

Cybersecurity planning and programs are often components of broader risk management activities

---

http://www.gpo.gov/fdsys/pkg/USCODE-2011-title44/pdf/USCODE-2011-title44-chap35-subchapIII-sec3542.pdf

[8] http://www.nsf.gov/pubs/policydocs/cafatc/cafatc_lf212.pdf

[9] http://www.praxiom.com/iso-31000-terms.htm

[10] http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf

within an organization, or may in fact introduce an organization to formal risk management practices. Risk management provides a means for prioritizing and sharing information about the security risks to an information technology (IT) infrastructure. Projects may choose to handle information security risks in different ways, including mitigating the risk, transferring the risk, avoiding the risk, or accepting the risk.[11] In the information security space, organizations almost always must accept some *de facto* residual risk -- the risk that remains after mitigations are implemented.

In addition to being required of some NSF projects (per the above-cited terms), risk-based approaches are particularly appropriate for information security and the science field for a variety of reasons:

- Pure compliance regimes (i.e., sets of highly specified rules) are inappropriate in the information security domain, particularly at this time, and particularly for operational cybersecurity programs which much address an expansive range of information-related risks. The state of the art and science around information security is changing rapidly, as are the threats. Programs are best tailored to the projects' information assets and constraints. Risk-based approaches allow organizations to forge ahead flexibly.
- Risk-based approaches may be particularly well-suited for organizations with limited resources and time. Compliance regimes (even ones that include risk-based processes, e.g., HIPAA) can be particularly burdensome when applied to organizations with limited resources. Risk-based approaches universally embrace the idea that tough decisions have to be made, and that risk management cannot and does not mean that all risk is avoided or stamped out.
- Science projects may have limited ability to transfer risk via insurance. Insurance plays a huge role in addressing risk at scale in our society. However, the 'cyber insurance' industry is only beginning to take off, and -- even if it were readily negotiable for science projects via parent institutions and the like -- insurance cannot remedy many of the most serious cyber-based losses to science projects. No amount of money can bring back one-of-a-kind scientific data, lost opportunities for discovery, or reputation within the science community.

However, risk-based approaches are not without their challenges. They do require time, effort, familiarity with a set of concepts and tools, organizational buy-in, and the involvement of project leadership. One of the purposes of this guide is to provide a useable 'crash course' in a relatively agile risk-based approach to information security.

1.1.3 The Role of Project Leadership

Governance and project leadership's role in a cybersecurity program is crucial. As information and information systems become increasingly critical to our economies, research, social lives, and national security -- and the number and diversity of information security threats grows -- it has become increasingly clear that organizational leadership must be involved in understanding and managing information security risks, and fine-tuning resource allocation.

The individual tasked with the cybersecurity program's oversight must have clear authority to develop and implement the needed security policies and practices. We recommend explicitly naming an Information Security Officer (ISO), whether that individual is already in a leadership role

---

[11] http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf, at p.5

in the project (e.g., a Principal Investigator), a key IT manager, or a team member with cybersecurity expertise. *See*, Section 1.1.6 below and the Master Information Security Policies and Procedures template, Section 2 “Roles and Responsibilities.”

1.1.4 Project Constraints and Lifespan

All organizations face constraints on the time, money, and expertise they can bring to bear on information security. NSF projects, even very large, long-lived ones, may face particularly stark constraints when considering the feasible scope and depth of a cybersecurity program. Unlike a long lived governmental entity or well-established commercial enterprise, projects usually have relatively short lifespans and/or limited ability to predict the future of funding availability beyond a particular funding period. Moreover, projects may or may not have the funding to attract and hire experienced, dedicated security personnel. Because cybersecurity programs do not simply spring into existence, requiring both time and effort evolve and mature, these constraints require project leadership to make strategic, pragmatic decisions about where to concentrate.

1.1.5 Making Use of External Resources and Partners

Sound leadership also means making use of available resources. NSF projects, not unlike other organizations, must make a number of decisions about what aspects of the program can be designed and implemented in-house, and when to reach out for assistance or outsource. Some activities may be obvious ‘DIY’ fodder (cataloging assets, training personnel on the project’s own policies), and others scream out for help (documenting legal requirements in case of a breach of personal data).

When developing a cybersecurity program there are more sources of assistance available than one might realize. The first place a project can look is at their own institution’s departmental resources. The department might have IT staff available to help with developing or maintaining a security program. This same staff might have experience with administration and management of systems. Your project might be able to leverage existing policies and procedures (e.g., incident response, change management). See what the department has available and make use of it.

Beyond the department is the institution's campus IT or information security office. Most campuses have some type of cybersecurity program in place and you should be able to leverage it. This resource may be able to help with the following.

- Assistance with risk assessments
- Security training
- Security services (e.g., monitoring, firewalling)
- Forensic services
- Knowledge of relevant laws and regulations (e.g., FERPA, HIPAA, state data breach and data retention statutes)

Outside of campus resources available to a project, there is the NSF CI community at large.

Leverage the NSF Community
- Experiences and practices of other CI projects
- See, http://trustedci.org/useful-links/
- Ask other CI projects directly and build relationships

CTSC (Center for Trustworthy Scientific Cyberinfrastructure)[12]

- Engagements and advice
- More about this in the next Unit

Bro Center of Expertise[13]

- Network security and monitoring

1.1.6 Information Security Policies and Procedures

Developing, implementing, and maintaining a cybersecurity program inevitably involves planning and documentation, most commonly in the form of policies and procedures. In fact, many of the "controls" we discuss in later sections are embodied and communicated directly through the written word. As a formative policy step, we recommend developing a "Master Information Security Policy & Procedures" (MISPP) document that provides (a) a brief, broad overview of the project and the importance of information security to the project, (b) a summary of roles and responsibilities, including naming the Information Security Officer, (c) an organized list and description of other, special purpose organizational information security policy documents (*e.g.*, Data Classification Policy; Incident Response Procedures), and (d) the core procedures for developing, implementing, and maintaining the program. This master document forms the core of the program. A template MISPP is included as an appendix to this guide. Throughout this guide, we will refer back to the MISPP and other special purpose policy and procedure documents you may need to develop.

Getting Started:

If your project or organization doesn't yet have a high-level / master information security policy written, consider starting with the **Master Information Security Policy & Procedures Template**. You can easily copy the Google Doc and edit it to create a policy that fits your specific situation, or just borrow the individual sections needed to flesh out a policy already begun.

1.2 Identifying Information Assets

Information assets sit at the heart of CTSC's risk-based approach to information security. Identifying, understanding, and documenting those assets is a natural early step and critical in linking together the tools and processes that make a program work.

---

[12] http://trustedci.org/

[13] http://www.bro.org/nsf/

1.2.1 Defining "Information Assets"

We define information assets as valuable and/or sensitive organizational information and information systems.

> *Information* is any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.[14]
>
> An *information system* is a discrete set of information and related resources (such as people, equipment, and information technology) organized for the collection, processing, maintenance, use, sharing, dissemination, and/or disposition of information.[15]

While these definitions are very broad, they provide a useful, simple lens for viewing the scope of assets requiring protection.

Assets have a basic level of organizational *value* and/or *sensitivity.* These qualities of value and sensitivity are key factors to consider in analyzing the anticipated impact of security incidents. Of course, value may be related to the monetary value of an asset; but it can mean much more. A science project's most valuable assets may well be those most critical to the project's science mission, regardless of fungibility. "Sensitive" describes information and information systems for which unauthorized access, use, disclosure, disruption, modification, or destruction could negatively impact organizational operations, organizational assets, individuals, other organizations or stakeholders. Many organizational assets are both valuable and sensitive; these terms are not mutually exclusive. Used together, these terms capture the scope of an organization's basis for utilizing resources to protect information assets.

Example Information Assets

	Valuable	***Sensitive***
Information	Research data	Regulated personal information
Information Systems	Telescope	SCADA

We distinguish assets from the broader organizational interests (*e.g.,* science mission, legal property interests, continuity of operations, reputation/goodwill, safety and well-being of individuals, other organizations and stakeholders) that security efforts assist in protecting. While these broader interests form the foundation for why we protect information assets, focusing on the assets themselves allows the cybersecurity program to clarify its scope, producing useful units of analysis for risk assessment and control selection.

---

[14] See, *National Information Assurance (IA) Glossary,* CNSS Instruction No. 4009, Apr. 2010.

[15] *See*, 44 U.S.C. 3502

1.2.2 Documenting the Asset Environment

A complete and accurate information asset inventory is one of the most powerful tools available to the information security officer. Every other step in the process of creating a healthy cybersecurity program begins with knowing what information and information systems are to be secured. Assets that haven't been assigned to someone to maintain are prone to neglect. Personnel turnover can dramatically reduce the effectiveness of a cybersecurity program if there is no way to bring new personnel up to speed on what the environment looks like.

> **Getting Started:**
>
> The Information Asset Inventory Template provides a lightweight framework for efficiently identifying and characterizing both information and information systems.

The included template is packed with tips; here we offer a couple of general recommendations.

First, we find it generally advisable to start the inventory process with information, as opposed to information systems. The mobility, and easy reproducibility, of information (particularly digital information) means that data flows can reveal the full expanse of a distributed information ecosystem. Tracking the information, and constructing data flows or maps, will help reveal many of the relevant systems, and potential points of compromise.

Second, to make inventories usable, we often must define assets at various levels of abstraction. Probably all projects have IT infrastructure as an asset, and one can often select well established best practice controls for IT infrastructure. Similarly, it may be practically necessary to characterize types or classes of information (e.g., "sensitive email communications" or "personal information on research data participants") and information systems (e.g., "MacX GPSr-based 1pps timers " or "personnel personal mobile devices") rather than more discrete units. At the same time, many NSF projects will have some very specific and even unique assets warranting closer analysis (e.g., a special instrument array; a specific data set). Our template attempts to strike a balance.

