# The MSP+ Cybersecurity Framework Overview

v2020.O-1.2

WISE RISE TOGETHER TOGETHER

ITNATION SECURE
cybersecurity by ConnectWise

## Legal Disclaimer

Please note that these playbooks are provided only as examples and are for reference purposes only. In many instances, your existing procedures may suffice. Prior to implementing or adopting these sample playbooks, ConnectWise strongly encourages any organization to consult with its legal counsel, accounting, financial and/or human resource professionals. By doing so, this will assist your organization in developing policies and procedures that reflect its organizational philosophy and that are appropriate to their specific circumstances and that are consistent with applicable federal, state, and local laws.

These are provided as a free resource and are provided “as is” without warranty of any kind and ConnectWise makes no legal representation concerning the adequacy of these playbooks or its compliance with federal, state, or local laws.

Never use sample policies and procedures that you find online as-is, as any policy you adopt needs to reflect the actual practices in your company. They must also be in compliance with all applicable laws and regulations, and there can be significant differences in state and local compliance requirements. You should always consult with a licensed attorney with experience specific to employment law prior to finalizing policies and procedures, whether they are individual documents or combined to form an employee handbook or procedures manual.

## Table of Contents

## Foreword

The service provider space is still a relatively new industry, and managed services as we know it today is barely twenty years old. When comparing that to the Industrial Revolution, which some would date back to the late 1700s which was followed by the age of science and mass production in the early 1900s, one can clearly understand that we are still learning and improving to meet the needs of business. And for some, cybersecurity has become the latest necessity within our digital age for protecting business, intellectual property, personally identifiable information, and so much more. For others, the need to secure data has been a lifetime of learning and achievement as technology has advanced.

Today, service providers are often called managed service providers (MSPs) or technology service providers (TSPs). They are at the front lines in defending themselves and their clients. They face challenges from threat actors working around the clock and anywhere in the world that have one objective, to get paid for denying the availability, integrity, or confidentiality of data that your clients depend on for their business survival. In many cases, these clients that believe their MSP provides cybersecurity as part of their service, and they don't have a clear understanding of the risk that exists. The overarching problem is that cybersecurity is the first major issue in technology that has a shared responsibility between the provider and the client.

While the client may assume the MSP owns the risk, we have an obligation to ourselves and our industry to discuss risk ownership with our clients and prospects. That's where the conversation began. We understood the challenge that our partners faced with discussing and managing risk while trying to align with a variety of standards that weren't designed for service providers or small and medium-sized businesses. On top of that, many service providers have proven to be outstanding at delivering IT services, but cybersecurity hasn't been their specialty. Simply adding cybersecurity talent to the team or sending someone to get certified isn't enough. It's compounded by the lack of experienced and certified talent available in the market today.

Today, a reasonable program starts with changes at the top by driving cybersecurity education and culture into an organization. It accelerates to include alignment of policies, procedures, tools, pricing models, talk tracks, support mechanisms, operational efficiencies, and incident response. Once you start to have that figured out in your security journey, you need to build a business plan to deliver those services to your clients and do so without a negative impact on existing teams and systems. And don't let me forget, you need to understand and meet the governance and compliance requirements that your clients are expected to maintain. In reality, for some of you, this would require a complete restructuring of your business, or creation of a new business just around cybersecurity.  We knew there had to be a better way to help our industry.

In this playbook and leveraging the new MSP+ Cybersecurity Framework (MSP+), we have taken the guesswork out of planning, education, and roadmap for service providers. The MSP+ Cybersecurity Framework aligns with the best available security best practices and meets most local and international guidelines for securing a small or medium-sized business, including your own. Much like the Payment Card Industry Data Security Standard (PCI-DSS), we see it as a way to provide guidance for service providers and a reasonable level of assurance to your clients that you can deliver cybersecurity solutions based on best practices.

This playbook, the Fundamental, Advanced, and Master books that follow are your guide to building and delivering cybersecurity solutions with confidence. In this book, you will find an overview of the MSP+ Cybersecurity Framework and a description of what a security program should look like for your business. In the remaining books, you will learn how to implement and deploy security using trusted methodologies that are supported around the world.

Each book builds on the previous to provide a maturity path for you and your team to develop the necessary skills and understanding of a 'security first' practice. As you continue through your journey, we have also created an assessment process to measure against, self-certify when you are ready, and, when appropriate, reach the highest standards of practice in our industry by achieving the SECURE MSP accreditation. The SECURE MSP process includes audited 3rd party verification that you have the necessary business practices in place to deliver cybersecurity solutions based on well-known standards and guidelines. Reaching SECURE MSP status will be a noteworthy accomplishment, one that very few will reach.