1.2.3 Security Objectives for Information Assets

A natural step during asset documentation is to go one step further to consider the security objectives for these assets. The "CIA" triad is a commonly recognized set of concepts from NIST/FISMA.[16] By determining and documenting the needs for *confidentiality*, *integrity*, and/or *availability* for an asset or set of assets, projects can jumpstart the process of prioritizing effort and communicating about the types of projections needed.

---

[16] *See*, FIPS Publication 199 and 44 U.S.C. 3542(b), Available: http://www.gpo.gov/fdsys/pkg/USCODE-2011-title44/pdf/USCODE-2011-title44-chap35-subchapIII-sec3542.pdf

Spotlight on Science: *Integrity and Availability*

In many settings, *confidentiality* is king, however *integrity* and *availability* often take center stage in science. The integrity of research data and the availability of scientific instruments can be critical to the science mission.

Confidentiality	Preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.
Integrity	Guarding against improper information modification or destruction, including ensuring information authenticity. A loss of integrity includes the unauthorized modification or destruction of information, and the unauthorized control of an information system.
Availability	Ensuring timely and reliable access to and use of assets. A loss of availability is the disruption of access to or use of an asset.

1.2.4 Utilizing Your Documentation

An information asset inventory becomes a primary source for the process of selecting baseline controls (discussed in Section 1.3), as well as in conducting asset-based risk assessments (discussed in Section 1.4), as well as feeding into policy development (e.g., access control policies, see 2.1.1; information classification policies, see 2.2.6). In addition to being an indispensable part of cybersecurity program planning, the information asset inventory can aid in measuring and improving the program. Tracking the number and complexity of information assets being secured allows one to predict what resources will be needed for information security going forward. Finding a way to improve security around one type of asset or interaction provides knowledge that can be applied to others if one has clear documentation of what those assets are and how they interact.

1.3 Selecting & Implementing Baseline Controls

Controls or *mitigations* are the management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and/or availability of information assets. We use “controls” and “mitigations” more-or-less interchangeably.

In this section, we emphasize the selection of *baseline* controls, because control development and selection (and, certainly, implementation) are ongoing and recurring processes in a risk-based cybersecurity program. However, the control selection process must begin somewhere, and a science project might take any one or a combination of several approaches for control selection. Consider the following options:

1. Utilize a cybersecurity maturity model (*see*, Section 1.5 below) or the NIST Framework for Improving Critical Infrastructure Cybersecurity[17] to identify best practices and common controls relevant to your program and information assets. While these frameworks can be very useful evaluation tools, they also provide substantial guidance regarding widely accepted controls, and can assist a great deal in planning a comprehensive program.
2. Go to NIST SP 800-53 rev 4.[18] NIST tackles security control baselines head-on and with a great deal of sophistication (Section 3.1), and provides an extensive catalog of controls (Appendix F).
3. Dive directly into best practices documents designed to get you up to speed on common and critical security controls. CTSC's Securing Commodity IT in Scientific CI Projects[19] is one such document. SANS has produced a publicly-available resource, Critical Security Controls.[20] Review the DISA STIGs for specific technical control implementation on most operating systems and software.[21]
4. Use the results of a quick or targeted risk assessment to identify the most dire threats to your most critical assets.
5. Use the results of a comprehensive risk assessment to tailor control selection to your particular project needs.

The pragmatic choice depends on the stage and lifespan of your project, as well as available resources. A newly funded project may or may not have sufficient ability to characterize its information security environment in order to rely heavily on risk assessments or even select specific technical controls. At the same time, the project may have the outlook and time to lay out a comprehensive vision of its cybersecurity program from a more top-down perspective. An existing project, near or in an operational state, may need to kickstart its program quickly, identifying critical risks and relevant best practices prior to using resources to flesh out and tailor the program.

Whether or not your baseline controls are informed directly by a risk assessment, we strongly recommend the identification and utilization of established best practices whenever and wherever they can be found. While information security is a quickly evolving field, and scientific CI projects may well face unique or challenging risk management decisions, there is also a great deal of solid best practice available, particularly around commodity IT and general best practices as we discuss throughout this guide. Section 2 of this guide is focused on providing concise discussions, resources, and template policies for best practices around a number of information security domains.

Like many of the processes discussed in this guide, control selection may benefit from eliciting help from security experts, peers, and available resources. Often, campus IT resources will be available to discuss this topic. CTSC is also available to aid with control decisions.

---

[17] http://www.nist.gov/cyberframework/
[18] http://csrc.nist.gov/publications/PubsSPs.html
[19] http://trustedci.org/guide/docs/commodityIT
[20] http://www.sans.org/critical-security-controls
[21] http://iase.disa.mil/stigs/a-z.html

1.4 The Role of Risk Assessment

1.4.1 A Flexible Input into Risk Management Processes

Risk assessments comprise a key component of most, if not all, risk-based approaches to information security. In most cases, risk assessments are used to identify, estimate, and organize threats to an entity. Their purpose is to inform decision makers and support broader risk management processes, particularly in weighing the relative estimated levels of risk associated with various potential adverse events. They serve as a means not only to identify the most likely and impactful cybersecurity threats, but to assist in the process of allocating scarce resources to mitigate those risks.

There is no single “right way” to conduct a risk assessment. Risk assessments can vary both in assessment approach (e.g., qualitative, semi-quantitative) and orientation or starting point (e.g., asset/impact-oriented analysis, vulnerability-oriented analysis). NIST Special Publication 800-30 rev 1 [22] provides a comprehensive overview of an approach to risk assessment, as well as a great deal of context on the variety of choices that need to be made regarding how to approach the process. Importantly, risk assessment can be scoped broadly (e.g., to assess all the information security-related risk to a project) or more narrowly (e.g., to analyze the risk to a mission critical asset). Moreover, a project’s approach to risk assessment may necessarily vary depending on where the project is in its lifespan. For instance, a newly funded multi-year project may not be well-positioned to conduct an extensive risk assessment, and may instead turn its attention to establishing information security best practices, implementing well-established controls, and fleshing out policy as the project ramps up. A well-established project may need to focus efforts on identifying its most valuable and sensitive assets and its most critical threats in order to rapidly improve its program. A more mature project and cybersecurity program may utilize a detailed risk assessment to assess the effectiveness of existing controls, and fine tune the program.

Risk assessment has some fairly intuitive conceptual underpinnings, but the process can be time consuming and truly challenging. The benefits of structured, careful risk assessments include the following:

- A risk assessment can assist a project in identifying gaps in a security program.
- The resulting documentation becomes a useful communication and discussion tool that can be validated, updated, and reused.
- More comprehensive approaches can help fine-tune programs, and provide a basis for evaluating control effectiveness.

The risk assessment approach we describe in the following subsections is designed to introduce core concepts and processes that can be utilized at varying levels of scope and sophistication depending on a project’s needs. In CTSC, we generally recommend an asset-based approach to risk assessment, where analysis of threats and mitigations flow from articulation of the project’s information assets (i.e., information and information systems).

---

[22] http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf

It is in the context of a risk assessment where nearly every risk-based approach uses some variation of the following equation to calculate and compare adverse risk events:

Impact x Likelihood = Risk

If we can scope and characterize a threat event, estimate the likelihood of that event occurring, and the potential negative impact if it does, we have some useful gauge of the magnitude of the risk. Unfortunately, the usable simplicity of these concepts stops there if you intend to take a systematic approach to assessing information security risks. To assist with the process, we've developed a Risk Assessment Table[23] for readers to copy and utilize, as well as modify to their needs. This table supports a semi-quantitative approach to risk assessment.

Getting Started:

View our **Risk Assessment Table**, including the sample entries and the comparative residual and inherent risk levels. We'll return to this tool throughout the next few subsections.

In the next several subsections, we introduce processes, concepts, and tips for conducting risk assessments. However, a few tips are overarching:

- Be careful and consistent in how you operationalize and apply each concept and scale.
- Be efficient where possible. Risk assessments are meant to produce actionable input into decision processes.
- Understand that this is an estimation process regarding possible future events. Even if your risk assessment is based on rock solid historical data, this is still a predictive process with uncertainty.
- Don't be afraid to solicit help and advice.

1.4.2 Characterizing Risks: Threats, Vulnerabilities, and Attack Surfaces

In Section 1.3, we highlighted the importance of knowing and documenting your information assets. That foundation feeds directly into the risk assessment process. As you've seen in the Risk Assessment Table, information assets represent the highest level organizer of the risk assessment process. We suggest an asset-based approach to risk assessment, particularly for new, distributed, or rapidly changing projects where a comprehensive understanding of the full range of assets may be distributed across a number of people, and through multiple documents.

Having identified your information assets, the next step in the risk assessment process is to characterize the risk to those assets. We generally characterize these risks in terms of "threats," defining that term quite broadly:

> A "threat" is any circumstance or event with the potential to adversely impact

---

[23] The Risk Assessment Table was based in part on Logic Manager's enterprise risk management-focused risk assessment table, CTSC's specific asset-based approach to risk assessment, as well as core concepts from the NIST Special Publication series.

> organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations and/or stakeholders through an information system via a loss of information security.

As such, threats include potential circumstances or events resulting from accidental, negligent, reckless, and malicious actions, as well as natural events -- *i.e.*, both “adversarial” and “non-adversarial threats.” Threats often can be described in terms of a threat source (*e.g.*, an actor) and the action taken against (and/or utilizing) an information asset. For example, *an employee inappropriately shares sensitive communications*. This approach is similar to taking a “root cause” approach to characterizing risks, a best practice designed to assist risk managers in conceptually separating key causal events from their ill effects.

One of the great challenges of characterizing threats to an asset is capturing the full number and scope of threats. Consider resources such as the catalogue of threat events in NIST SP 800-30 (Appendix E), reaching out to experienced information security personnel, and participating in information sharing groups to build your institutional knowledge of information security threats. Another challenge is scoping your descriptions of threats. Our best advice is that this simply takes some practice, and -- ultimately -- consistency in an approach.

CTSC defines a “vulnerability” as a weakness in an information system that warrants mitigation.” Again, this is a quite broad definition. Some cybersecurity risk assessment approaches suggest that a threat always maps to a vulnerability. Our approach is less constrained, and accounts for attack surfaces that may not be fairly described as “weaknesses” or “gaps.” *Attack surfaces* are the portions or components of an information system through which the unauthorized access, use, disclosure, disruption, modification, or destruction of information assets may take place. A single asset (*e.g.*, raw research data collected by a specialized instrument) may be susceptible to attack via multiple surfaces.

1.4.3 Estimating Impact

Impact refers to the estimated potential magnitude of harm to organizational interests (*e.g.,* science mission, property, operations, reputation/goodwill, safety and well-being of individuals, other organizations and stakeholders) due to an unmitigated loss of information security.

In using the Risk Assessment Table, provide impact estimations for each we suggest operationalizing impact along a 5 point scale, but similar systems use a range of three point to 10 point scales. Regardless of the scale you use, it is critical that the each value be well defined and well understood by those applying the ratings. Consistent application is key.

In estimating impact, the following factors should be considered where applicable:

- Asset value
- Asset sensitivity
- Nature of the interest and type of resultant harm flowing from a loss of confidentiality, integrity, and/or availability (*e.g.*, loss of human life, damage to reputation, inconvenience to end users)
- Scope of resultant harm across time (including length of time), and number and type of stakeholders

- The transaction or response costs associated with handling the incident
- The knowledge, confidence and expertise of the those performing the estimation

1.4.4 Estimating Likelihood

Likelihood is an estimation of the probability of the occurrence of a security incident, where a security incident is defined as a threat that has manifested itself in such a way as to warrant a response due to an imminent or actual loss of information security. Therefore, incidents and likelihood estimates encompass a range of events, from successful, harmful attacks to attempts or near-misses where response is warranted.

Once again, estimating the likelihood of particular information security incidents is a multifactor affair. While historical evidence, experience, and threat intelligence can help, estimating likelihood can be a very subjective and challenging activity. Much more than impact, this takes insight into what's happening "in the wild."

In estimating likelihood, the following factors should be considered where applicable:

- Anticipated frequency of the adverse event occurring
- Motivation, knowledge, and capabilities of potential threat sources
- Specifics of any relevant vulnerabilities
- The knowledge, confidence, and expertise of the those performing the estimation

The first factor, frequency, can be particularly helpful in operationalizing likelihood. In the Risk Assessment Table, we suggest using a 5 point scale. However, it is advisable to calibrate your scale to specific frequency ranges. For example, you may wish to define "Very Infrequent" as one-incident-per-year. Again, consistency is key. Operationalize the scale clearly and in terms that make sense for your project.

Spotlight on Science: *No Uninteresting Targets*

Science projects may feel that they "aren't interesting enough targets" for computer criminals. Unfortunately, merely having a mobile computing device and/or an internet connection is enough to make anyone a target. Many attackers are simply thrill- or reputation-seeking or looking to steal resources so there doesn't have to be a monetary incentive at play. Many compromises don't involve a human actively targeting systems to begin with. There are many automation tools that may be dispatched to attack system after system and simply "call home" when something has been penetrated.

1.4.5 Estimating Control Effectiveness and Residual Risk

Using the Risk Assessment Table, your ratings of impact and likelihood produce an estimate of *inherent risk level* -- that is, the level of risk associated with an unmitigated security incident coming to pass. If current controls are in place to prevent, detect, contain, respond to, and/or otherwise recover from the incident, this is your opportunity to account for the effectiveness of these controls.

Again, we use a 5 point scale, with "1" denoting ineffective or non-existent controls and "5" denoting extremely effective controls. The rating is used to reduce the inherent risk (impact x likelihood) according to the following formula:

$$r = n \times \frac{(6 - c)}{5}$$

In this equation, n = inherent risk (i.e., impact × likelihood), and c = control effectiveness. The resultant number, r, is an estimation of *residual risk* -- i.e., the level of risk associated with a threat taking into account the effectiveness of existing controls.

While there exist other reasonable formulas to estimate residual risk, we chose this one with the following goals in mind:

- Keep the Impact (i), Likelihood (l), and Control Effectiveness (c) on the same simple 5-point scale.
- Keep the Inherent Risk (n) and Residual Risk (r) on the same simple 25-point[24] scale.
- Ensure that Residual Risk (r) scales reasonably relative to Control Effectiveness (c), rather than dropping off sharply in response to relatively ineffective or incomplete controls.

Records of incidents, active testing, as well as a strong understanding of mitigation costs are warranted to assess the effectiveness of each control in mitigating a particular risk.

1.4.6 Utilizing the Results of Risk Assessments

As discussed earlier, risk assessment -- and particularly the semi-quantitative assessments indicated in the Risk Assessment Table -- serve, first and foremost, as an input into decision making processes. Specifically, they assist in matching available effort and resources to feasible threats in order to achieve acceptable levels of risk. Residual risk levels may be informative in their own right, but they are particularly meaningful in comparison with one another. Moreover, regardless of the levels of residual risk, the next step is critical and not predetermined by any math: Is further mitigation warranted? The goal is to achieve acceptable levels of risk and that necessarily means selectively accepting residual risk, and prioritizing effort and resources. Regardless of who conducted the risk assessment up through the calculation of residual risk levels, the results warrant the attention of the project's ISO and/or leadership, both to understand the results and determine next steps.

---

[24] They aren't exactly the same. On the Risk Assessment Table template, Inherent Risk is a 1-25 scale and Residual Risk a 0-25 scale. This simply a result of rounding to whole numbers in Google Docs.

1.5 Evaluating the Program

Evaluating a cybersecurity program means more than conducting risk assessments or evaluating the effectiveness of existing controls. Additionally, in most projects, the network will continually be expanded and updated, its components changed, and its software applications replaced or updated with newer versions. Also, personnel changes will occur and security policies are likely to evolve over time. These changes mean that new risks will surface and risks previously mitigated may again become a concern. Thus, the risk management process is ongoing, and the same basic steps above can be applied.

Spotlight on Science: *Getting Help with Evaluation*

Part of CTSC's mission is to help NSF projects evaluate and improve their cybersecurity programs. We can also help you investigate and answer questions about specific security areas where your project needs help filling gaps.

1.5.1 Program Maturity and Metrics

The information security community and policy makers are taking an increasing interest in approaches and methods for evaluating cybersecurity programs. This interest goes beyond compliance regimes, extending to the exploration of different metrics (e.g., outcome versus process metrics) and the proliferation of cybersecurity maturity models.

Just as recent years have seen a massive increase in the number, scale, and visibility of cybersecurity incidents and increasing awareness and understanding of the need for systematic defense, there is also a growing appreciation that (a) cybersecurity is not a one-size-fits-all affair and (b) few if any organizations, even those with robust programs, can expect to operate free of security incidents. As such, the current trend is toward process metrics and evaluation models aligned with risk-management practices.

Cybersecurity maturity models are commonly characterized by organized approaches to evaluating cybersecurity programs across security domains and practices, and maturity that describe increasing sophistication of cybersecurity practices (e.g., *Ad Hoc*, *Defined*, *Managed*, *Optimized*, *Adaptive*[25]). Applying maturity models or the "Implementation Tiers" of NIST's Framework for Improving Critical Infrastructure Cybersecurity not only gives an organization insight into the current state of its program, but can assist in identifying a target state and roadmap.

More generally, benefits of implementing evaluation processes include increased accountability, increased program effectiveness, and input into resource allocation.

---

[25] http://www.boozallen.com/media/file/Cyber-Operations-Maturity-Framework-viewpoint.pdf See Appendix B on p.16.

We recommend a few general “first steps” in considering methods to evaluate your information security program:

1. Make certain you are aware of and meet any specific legal or contractual compliance requirements. These may effectively set the baseline expectations for your program.
2. Ensure that you plan for and implement periodic internal evaluations of the cybersecurity program. (We recommend documenting these processes in your Master Information Security Policies and Procedures[26] or other similar, core policy or plan.) While these cyclical processes will involve risk assessments, new threats, and the evaluation of specific controls, they can also look at the program holistically, as well as prepare you for external reviews.
3. Communicate with your funding agency, home institutions, and colleagues about performance measurement practices and expectations. CI projects have been known to conduct peer assessments of security programs as a low cost way to get outside input, and compare notes.
4. Explore some of the tools and maturity models listed below.
    a. NIST’s Framework for Improving Critical Infrastructure Cybersecurity[27]
    b. NIST Special Publication 800-55 rev 1, Performance Measurement Guide for Information Security[28]
    c. Higher Education Information Security Council (HEISC) Information Security Program Assessment Tool[29]
    d. CERT Resilience Management Model (CERT-RMM)[30]
    e. Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)[31]
    f. Booz Allen’s Cyber Operations Maturity Framework[32]
5. Consider whether an external organization can help with an assessment of your program. External peer or expert reviews can provide added objectivity, as well as fresh perspectives.