Please take your time to read and understand the books. Our team will join you on the journey and provide the education, labs, and implementation guidance required to reach your goals of protecting your business, removing risk for your clients, and generating new revenue with cybersecurity leading the charge.

I would like to take this opportunity to personally thank the entire team of authors and architects for their hard work and dedication in making this framework a reality for our IT Nation Partners; Joy Beland, David Bork, Frank DePrisco, Bryan Lowe, Drew Sanford, and Wayne Selk.

Securely,

Jay Ryerse, CISSP
ConnectWise
Vice President, Cybersecurity Initiatives

# Introduction

Welcome to the IT Nation Secure MSP+ Cybersecurity Framework Playbook.  Inside, you will find several security best practices to establish, improve, or enhance security controls you may or may not have implemented to date.  This playbook is available to all IT Nation partners.

If you have received this book and are not a current IT Nation partner, please visit https://www.connectwise.com/theitnation/join. It is free.

Joining the IT Nation will ensure you have access to the most up to date playbook as we make changes due to changes in best practices as a result of the evolving threat landscape.

The rest of the introduction below will answer some of the commonly asked questions around this new security framework. Should you choose to become certified, a list of the benefits is included.  The team at IT Nation have created this framework to make it easy to assess and help you, the MSP, figure out the best security for your organization.  We hope you will find this information informative and useful throughout your security journey, wherever that may lead.

## What is the IT Nation Secure MSP+ Cybersecurity Framework?

The IT Nation Secure MSP+ Cybersecurity Framework provides the outline for a certification program for the MSP community. Based upon best practices and providing a journey of growth from baseline security elements to that of a repeatable and adaptive program, the MSP+ Cybersecurity Framework is designed as a resource to assess and enhance the cybersecurity posture and services provided by MSPs to their clients. The MSP+ Cybersecurity Framework is designed to serve as a verification and validation process to ensure that suitable levels of cybersecurity procedures and processes are in place along with the relevant cyber-hygiene to protect their own systems, services and data, as well as that of their clients.

## How does this fit with our Security Journey?

The IT Nation Secure MSP+ Cybersecurity Framework provides a roadmap for the security journey an organization needs to undertake to build an active, long-term, sustainable culture around cybersecurity. The MSP+ Cybersecurity Framework phased approach outlines and guides the growth of a cybersecurity program across the business and services of an MSP organization.

## How do I apply this framework?

The IT Nation Secure MSP+ Cybersecurity Framework outlines the progress for cybersecurity maturity and growth. Many MSP organizations know that there are things they need to do to improve their security posture and program. However, there are MSPs who do not necessarily know how to make those improvements or where to begin. The MSP+ Cybersecurity Framework grew out of the need to provide easy to follow assistance in identifying and managing cyber risk for the MSP to mature its business and services.

## Why the different colors?

The color-coded guides from IT Nation Secure are inspired by the publication of the U.S. Government's "Rainbow Series" of books for evaluating "Trusted Computer Systems," where each book was a different color. If stacked together, the Rainbow Series of books would be six feet tall. Much like the Rainbow Series, IT Nation felt that having a color code would aid the MSP community with the adoption of the MSP+ Cybersecurity Framework. Fortunately, with digital technology, the MSP+ Cybersecurity Framework will not harm too many trees with its publication. Following is a breakdown of the colorized playbooks for the MSP+ Cybersecurity Framework:

- Fundamentals (Yellow) Book provides the baseline of Secure MSP cybersecurity concepts for the foundation upon which to construct a mature and adaptive program across an MSP business and services offered to clients. The Yellow Book presents the essential cybersecurity guidance to MSPs on how to implement a secure IT infrastructure to help reduce risk and vulnerabilities within the services provided to their clients.
- Advanced (Green) Book offers informed guidance for expanding into the next elements of the MSP+ Cybersecurity Framework. The Green Book focuses on the security journey for overall improvement and how to get better at monitoring and managing risk across the MSP operations and services. By taking this next step in the MSP+ Cybersecurity Framework, an MSP can better understand the effectiveness of their existing cybersecurity risk management efforts and work to identify any improvement opportunities within the context of their whole organization. MSP+ Certification may be accomplished through a cybersecurity self-assessment against the MSP+ Cybersecurity Framework.
- Master (Blue) Book outlines the plan for Secure MSP Accreditation to attain the next maturity level of the security journey of the MSP organization. The Blue Book also offers relevant guidance to develop a formal system of metrics and measurement when defining a risk and security program across the MSP organization. The Blue Book defines the requirements for Secure MSP Accreditation that involves an assessment by an independent third-party (IT Nation) as a due diligence activity to validate a level of assurance with the overall security of the MSP operations and services.