---

[26] https://docs.google.com/document/d/1sfHvJ2-3ELksKQ2yHcpXMqdpK8J87roFCL2LjyC5iWQ/edit
[27] http://www.nist.gov/cyberframework/
[28] http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf
[29] http://www.educause.edu/library/resources/information-security-program-assessment-tool
[30] http://www.cert.org/resilience/products-services/cert-rmm/index.cfm
[31] http://energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf
[32] http://www.boozallen.com/media/file/Cyber-Operations-Maturity-Framework-viewpoint.pdf

2 Controls and Contexts

2.1 Identity and Access Management

2.1.1 Access Control and Privileges

This section covers access control in general and applies it to information systems directly. Physical access control is covered in the “Physical Security” section.

Access control is fundamental to information security, and represents an organization’s policies and practices around who has access to what information and information systems, the extent of that access (e.g., level of privilege), and when and under what conditions that access is granted and revoked. Access control policies and procedures can be simple or complex, and may be impacted by available technologies, project scale, and legal/regulatory requirements.

Projects should pay particular attention to the management of privileged accounts, and access to sensitive information and information systems. While your organization will likely need to develop and adopt tailored policies, we offer a template Access Control Policy with ideas for what to include and how to structure it. We suggest an asset-based approach to laying out general policies on access control.

Consider the following practices:

- Remote root access should not be allowed across trust boundaries, and should be further restricted wherever possible.
- Root access by users should be done in a manner that provides accountability to the user.
- Services that are only to be accessed from within a trust boundary (e.g., only hosts on the same cluster) should have access restricted to those hosts only. Even if the service does not have a known vulnerability, it should be restricted only to the hosts/networks where it is needed. Where access is allowed across trust boundaries, a strong authentication mechanism should be used to authenticate hosts or users. For example, host based SSH authentication should be restricted to nodes within a cluster.
- Monitoring gives the ability to detect problems and take the necessary actions to correct them. It can be used to discover the security holes opened intentionally by attackers or unintentionally such as disabled or unused services that may be enabled by mistake. While implementing a full Intrusion Detection/Prevention service is not a practical option for every project, some form of routine monitoring should be conducted.

Getting Started:

You may use the **Access Control Policy Template** as a starting point for creating and documenting your project or organization's policies. Some individual assets may require their own policies. The **Asset-Specific Access and Privilege Specification** template can be used as a basis for these more specialized documents.

When granting personnel access and privileges to information and information systems, the best practice is to grant the lowest level of access and privileges required for that person to do his or her job efficiently. This is often referred to as "least privilege."

Projects should consider both maintaining a list of all personnel, with a description of authorized access and privileges, and conducting a regular, periodic review of identity and access management components to ensure they are appropriately limited. Processes should be in place to remove access when personnel leave the project, are terminated, or no longer require access to certain information assets.

Getting Started:

The **Personnel Exit Checklist** is broken into three areas: physical security, revoking system access and administrative concerns. The checklist can be used to record task completion, the initials of the responsible staff member, date and a notes field.

2.1.2 Passwords and Identity Management

Identity management (IdM) is a vast and critically important area of information security, and an area where scientific CI and collaborations have presented serious challenges and offered considerable innovation. IdM is fundamental to securing information and information systems, but equally central to enabling collaboration, accounting, attribution, and other functions that make 21st century science possible. We can't begin to fully cover IdM in this document. CI projects' IdM implementations may involve complex credentialing schemes, trust relationships among multiple organizations, institutions, and communities, the limitations of legacy systems,... the list goes on. However, most if not all projects still rely heavily on passwords.

Password management practices and policies, particularly those around password length and complexity, are the subject of considerable debate. We believe the following recommendations, and the included Password Policy Template offer a good start at specifying a scientific CI password management implementation.

Our Password Policy Template was influenced a great deal by the SANS Password Policy[33], and the work of the Software Assurance Marketplace (SWAMP) security and identity management teams.

Getting Started:

The **Password Policy Template** may be used as a starting point for your project's policy.

Recommended practices:

- Use strong authentication mechanisms (e.g., require strong, complex passwords, GSI, SSH keys, OTP) for services. Set a strong minimum standard for password strength for all project accounts.
- Be sure you harmonize internal facing policies with the recommendations and requirements you place on external users (e.g., through an Acceptable Use Policy).
- Ensure that your administrators and security personnel can react quickly to potential password compromises.
- Clearly state and communicate policies on the protection of issued credentials. Everyone must play a role in protecting the secrets that give them access to project assets. See the Password Policy Template and Acceptable Use Template for more. Include password protection in your training and awareness efforts.
- Ensure that, where passwords are transmitted across a network, they are encrypted.
- Encourage the use of well-established password managers (e.g., LastPass, KeePassX, 1Password, Dashlane), and informed practices on how to use them well.[34]
- Implement common password checking and reject user-generated passwords that show up on the list. Some passwords and passphrases are considered weak not because they fail to meet length and complexity requirements, but because they are commonly used, or based on dictionary words, common phrases, famous quotes or a simple variant of either. We recommend the use of a common password library, such as the cracklib library, to perform such a check and reject common passwords.
- A common mitigation against online brute force password attacks provides for account locking or IP blocking following a number of failed authentication attempts. There are variations on how to implement this, but implementing something is good practice. The account lockout threshold should be high enough that legitimate users do not accidentally lock their own accounts. Also, account lockouts can be used as a denial of service attack so blocking a specific IP address may be better than a complete account lock.
- Carefully control access to privileged accounts and require accountability and higher security requirements for users who have privileged access. Consider increased minimum standards (e.g., increased character length requirements) for administrative/privileged accounts. Very large, random passwords are made feasible by contemporary password managers, and size dramatically increases resistance to certain types of attacks.

---

[33] http://www.sans.org/security-resources/policies/general/pdf/password-protection-policy

[34] We note that passphrase based systems can also produce strong results, with added benefits of memorability. Due to the relatively recent advent of passphrase practices and increasing utility of encrypted password managers (in a world where many of us have 10's if not 100's of unique passwords) we focus on passwords, though passphrases can be particularly helpful in designing hard-to-crack, yet memorable mechanisms for accessing password manager accounts.

- When possible, use multifactor authentication mechanisms, particularly for privileged access. (Password + One Time Password or SSH Key + One Time Password). Multifactor authentication is becoming increasingly affordable and usable, and can have a dramatic positive impact on access risks.
- Whenever a system may be administered by more than one individual, sudo should be used to delegate that ability so that the system can accurately log which user took each action.

2.1.3 Enforce Access Control, Monitoring, and Logging

In order for an information system to be useful to users, it must be made available for access by users. An information system may have different components available to different sets of users. Configuring each component to allow a particular set of users is the challenge of "access control". Once a user has gained access to the system, activities should be monitored to make sure that the user does not perform unapproved actions. Additionally, all activity should be logged, ideally to a remote system, for possible auditing at a future time.

System monitoring does not need to be strictly user-focused. Intrusion detection systems (e.g., OSSEC HIDS[35]) can monitor networks or hosts for malicious activities and alert system administrators of potential policy violations. Vulnerability scanners (e.g., QualysGuard[36]) can be employed to routinely probe the system for weakness and alert system administrators of possible configuration problems. Configuration management utilities (e.g., Puppet[37]) can monitor crucial system configuration files and revert to a known good state. Log analysis tools (e.g., logwatch) can scan system logs and issue reports of past activities of interest. Any system design should consider all of these components to help defend against malicious activities.

Resources:

- NIST 7316 Assessment of Access Control Systems[38]
- NIST SP 800-115 Technical Guide to Information Security Testing and Assessment[39]
- NIST SP 800-92 Guide to Computer Security Log Management[40]

2.2 General Technical Controls

2.2.1 Configuration and Maintenance

Information systems are in a constant state of change influenced by a number of factors such as changes to support new features, patching software for correcting flaws and vulnerabilities and to accommodate new hardware or software to the system. To ensure that configuration changes made to systems do not adversely affect the security of the organization, a well-defined configuration management process that integrates information security is needed. A configuration management process should include a description of the roles, responsibilities, policies, and procedures that apply

---

[35] http://en.wikipedia.org/wiki/OSSEC
[36] http://en.wikipedia.org/wiki/Qualys
[37] http://en.wikipedia.org/wiki/Puppet_%28software%29
[38] http://csrc.nist.gov/publications/nistir/7316/NISTIR-7316.pdf
[39] http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf
[40] http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf

when managing the configuration of products and systems.

A configuration management process should address:

- identification and recording of configurations that impact the security posture of the information system and the organization;
- the consideration of security risks in approving the initial configuration of systems;
- the analysis of security implications of changes to the information system configuration; and
- documentation of the approved/implemented changes.

Additional resource: NIST Special Publication 800-128 "Guide for Security-Focused Configuration Management of Information Systems"[41]

2.2.2 Operating Systems and Device Firmware

Every device is controlled by something; all userspace software runs on something. That 'something' may provide points of entry for attackers, or it may simply enable ill-behaved user-installed software to do so. Nothing on a system can be trusted if the underlying operating system has been compromised.

Rule 0 of operating system security is to apply security updates in a timely manner. Ideally, this is within hours, but a 48-hour window is not unreasonable for low-risk assets.

When working with embedded devices, it is especially important to be certain that the firmware on any device that is difficult/expensive to replace or otherwise likely to be in long-term use is capable of being updated or replaced. Too often, these things are rushed to market with no way to ensure that known vulnerabilities ever get fixed.

While the configuration of specific operating systems vary, the widely accepted best practice is to give not just every user but every process on the machine the most restrictive permissions possible (i.e., "least privilege") while still getting the job done, and to isolate users and processes from one another to the greatest extent possible.

For low-risk targets, keeping any appropriate OS properly configured and updated is enough. However, for higher-risk targets, such as servers that contain sensitive information or control systems for sensitive equipment, additional controls should be considered:

- Restrict software running on the machine to the barest minimum: More software means more potential points of compromise.
- Use virtualization or other segregation strategies (e.g., Linux chroot, BSD jails) to prevent one user or piece of software from accessing another's resources.
- Keep sensitive systems physically separated (i.e., on different hardware) from one another and especially from less security-critical systems.
- Use an operating system such as Linux or UNIX (e.g., BSD, AIX, Solaris, Illumos) that offers hardening kits to further secure the system with manageable maintenance overhead. SELinux

---

[41] http://csrc.nist.gov/publications/nistpubs/800-128/sp800-128.pdf

is one such hardening system worth considering if you run Linux. One alternative to SELinux is grsecurity, but be aware that this option requires more advanced knowledge to correctly configure.

- Microsoft Windows clients should use the Enhanced Mitigation Experience Toolkit (EMET) [42] to enable exploit mitigations in software that is exposed to untrusted data, such as web browsers, PDF viewers, and Office applications.

2.2.3 Network-level Controls

Networks provide the computer communication infrastructure for cyberinfrastructure projects. It is important to ensure that the way in which your network is designed and used does not inadvertently provide avenues of attack. Over the life of the project new devices will be added to the network and changes will be made to the network topology.

In some cases, projects will make use of existing networks. Potentially, these networks will be under the control of either departmental, or campus IT organizations. In these cases, it is important for the project to understand their responsibility for being good network citizens. The following issues will still be important so take time to understand how the network owners address them and what your project must do to comply with their policies.

Brand new network infrastructures offer a unique opportunity, in that they allow a project to design security from the start. Inherited infrastructures bring with them their existing security which may or may not be adequate for the job. When designing a new network take the time to do an evaluation of the security needs and how to make sure the environment will mitigate the risks identified.

When securing your network, you should address the following ideas:

Restrict devices to specific network segments
In practice, user accessed devices such as print servers and file servers should be assigned to connect to a single segment in your network.

> Spotlight on Science: *Network Protections for Science DMZs*
>
> Science DMZs by necessity lack the stateful firewall and/or VPN protection relied on by some other technologies. Restricting communication to a reasonable set of IPs as well as carefully monitoring both traffic to/from and activity inside the Science DMZ are essential to preventing and responding to security incidents.
>
> Science DMZ security is covered in more detail in Section 2.7.2.

Firewall
Your project should have a default configuration for all firewalls. If you are unsure of how to go about configuring your firewall, check with your campus IT security department and they should be able to help. In many cases, campus or departmental IT organization provide firewall services.

---

[42] https://www.microsoft.com/emet

The following are good sources of information on firewall configuration:

- SANS Institute Firewall Checklist[43]
- *Securing Your* Network with *Firewalls* and Ports - MSDN[44]

Electronic communications

Internal clients and servers should not communicate directly with external systems. If a communication channel with external systems is needed some type of device, such as a firewall, should be used.

Virtual Private Networks (VPN)

If possible, consider containing the information systems within a VPN. This will greatly reduce the attack surface since an adversary would have to compromise someone with VPN access before attacking the information systems within the VPN.

Protecting DNS traffic

DNS should be deployed in a way that it protects the internal system from direct manipulation.

- NIST Securing DNS Guide How to Secure a Domain Name Server (DNS)[45]

Use of secure routing protocols or static routes

Either secure routing protocols or static routes should be used when exchanging information with outside parties. Best practice would be to never share routing information with any outside party.

Deny use of source routing

Source routing should not be allowed.

2.2.4 Application Administration and Use

Selecting applications with good security track records is essential not only to the security of information and services handled by those applications, but also the security of the systems upon which they reside. Anything that faces a network connection should, at a minimum:

- Have a prominently documented avenue for reporting bugs in general and security issues in particular.
- Have clear documentation on how to configure the software in the most secure manner possible.
- Have a reputation for promptly handling vulnerability reports.
- Publicly document past vulnerabilities and in what software version(s) they are fixed.
- Publicly document what authentication mechanisms and other security measures are used by the software.

For open source applications, the ability to view the code and development activity directly can provide valuable insight into the project's security. It is worth checking that such projects are still

---

[43] http://www.sans.org/score/checklists/FirewallChecklist.pdf

[44] http://msdn.microsoft.com/en-us/library/ms960403(v=cs.70).aspx

[45] http://csrc.nist.gov/groups/SMA/fasp/documents/network_security/NISTSecuringDNS/NISTSecuringDNS.htm

under active development, and that they are following the application development practices provided in the Application Development section.

2.2.5 Managing Data Repositories

Data repositories are usually comprised of at least one database. Along with the database providing organization to the structure of the data, tools are provided to make the querying of that data simpler for scientists.

These repositories provide a place for scientists to store their data and also find information from other research projects. While it is common for these repositories to be open to the entire research community supported by the data, it is also common for certain parts of the data to be controlled by some type of access control logic. This could be to protect proprietary data or to keep research findings private until after publication. Good technical security practices should be supported by clear communications with the user community, as trust in security and privacy controls can be central to the success of a repository.

When addressing security of the data repository, the first step that should be taken is to use standard, established database security practices. Additionally, a project might want to address the types of data they have in their repository and develop an information classification policy. See Section 2.2.6 immediately below. Other policies that should be developed around access control (*see*, 2.1.1) and disaster recovery (*see*, 2.6.1).

2.2.6 Protecting High Value & Sensitive Information

Information itself, embodied as electronic data or otherwise, comprises the most fundamental asset in information security. As such, just as technical or physical information systems must be managed in line with a project's mission and risk management processes, so too should information itself be managed and protected as warranted. While not all information that generates from, passes through, or is stored within a project carries heavy requirements for confidentiality, integrity, or availability, scientific CI may work with information carrying a variety of security and privacy requirements.

Research data, including raw, time-sensitive, or one-of-a-kind -- and potentially huge -- data flows may be one of the most valuable, most science "mission critical" project assets of any kind. While there is a tendency to think first of confidentiality when considering the security of information, the research community is full of examples of information where the availability and integrity of information is essential to the scientific endeavor.

High value and useful information is often also sensitive information, carrying both heightened security requirements and heightened risk of being targeted. That said, confidentiality requirements and concerns generate from myriad sources. Research, legal, regulatory, and ethical requirements may amplify the need to protect access to and distribution of information. Sources include federal and state privacy laws and regulations, export control laws, employment laws, contractual relationships, human subjects policies, institutional policies and practices, and the need for academic pre-publication secrecy.

Many, if not all, of the controls and practices identified in this guide are relevant. The section below on Data Repositories highlights a few key controls for protecting electronic data. Additionally, a comprehensive information security program will address the security and appropriate distribution of information in physical form (e.g., physically securing sensitive paper documents), as well as expectations, policies, and procedures regarding high value and sensitive information within personnels' personal knowledge. Projects may wish to consider implementing a formal Information Classification Policy.

Getting Started:

The **Information Classification Policy Template** may be used as a guide to picking classification categories for your project's data.

Information classification policies support the management and protection of information by formalizing the categorization of information, and processes for making those categories a functional part of information handling. Put simply, these policies help organizations simplify and clarify how they communicate about information. This can be particularly critical for projects with information carrying confidentiality requirements. Creating, implementing, and enforcing an information classification policy requires judgment, ongoing effort, and understanding throughout an organization.

Classification categories can and likely should be customized for a project's security needs. There is no single standard for an information classification policy; a review of the available regimes indicates a variety of category labels[46], as well as some variety in concerns that underlie the particular choices. We offer a few recommendations:

- Classification category names should be descriptive of how the information should be handled, and clearly defined with examples. Consider using category names that clearly state who is authorized to have access to the information and the authorized scope of distribution.
- The classifications assigned to specific pieces and types of information should logically reflect the level of risk associated with a loss of confidentiality, integrity, and/or availability of the information.
- Over-classification of information should be avoided. Information that is not high risk should not be labeled as such. Compliance requirements based off information classification will require excessive controls that may not be needed if the information was correctly labeled as low risk.
- Where possible, the information category should be embedded in and/or visible on the information itself.
- Utilize the fewest number of discrete categories that reasonably aligns with your project's security needs. Unnecessary complexity may hinder implementation and add confusion.

---

[46] Information Classification Policy (ISO/IEC 27001:2005 A.7.2.1)
http://www.iso27001security.com/ISO27k_Model_policy_on_information_classification.pdf;
CMU Guidelines for Data Classification
http://www.cmu.edu/iso/governance/guidelines/data-classification.html;
Texas State Data Classification Policy Template
https://www2.dir.texas.gov/SiteCollectionDocuments/Security/Policies%20and%20Standards/data_classification_policy.rtf

Information classification may appear cumbersome as an organization kicks off implementation, but it becomes easier and part of the natural flow of working with information as an organization gains experience with the process. Moreover, the classification process can have the added benefit of increasing communication around the purpose and importance of an organization's work.