## How do I know if I am on the most current version of the books?

We have a very unique versioning naming convention in place to ensure you are on the latest version of the Books.  Our version schema is as follows:  v<YYYY>.<B>-<V>.<U>

Where <YYYY> is the year of publication; in this case 2020.  <B> is the book, D – Framework Disciplines, O – Overview, F – Book 1: Fundamentals, A – Book 2: Advanced, M – Book 3: Master. <V> is the major version. <U> is the update for the major version.

If you have a 2020.O-1.1 – then that is the initial public release of the Overview document.  The ITN Secure team will be updated these books throughout the remainder of this year.  New publications will have a statement of superseded as well as a new version number. The information may still be relevant in the older publications; however the newer documents will be used for the certifications.

## What does it mean to be "Secure MSP Certified" by IT Nation?

There are two types of certifications MSPs can achieve through the Secure MSP program. The first is to self-attest all the requirements and objectives that have been completed and receive an **MSP+ Certification**. This means the MSP can simply take an assessment and sign-off that the organization has attained all the requirements and objectives set forth by the Secure MSP governing body, IT Nation Secure. This is covered within the **Advanced Book**. After completing all these objectives, your organization will have implemented all the necessary security controls, policies, and processes to best protect your organization and your SMB clients from a cybersecurity incident.

The second certification is the **Secure MSP Accredited Partner.** This certification builds upon the Advanced Book by adding a few additional controls and producing evidence to support your self-attestation. The self-assessment and evidence will be reviewed by the governing body, IT Nation Secure staff, to ensure all items meet the standard outlined in the **Master Book**. Once accepted, you will be granted access to the elite membership logo to use and promote your business.

Mirrored after the Cyber Essentials certification, the following outlines the path to certification for both MSP+ and Secure MSP:

1. Decide which level you want to attain: MSP+ Certification or Secure MSP Accreditation.
2. Review the requirements for the certification and if for Secure MSP, collect the evidence.
3. Ensure all the security controls outlined in the requirements for the certification have been implemented.
4. Submit your self-assessment questionnaire or update it if for Secure MSP.
5. If achieving a Secure MSP Accreditation, upload all the required evidence for review.
6. Review and resolve any discrepancies outlined.
7. Resubmit the evidence for the discrepancies noted, if any.
8. Final review and certification issuance, assuming a positive outcome of the review.

We look forward to taking you on this journey. The remaining document provides a brief overview for you to better understand the requirements for the security foundation and the MSP+ and Secure MSP certifications. The IT Nation Secure team is with you.

# MSP+ Cybersecurity Framework Overview

This Disciplines Playbook is designed to provide the reader with an understanding through definition regarding each specific section and chapter for the three levels: Fundamentals, Advanced, and Master.  These three levels each build upon the other. The chapters feature specific topics for MSPs to implement within their environment. The definitions below should encourage the reader to pick up, read, and implement the security controls outlined in each of the books, if they so choose.  Some of the guidance and direction may not fit the organization's current needs, and that is okay. If circumstances change, then the guidance is there.

In addition, it may take a few years to get the organization to a comfortable level. This is due to many factors like budget, personnel, and business risk objectives. The business should prioritize the items in an order that makes the most sense for the company. A great security program involves a risk-based approach; therefore, governance is a must-have for every organization. Governance is the foundation that drives the rest of the security platform within your business, from the executives at the top to the newest employee in the company. We at IT Nation strongly believe that your Governance Program is the most critical piece of your security, so we started there first.

## MSP+ Cybersecurity Framework Requirements Tables

You will notice a table at the end of each of the specific topics.  This table outlines at a glance the requirements for achieving each of the levels within the MSP+ Cybersecurity Framework.  To help better understand the notations in each column review the following list for what each letter indicates:

- I – informal or partial
- O – optional
- X – full, completed requirement
- <BLANK> - not required

Using the Privacy Program table as an example, the first line shows "Privacy Officer" with a <BLANK> in Fundamentals, a <BLANK> in Advanced, and an "O" in the Master column.  This means there is no requirement for a Privacy Officer in either the Fundamentals or Advanced.  If you are working toward a certification or accreditation, a Privacy Officer is not required for MSP+ Certification and only a nice to have for Secure MSP Accreditation.

| MSP Level | Fundamentals | Advanced | Master |
|---|---|---|---|
| Privacy Officer | | | O |

# Governance Program

This program sets the stage for everything your business buys, implements, and sells around cybersecurity.  It is the glue that keeps your data safe, lays the foundation for your security culture, and provides the daily security direction for the employees. There are several pieces to this program. Each is vitally important to establishing, maintaining, and enhancing the overall security posture of the organization. This is also the program that establishes the effectiveness of your security controls, realize the gaps, and identify when those controls are succeeding or failing.