2.2.7 Hardware Platforms

Most hardware security concerns are handled with appropriate physical access policies. However, management of hardware presents risks on the networking and software/data levels. When considering the security of any hardware platform, make certain to give thought to the following:

- Who will have physical access to the hardware, and how will those who shouldn't access it be prevented from doing so? (See the section on Physical Security)
- How will the person managing the hardware access it? Can any firmware on the device be updated in the case of a security vulnerability? (See the subsection 'Operating Systems and Device Firmware' below)
- How will data contained on the hardware be backed up? (See the section on Operational Risks)
- How will the hardware's resources (power, network connection, environmental temperature) be maintained? (See the section on Physical Security)
- If the hardware in question is an appliance (i.e., hardware that comes with a specialized software stack), is the software running on it reasonably secure? (See the subsection 'Operating Systems and Device Firmware')

2.2.8 Asset Disposal or Redeployment

FIPS-199, Standards for Security Categorization of Federal Information and Information Systems states: "A loss of confidentiality is the unauthorized disclosure of information." Proper disposal of system assets is one way to maintain confidentiality. The main concern is long term storage devices found in many modern assets. Mobile devices, photocopiers, printers, tablets and many other assets all contain some type of storage device. Your policy on disposal should include instructions on what to do to sanitize those media. Those instructions should include, at a minimum, direction on how to destroy or erase the contents of those storage devices found in all your assets. NIST Special Publication 800-88, "Guidelines for Media Sanitization",[47] provides more details on how to implement an asset disposal policy.

Getting Started:

The **Asset Management Policy** may be used to jump start your project's policy creation.

---

[47] http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_with-errata.pdf

2.2.9 Mobile Devices and BYOD

Increased use of mobile devices (e.g., smartphones and tablets) to access institutional networks and project information assets increases the number and scale of attack surfaces through which security incidents may originate. Meanwhile, the incidence of mobile malware is regularly reported as increasing rapidly.[48] Adding to the complexity of mobility's security implications is the Bring Your Own Device (BYOD) movement which has swept through the enterprise world, and is a familiar norm in many academic and research settings. While BYOD takes on many forms, it almost universally implicates dual work/personal use of mobile devices, i.e., personnel accessing work data and information systems via personal devices and/or using work devices in a variety of non-work settings and for non-work purposes.

For science projects, the risks associated with mobile may be particularly relevant for projects with sensitive data and communications, or networked control systems.

Mobility and BYOD have been two of the primary drivers away from purely perimeter oriented views of information security best practices. These readily moveable and often personally owned endpoints face an increased inherent risk of loss, theft, or simply coming into contact with non-personnel. It may be impractical or difficult to enforce the use of anti-virus software, and regular software updating. The many device operating systems that result from an entirely open BYOD environment means that not everyone's device is equally securable.

However, except in extremely sensitive environments, it may be impractical (and even unwise) to place more extreme controls in the way of mobile device use. Projects may lack the resources (or desire) to purchase work-only devices (particularly phones) for their employees, or purchase and implement a mobile device management (MDM) solution. As such, policies and personnel education around those policies are key. Consider the following steps:

- As always, review and align to parent institution policies.
- Require that all mobile devices accessing project data or systems to be maintained with up-to-date operating system patches. Devices running Android operating systems often lack features to protect data (encryption, remote wiping) and more than 60% are running unpatched OSs from two years ago or older[49]. Caution should be given with allowing access to sensitive data from an Android platform.
- Require basic, included security controls (e.g., unlock codes, data encryption, remote wiping and device locating capabilities) to be turned on.
- Require personnel to report mobile device theft/loss to the project within a tight window following the event and require the personnel to change any passwords that were exposed to the mobile device.
- Forbid personnel from accessing sensitive data or systems from unapproved devices.
- Forbid personnel from accessing sensitive data or systems from insecure open WiFi networks without using a VPN.

---

[48] McAfee Labs Threats Report, June 2014, p.19, Available: http://www.mcafee.com/hk/resources/reports/rp-quarterly-threat-q1-2014.pdf

[49] Android Developer Dashboards, See the Platform Versions section at https://developer.android.com/about/dashboards/index.html

These policies may be captured in an acceptable use policy, an employee handbook, or even in a standalone mobile usage policy. Regardless, your project’s mobile policies should be part of your information security training and awareness program.

2.2.10 Supervisory Control and Data Acquisition (SCADA)

In 2010 the discovery of the Stuxnet worm demonstrated how industrial control systems, such as supervisory control and data acquisition (SCADA) and programmable logic controller (PLC) systems, could be subverted by an attacker. Even systems protected by air-gap networking, physically isolated from unsecured networks, became victims of the worm via infected USB devices inserted in the systems.

Some large facilities in the CI community may use SCADA systems for controlling large equipment such as telescopes or wind farms. Additionally, SCADA may be used for infrastructure services including power distribution systems, heating/cooling systems, ventilation and air treatment systems. If your project uses industrial controls, it’s critical to ensure they are protected from and resistant to malicious attacks. Hacking an industrial control system can result in corrupted data, service interruptions, physical damage to equipment and can even threaten human life.

Some industrial controls lack the ability to have their firmware updated to address vulnerabilities making them defenseless targets for attackers. Therefore it’s imperative that equipment vendors have a comprehensive program to maintain the security of their products. In addition, projects that use industrial controls should have a strong communication and service relationship with equipment vendors in order to get critical ongoing support.

Securing SCADA systems is unsurprisingly similar to the process outlined earlier in the “Establishing a Risk Management Framework” section of this guide. This process begins with understanding your SCADA system (system characterization), identifying threats to the SCADA system, identifying system vulnerabilities, conduct a threat/impact/probability analysis and selection of controls to mitigate the risk.

The Department of Energy publishes a guide to improve cybersecurity of SCADA networks.[50]

SCADA Cyber Security Testbed Development[51]

An Evaluation of Cybersecurity Assessment Tools on a SCADA Environment[52]

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) offers several resources on the best practices for securing control systems and SCADA equipment.[53]

¶

¶

---

[50] http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/21_Steps_-_SCADA.pdf

[51] http://www.linklings.net/MOSES/papers/NAPS06-258.pdf

[52] http://powercyber.ece.iastate.edu/publications/conf_sec_tools.pdf

[53] https://ics-cert.us-cert.gov/

2.3 Managing Relationships & Social Controls

2.3.1 Training and Awareness

Efforts aimed at personnel training and awareness are widely, if not universally, considered part of any comprehensive organizational cybersecurity program. Human beings, including well-meaning, non-adversarial organizational personnel, are often described as the “weakest link” in any cybersecurity effort. The positive impact of well-written policies and highly-tailored technical controls can hinge on personnel awareness, understanding, and compliance.

Projects should establish, implement, and maintain cybersecurity awareness and training activities for all personnel. Consider including the following content:

- Communicating why cybersecurity efforts are important to the project and the potential impact of cybersecurity incidents
- Information on common cybersecurity threats and how to identify and respond to them
- Review of the projects’ policies and procedures, including roles and responsibilities, incident response plans
- Close review of the policies that require personnel action or attention

Awareness and training activities need not necessarily be highly involved and time-consuming, but they should be regular and direct. Whether quarterly, biannually, or annually, all personnel should participate on a recurring basis. Additional resources on security awareness and training include: NIST Special Publication 800-50, Building an Information Technology Security Awareness and Training Program.[54]

Getting Started:

You may use the **Information Security Training and Awareness Policy Template** as a basis for writing a policy specific to your project or organization’s needs.

CTSC has made available an information security training presentation that may be used for your organization: **CTSC Information Security Training slidedeck**[55] was structured off the Texas Department of Information Resources[56] - “Security Training Policy Template”.

---

[54] http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

[55] http://trustedci.org/guide/docs/trainingdeck/CyberHygiene

[56] http://www2.dir.state.tx.us/SiteCollectionDocuments/Security/Policies%20and%20Standards/security_training_policy.doc

2.3.2 Resource Users

Acceptable use policies (AUPs) are a common way for organizations to communicate to resource users the acceptable, and unacceptable, uses of information systems, including networks, websites, compute resources, as well as repercussions of violating those policies. We include a template AUP to consider tailoring to your project's needs. We encourage you to develop a clear, concise AUP, written in plain language. AUPs should be made readily available to users, and where feasible require explicit acknowledgment prior to resource access. Even if your AUP is written with a third party user (e.g., a researcher) in mind, consider whether requiring acknowledgment by project personnel is appropriate. Finally, AUPs can be documents of particular legal significance, and may include contractually binding language, as well as other legal statements. We strongly encourage you to seek legal assistance (e.g., from your institution's general counsel's office) prior to implementing an AUP.

Getting Started:

The **Acceptable Use Policy Template** may be used to help develop an AUP specific to your project.

Privacy policies are an increasingly common fixture for websites and online services of all kinds. In general, they communicate to users the ways the resource provider gathers, uses, discloses and manages data regarding user, and may include details regarding when and how users will be notified in the event of an actual or potential leak of personal information. Like AUPs, privacy policies can be documents of particular legal significance. Depending on the site or service you offer, to whom you are offering it, what legal entities are involved, the parties' jurisdictional locations, and a host of other factors, your project may want and/or be required to have a privacy policy (or policies), and the policy may be required to meet particular requirements. We strongly encourage you to seek legal assistance (e.g., from your institution's general counsel's office) for assistance in determining the need for, as well as writing and implementing, a privacy policy.

2.3.3 Partners & Contractors

Relationships with partners and contractors can take many forms, from contractual business relationships to informal collaboration. For addressing information security in the context of these relationships, we offer a few broad recommendations:

- Communicate and formalize expectations at the outset of the relationship. Whether through contractual terms (e.g., in service level agreement (SLA)), a memorandum of understanding (MOU), or other clear communications, getting on the same page (literally) is critical. It may be important for your organization to share key information security policies with your partners, and/or request to review the corresponding policies. An MOU might include the following mutual agreements:
    - Notify partners of any incident or compromise as soon as possible.

  - Ensure that system administrators and security personnel cooperate with the organization in a timely manner and follow formal processes agreed upon in advance.
  - Perform a thorough vulnerability assessment of any new resource.
  - Maintain all systems with the latest security patches, closing vulnerabilities in a timely manner commensurate with risk levels of the particular vulnerability.
  - Keep confidential information safe and not disclose information to an external party without the approval of all parties involved.
  - Disclose information internally on strictly a need-to-know basis.
  - Make all security policies, guidelines, and procedures readily available to staff and users.
- Communicate internally and with parent organizations. Your organization's personnel may need explicit input on how to interface with partner organizations in order to reduce information security risks. Many players may be involved in setting up formal relationships with vendors and contractors, and your project may well need to play an active role in communicating with multiple parties to ensure that information security is addressed.
- Ensure a reasonable level of visibility into the third parties' activity, so you have an opportunity to identify emergent security concerns.

2.4 Physical Controls

Physical access to computing resources and/or the infrastructure they rely on exposes a number of attack vectors, as physical access can be used to bypass many non-physical security controls such as firewall rules, filesystem permissions, and user login requirements. As with any other form of access, physical access to resources should be limited to the minimum needed for each individual to fulfill his/her work functions. Special care should be given to assess risks associated with the infrastructure supporting each computing resource, and to the higher vulnerability of mobile devices to theft or tampering compared to devices bound to a single location.

According to FIPS 200, "organizations must:

> (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals;
> (ii) protect the physical plant and support infrastructure for information systems;
> (iii) provide supporting utilities for information systems;
> (iv) protect information systems against environmental hazards; and
> (v) provide appropriate environmental controls in facilities containing information systems."

Getting Started:

The **Physical Security Policy Template** may be used to simplify the creation of an appropriate policy for your project.

When using the template, it is important to be mindful of risks and protections inherent in using facilities belonging to or shared with other organizations.

2.4.1 Plan and Protection

The physical and environmental security policy should identify risks to the systems and facilities to address unauthorized physical access, loss, damage or interference. Basically, any risk that could cause interruptions to its critical operations should be considered when looking at controls for physical security.

2.4.2 Monitoring, Logging, and Retention

A project should have technical and procedural controls in place for monitoring physical security. These should include logging of access to devices so that individuals can be identified as to who and when the access was made. Also, consider whether there are regulatory or compliance requirements for retention of records.

2.4.3 Maintenance and Testing

Like cybersecurity, your physical security system must be tested periodically to ensure it operates correctly. Testing and maintenance records of the physical security should be kept for a period of time. The length of time these records are kept can be determined by the project but might also be affected by regulatory or compliance issues.

Resources:

- NIST SP 800-12: An Introduction to Computer Security: Physical And Environmental Security[57]
- DHHS POLICIES AND PROCEDURES: Physical and Environmental Security Policy[58]
- University of Miami School of Medicine: Physical and environmental security[59]

2.5 Application Development

A complete overview of secure coding practices is beyond the scope of this document. However, it is worth addressing some general points, including language and framework selection, handling vulnerability reports, and concerns specific to the development of web applications.

2.5.1 Languages and Frameworks

When selecting a language or development framework for a project, many of the same things that lead to good code in general are also important to security. First and foremost, choose to build on a platform that is actively maintained and preferably open source. The deprecation of a platform tends to lead to stagnant and usually vulnerable code in dependent applications, which in turn means that security updates are unlikely to happen at all in practice, regardless of the intentions of a project's developers. Too often, deprecation of an application’s underlying framework leads to neglect of that application. An application that does not receive developer attention over a long term usually aggregates unpatched but known security flaws -- flaws that are potential points of entry for an attack. While choosing an open source language or framework does not completely eliminate this

---

[57] http://csrc.nist.gov/publications/nistpubs/800-12/800-12-html/chapter15.html
[58] http://info.dhhs.state.nc.us/olm/manuals/dhs/pol-80/man/07physical_env_security.pdf
[59] http://it.med.miami.edu/x2230.xml

possibility, if an open source tool in active use is abandoned by its creators, it is normally picked up and continued by members of its user community.

Of secondary concern is whether the language's libraries or the chosen framework provide the primitives necessary for developers who are not themselves security experts to develop secure applications. This includes reliable cryptographic primitives, authentication systems, functions for sanitizing user input, and -- in some cases -- facilities for recognizing patterns associated with abuse of a service or resource. Small projects especially cannot bear the overhead of developing these tools in house with the amount of research, attention, and constant review and upkeep necessary, so choosing the right development stack is essential.

2.5.2 Vulnerability Reports

Handling vulnerability reports is one place where small software development projects often fall down. First of all, the correct avenue for reporting vulnerabilities must be absolutely clear to the software's entire user base. At least, a cursory reading of the project's main web page must reveal how to report a security vulnerability. Reporters should be requested to keep vulnerability reports confidential until the project has had time to issue a fix. However, project maintainers must understand that those who discover vulnerabilities may not be under any obligation not to release said knowledge publicly. The project's handling of the incident may heavily influence whether the person reporting a vulnerability discloses it privately or not.

Vulnerability reports should be handled as quickly as possible, especially for software that may be handling sensitive information or controlling sensitive equipment. First, reply to the person who reported the vulnerability and engage them in the process. Not contacting someone who's submitted a vulnerability in a timely manner (less than one business day ideally, up to a week for small or pre-release projects) will often lead to that person assuming that the vulnerability is not being addressed and release information about it publicly.

Like any bug, a security vulnerability should be patched and a regression test created to prevent it from being re-introduced. When an update is issued to the software's consumers, it should be made absolutely clear what systems are impacted (e.g., "this may affect your system if you compiled in support for TLS"), the severity of the problem, and what it may allow an attacker to do.

It is important to differentiate security patches from other software improvements for the benefit of users who do less-frequent updates when security is not at issue, and to number or otherwise uniquely identify each vulnerability so that it can be referenced with clarity.

2.5.3 Web Applications

While web applications are not, at their core, more of a security risk than other software development, they deserve special attention due to their march toward ubiquity, the likelihood that data from more than one user or organization will end up centralized on one system, the readiness with which they are remotely attacked, and the difficulty in finding any attackers. Developers working on web applications should be mindful of OWASP's Top Ten list of web vulnerabilities[60] as well as development best practices for the language or framework in use. When possible, web applications that handle sensitive data should undergo routine penetration testing by a security

---

[60] https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

professional.

Spotlight on Science: *Gateways On the Web*

Remember that many science gateways include a web application as a component. When implementing or maintaining a science gateway, it is important to consider all aspects of web application security with regard to any interface that operates over HTTP or similar protocols.

2.6 Emergency Preparation and Response

2.6.1 Contingency Planning

Contingency planning is an important part of an overall disaster recovery plan. Contingency plans deal with using interim measures to recover a system after a disruption of services. NIST 800-34 states: “Interim measures may include relocation of information systems and operations to an alternate site, recovery of information system functions using alternate equipment, or performance of information system functions using manual methods.”

Contingency and disaster recovery planning are much like information security planning. These plans, like risk management, should identify potential vulnerabilities and threats and then implement approaches to either prevent such incidents from happening or limit their potential impact.

NIST 800-34 identifies the following steps as a planning process that a project may apply to develop and maintain a viable recovery program for their information systems.

1. Identify assets. Identify and prioritize information systems and components critical to supporting the project’s mission/business processes.
2. Identify preventive controls. Measures taken to reduce the effects of system disruptions can increase system availability and reduce contingency life cycle costs.
3. Create contingency strategies. Thorough recovery strategies ensure that the system may be recovered quickly and effectively following a disruption.
4. Develop an information system contingency plan. The contingency plan should contain detailed guidance and procedures for restoring a damaged system unique to the system’s security impact level and recovery requirements.
5. Ensure plan testing, training, and exercises. Testing validates recovery capabilities, whereas training prepares recovery personnel for plan activation and exercising the plan identifies planning gaps; combined, the activities improve plan effectiveness and overall organization preparedness.
6. Ensure plan maintenance. The plan should be a living document that is updated regularly to remain current with system enhancements and organizational changes.

Getting Started:

The **Disaster Recovery Policy Template** may be used to develop a policy tailored to your project, based on NIST Special Publication 800-34 "Contingency Planning Guide for Federal Information Systems".)

Resources:

- NIST SP800-34 "Contingency Planning Guide for Federal Information Systems"[61]
- Department of Health and Human Services Enterprise Performance Life Cycle framework: Contingency Plan[62]
- Cisco Disaster Recovery: Best Practices[63]
- SANS InfoSec Reading Room: Computer Security Considerations in Disaster Recovery Planning[64]
- SearchDisasterRecovery.com: IT Disaster Recovery Plan Template[65]
- everyday-tech.com: How To Create A Disaster Recovery Plan[66]
- Sybase Checklist for Disaster Recovery[67]

2.6.2 Incident Handling

Regardless of the security measures put in place for an information system, there remains the possibility of unauthorized access to the system and its data, commonly referred to as a "computer security incident". What constitutes an incident will depend on the organization and the system or resources involved. Examples of incidents include attempts to gain unauthorized access to systems or data, denial of service, unauthorized use of resources, or changes to system hardware, software, or data without the owner's consent. An organization should prepare for a possible incident by designating individuals who can handle the analysis, mitigation, and notification of the incident.