Information Security Governance requires assigning roles and responsibilities, creating organizational structure, and defining measurements. These are all developed strategically and with the guidance of the board of directors and/or executive leadership.

Information Security Governance is often confused with IT Management, but these are not the same. IT Management is primarily concerned with making tactical decisions to mitigate and prevent security risks. Governance is a focus on the strategic, not the tactical. It is not the implementation of the policy; it is the oversight and creation of the program.

As part of your Governance Program, Information Security Policies will help establish the program and security within your organization.

Creating effective information security policies (ISPs) and ensuring compliance is a critical step in preventing security incidents. Policies are important for new and established organizations because they provide clear guidance and direction on how businesses, employees, contractors, and third parties conduct themselves while using information systems.

## Privacy Program

Privacy is becoming a crucial area of focus for organizations of all sizes, and privacy topics are in the news constantly. It is critical to know your organization's business, people, and data before you can build your privacy program. You must lay the foundation, merge any existing and new pieces into one program, and lead the way on all things privacy. Where do you start? What are the priorities? How do you introduce privacy concepts? You need a plan.

**Privacy Program: Business, People, and Data**
Before building the privacy program, take time to get to know the business by becoming familiar with the products or services you offer. Understand who your customers are. Then, looking to privacy, determine what the senior leaders see as most important. Additionally, ask if there are any current policies or practices in place.  If so, you have something to build on, but if not, now is the time to get started.

Next, get to know the people.  Your colleagues will be vital in helping you understand what kind of data the organization collects, processes, and stores.  Find out what privacy issues your coworkers have confronted in their roles.

Finally, to help build your privacy program you need to understand what data your company has, where it comes from, and how it flows through the company.  Every organization has a variety of categories of data, and they are often used for different purposes.  This is probably the most complicated piece of learning about the company and involves most, if not all, of the company's divisions. Do not expect to figure it all out right away. Getting started with a rough sketch of what kinds of data you have, why you have the data, and where the data is stored is a good start to understanding the nuts and bolts of your job.

Now it is time to start building the privacy program. Pulling existing privacy concepts together or building the privacy foundation anew not only establishes your program, but also helps your colleagues get a cohesive picture of privacy and its importance to the organization. There are seven key initiatives that you should include.

**Seven Key Initiatives for Building a Privacy Program:**

**Initiative #1: An internal privacy policy**
**Initiative #2: A protocol for data retention**
**Initiative #3: Employee training**
**Initiative #4: An external privacy policy**
**Initiative #5: A breach response plan**
**Initiative #6: Privacy by design**
**Initiative #7: GDPR assessment**

**Keep Building on your Privacy Program**
As you make progress on these seven key initiatives, you will be on your way to a robust privacy program. As you continue to build and improve your program, there may be challenges, but there are numerous privacy resources to keep you current and help you tackle privacy issues. Being a part of the community of privacy professionals is a valuable resource and can help you navigate your way to the privacy program you hope to build at your organization. Enjoy your progress and do not forget to stay aligned with senior leadership on your need to keep an ongoing role in all parts of the organization. It is the secret to continued success.

| MSP Level | Fundamentals | Advanced | Master |
|---|---|---|---|
| Privacy Officer | | | O |
| External Privacy Policy | | I | X |
| Internal Privacy Policy | I | X | X |
| Employee Training | X | X | X |
| Privacy by Design | | | X |
| Breach Response Plan | | I | X |
| Protocol for Data Retention | I | X | X |
| Privacy Assessments | | I | X |

## Security Program

The security program is made up of several other programs, some of which overlap with other sections in this document. The main topic for this section is to define how your security program interacts and intersects with these programs along with the impact to the organization. This will become your largest program to implement within the organization, since it encompasses all of your security components.

| MSP Level | Fundamentals | Advanced | Master |
|---|---|---|---|
| Awareness Training | X | X | X |
| Executive Support |  | I | O |
| Security Culture |  | I | X |
| Identity and Access Mgmt (IAM) |  | O | X |
| Physical Security | X | X | X |
| System Hardening | I | I | X |
| Perimeter Security | I | X | X |
| Endpoint Protection | X | X | X |
| Endpoint Detection & Resp (EDR) |  | O | X |
| Managed Detection & Resp (MDR) |  | O | X |
| Risk Management Program |  | I | X |
| System Auditing | I | X | X |
| 3-2-1 Backup Solution | I | X | X |
| Security Plan |  | X | X |
| Secure Network Design | I | X | X |