---

[61] http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

[62] http://www.hhs.gov/ocio/eplc/EPLC%20Archive%20Documents/36-Contingency-Disaster%20Recovery%20Plan/eplc_contingency_plan_practices_guide.pdf

[63] http://www.cisco.com/en/US/technologies/collateral/tk869/tk769/white_paper_c11-453495.html

[64] http://www.sans.org/reading-room/whitepapers/recovery/computer-security-considerations-disaster-recovery-planning-1512

[65] http://cdn.ttgtmedia.com/searchDisasterRecovery/downloads/SearchDisasterRecovery_IT_DisasterRecoveryTemplate.doc

[66] http://everyday-tech.com/how-to-create-a-disaster-recovery-plan/

[67] http://www.sybase.com/sb_content/1029285/dr_checklist.pdf

Getting Started:

The **Incident Response Policy and Procedures** Template may be used to develop an appropriate policy and the procedures required to execute an IR plan.

References:

- NIST SP 800-61 Computer Security Incident Handling Guide[68]
- NIST SP 800-86 Guide to Integrating Forensic Techniques into Incident Response[69]
- NIST SP 800-83 Guide to Malware Incident Prevention and Handling for Desktops and Laptops[70]

Spotlight on Science: *Notify Helpdesk*

It is not uncommon for incident reports that should go to a particular project to end up at the parent organization's help desk, simply because the reporter isn't sure where to go. It never hurts to provide the parent organization's helpdesk with contact information needed to make sure incidents are properly reported.

2.7 Concerns Unique to Science

Often, the biggest challenge in cybersecurity for science is that science often uses technologies and processes that are outside the mainstream. Science itself is extremely varied in its technology needs. So, it is not uncommon for a project or organization to need to figure out how to secure a system or systems for which there isn't a great deal of explicit guidance available.

Many unique-looking science systems are aggregates of well-understood techniques and technologies. Often, breaking something complex, such as a science gateway, down into component technologies (e.g., web application/portal, database servers, and job queues for industrial controls) will produce useful insight as to what controls may be needed. Another, often complementary, approach is to carefully characterize the system itself, and work from there.

Asking the following questions when approaching such an information system will put one well on the way to an understanding of how to secure it:

- What are this system's components?
- Are there known best practices for any of the component technologies? What are they?
- How do these components interact with one another?
    - Do they need to authenticate with one another? If so, how is that accomplished?

---

[68] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
[69] http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf
[70] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf

    - Where are the boundaries between the components? How is this separation maintained, especially where it impacts the movement of information or control over code and configuration?
    - How do the system's various components communicate with one another?
- Who is authorized to access the system and what privileges do they possess?
- How does the system handle authentication and authorization on a technical level?
- What APIs does the system offer? How are other applications expected to use the APIs, and what protections are in place to prevent undesired behaviors?
- How is the system's data stored?
    - Don't forget to look at backups as well as the primary data storage.
- What level of accounting/logging is needed?
- What other data can be accessed via the system?
- What equipment can be controlled via the system?
- What platform(s) and language(s) were used to build the system?
- If system components are developed in-house, is the development team using best practices to maintain the security of the code base?

2.7.1 Custom Scientific Equipment

In addition to commodity information technology hardware and software, many projects may use unique equipment that serves a specific role in the research process. For instance, interferometers may be used for measuring gravitational waves and Digital Optical Modules (DOMs) for measuring neutrinos. Projects measuring environmental data across a large geographic area may use specialized field instrumentation to create wireless sensor networks.

Custom scientific equipment requires the same security attention as commodity hardware and software and often even greater attention, as such equipment may constitute a project's largest investment and most mission critical asset. Some custom equipment can be remotely controlled by a network connection which increases the risk of unauthorized access and/or abuse. The abuse or misuse of certain types of equipment can result in physical damage to the instrument and it's surrounds, including the threat to human life.

Another form of abuse that is becoming more common is the misuse of resources in scientific research for monetary gain.[71] CI projects offer the community tremendously powerful resources that could be exploited to mine digital currency that can be converted into traditional currencies. For instance, having each user agree to observe an acceptable use policy that bans the abuse of resources, along with a network monitoring service that detects mining activity and communications would be effective controls to minimize this risk.

2.7.2 Science DMZ

Science DMZs[72] came into being as an approach to provide the low-latency, high-bandwidth connections demanded by scientific computing applications without giving up on security. Because a Science DMZ exists at the edge of its local network (or as close as possible thereto), typically outside

---

[71] Tim Hornyak. (2014, June 5). US Researcher Banned for Mining Bitcoin Using University Supercomputers. CIO [Online] Available: http://www.cio.com/article/753803/US_Researcher_Banned_for_Mining_Bitcoin_Using_University_Supercomputers

[72] https://fasterdata.es.net/science-dmz/

institutional firewall and monitoring infrastructure, seeing to the DMZ's security needs typically falls to the project running it rather than larger institutional resources.

Much of a Science DMZ's speed is owed to its avoidance of stateful firewalls and traffic shaping mechanisms normally in place on large enterprise networks. Network-level security is often handled largely or even solely through router ACLs. This particular approach is most effective when those ACLs are automatically updated in response to information gathered by an intrusion detection system (IDS) such as the Bro Security Network Monitor.[73] Bro keeps detailed records of application-layer state. Its analytics can be mapped to behavioral patterns of end users, so automated security scripts can respond in real-time, e.g., updating router ACLs or notifying security on-call personnel.

In addition to helping to keep traffic moving, network performance monitoring tools such as perfSONAR[74] can enhance security on a Science DMZ. Such tools will give the project a clear understanding of how the flow of traffic is moving on the network, information that may aid in coping with, e.g., DDoS attacks.

Collecting session data, such as netflow or IPFIX, is useful because it can be done passively, providing situational awareness for the network without adversely affecting network performance. This data, especially when correlated with data from an IDS like Bro, can help identify outlier behaviors that may be early indicators of malicious activity, e.g., an attacker's lateral movement within the network, command and control traffic, or data exfiltration. Since session data does not contain the contents of the traffic, it does not take up much space, allowing an extensive history to be saved and analysed. SiLK[75] and Argus[76] are two session data suites that may be used for this type of data collection and analysis.

Further reading:
Science DMZ Security - Firewalls vs. Router ACLs[77]

2.7.3 Science Gateways

A science gateway is a set of tools, applications, and data collections that are integrated via a portal or a suite of applications. Gateways provide access to a variety of capabilities including workflows, visualization, resource discovery, and job execution services, allowing scientists around the world to more effectively collaborate using shared cyberinfrastructure and data.

Each of these topics is covered in this guide and more information may be found at the Gateway Security website[78].

---

[73] http://bro-ids.org/
[74] http://www.perfsonar.net/
[75] https://tools.netsa.cert.org/silk/docs.html
[76] http://qosient.com/argus/argusnetflow.shtml
[77] https://fasterdata.es.net/science-dmz/science-dmz-security/
[78] http://www.sciencegatewaysecurity.org

Appendix: Templates, Forms, and Resources

All templates and forms can be found and copied at ***trustedci.org/guide****.*

Template Policies

Acceptable Use Policy Template http://trustedci.org/guide/docs/AUP
Set of rules that a user must agree to follow in order to be provided with access to a network and/or resources. Used to reduce liability and act as a reference for enforcement of policy.

Access Control Policy Template http://trustedci.org/guide/docs/ACP
Defines the resources being protected and the rules that control access to them.

Asset Management Policy Template http://trustedci.org/guide/docs/AMP
Requirements for managing capital equipment including: inventory, licensing information, maintenance, and protection of hardware and software assets.

Asset-Specific Access and Privilege Specification http://trustedci.org/guide/docs/asset_access
List of roles, privilege levels and their justification for an asset.

Disaster Recovery Policy Template http://trustedci.org/guide/docs/recovery
Contains policies and procedures for dealing with various types of disasters that can affect the organization.

Incident Response Policy and Procedures Template http://trustedci.org/guide/docs/IR
A pre-defined organized approach to addressing and managing a security incident.

Information Asset Inventory Template http://trustedci.org/guide/docs/IAI
Provides a framework for cataloguing and describing a project's assets relevant to cybersecurity, i.e., both information and information systems.

Information Classification Policy Template http://trustedci.org/guide/docs/info_class
Used to ensure consistency in classification and protection of data.

Information Security Training and Awareness Policy Template http://trustedci.org/guide/docs/TAP
Outlines an organization's strategy for educating employees and communicating policies and procedures for working with information technology (IT).

Master Information Security Policy & Procedures Template http://trustedci.org/guide/docs/MISPP
Represents the core information security policies and procedures including information security-related roles and responsibilities; references to other, special purpose policies; and the core procedures for developing, implementing, and maintaining the information security program.

Password Policy Template http://trustedci.org/guide/docs/password
A set of rules designed to establish security requirements for passwords and password management.

Physical Security Policy Template http://trustedci.org/guide/docs/physical
Details measures taken to protect systems, buildings, and related supporting infrastructure against

threats associated with their physical environment.

Forms & Tables

Personnel Exit Checklist http://trustedci.org/guide/docs/exitlist
Form to be completed at the end of employment that addresses revoking access to resources, physical space and the return of organizational assets.

Risk Assessment Table http://trustedci.org/guide/docs/RAtable
Spreadsheet for doing semi-quantitative risk assessments based on the method presented in Section 1; especially helpful in that it automates the math and highlights risk levels for a nice visual presentation.

Resources

Securing Commodity IT in Scientific CI Projects: Baseline Controls and Best Practices
http://trustedci.org/guide/docs/commodityIT
Best practices to establish a baseline level of information security practice for commodity Information Technology (IT) infrastructure.

CTSC Infosec Training Slidedeck http://trustedci.org/guide/docs/trainingdeck/CyberHygiene
A set of slides for personnel training on good, general cybersecurity "hygiene."