## Measurement Program

This area will focus on how to facilitate decision making and improve performance and accountability through the collection, analysis, and reporting of relevant performance-related data.  The purpose of measuring performance is to monitor the status of measured activities and facilitate improvement in those activities by applying corrective actions based on observed measurements.  This section will use information and guidance found in NIST SP 800-55rev1.

| MSP Level | Fundamentals | Advanced | Master |
|---|---|---|---|
| Measure Capabilities | I | X | X |
| Identify Gaps | X | X | X |
| Data-driven Metrics | I | X | X |
| Optimization of Security |  | O | X |
| Established Efficiency |  |  | X |

## Security Lifecycle/Review

This playbook will focus on the lifecycle of your information security. The reference materials for this playbook are from NIST SP 800-35 and SP 800-64.

Organizations are constantly evaluating and selecting a variety of information security services, both people and technology, to maintain and improve their security program and architecture. These services range from policy development to data loss prevention (DLP) solutions.

Factors to be considered when implementing information security services include service provider qualifications, operational requirements, the type of service, and the ability to deliver adequate protection to the organization.

| MSP Level | Fundamentals | Advanced | Master |
|---|---|---|---|
| SLM Profiles | X | X | X |
| Managing Risk | O | I | X |
| Well Trained Workforce | | I | X |
| Security/Business Dependencies | | I | X |
| Risk-based Management Decisions | | O | X |

# Risk Management Program

Risk management is the process of implementing and maintaining countermeasures that reduce the effects of risk to an acceptable level. The risk analysis process gives management the information it needs to make educated judgments concerning your company's information security program. The process identifies the existing security controls, calculates vulnerabilities, and evaluates the effect of threats on each area of vulnerability, along with the possibility that the threat will occur.

In most cases, the risk analysis process attempts to strike an economic balance between the impact of risks and the cost of security solutions intended to manage them. At the basis of selecting cost-effective protective measures is the assumption that the cost of controlling any risk should not exceed the maximum loss associated with the risk (e.g. if the potential loss attributable to a risk is estimated to be $500,000, the cost of the protective measures intended to prevent that loss should not exceed that amount). In other cases, the decision to implement or not implement countermeasures may be driven by the importance of the system or its data or by mandates as opposed to its cost.

## Risk Analysis Terminology

**Asset** - Anything with value and in need of protection.

**Threat** - An action or potential action with the propensity to cause damage.

**Vulnerability** - A condition of weakness. *If there were no vulnerabilities, there would be no concern for threat activity.*

**Countermeasure** - Any device or action with the ability to reduce vulnerability.

**Expected Loss** - The anticipated negative impact to assets due to threat manifestation.

**Impact** - Losses as a result of threat activity are normally expressed in one or more impact areas. Four areas are commonly used: Destruction, Denial of Service, Disclosure, and Modification.

## Vulnerability Management & Assessment Program

This section outlines the vulnerability management program and provides guidance and direction for assessing the impact of the identified vulnerabilities within your organization. This section assists in identifying the gaps within your organization, highlighting where you are most vulnerable.

| MSP Level | Fundamentals | Advanced | Master |
|---|---|---|---|
| Vulnerability Mgmt Program | I | X | X |
| Threat Intelligence |  | I | X |
| Defined Metrics | I | I | X |
| System Scans | I | I | X |
| Application Scans |  | O | X |

## Patch Management Program

Most organizations have a patch management program with varying scale.  This section is aimed at providing a standardized overview as well as best practices for implementing a patch management program to meet or exceed the objectives for your organization.

| MSP Level | Fundamentals | Advanced | Master |
|---|---|---|---|
| Patch Mgmt Plan | I | X | X |
| Configuration Mgmt | I | I | X |
| Change Mgmt |  | I | X |
| Patch Testing Plan |  | I | I |

## Business Continuity & Recovery Planning

Most MSPs understand the need for disaster recovery.  This section accounts for the important activity of keeping the business running while recovering from a disaster with proper planning.

| MSP Level | Fundamentals | Advanced | Master |
|---|---|---|---|
| Disaster Recovery Plan | I | I | X |
| Business Continuity Plan | I | I | X |
| Business Impact Analysis |  | O | X |
| Roles and Responsibilities | I | X | X |
| Measure Testing & Training |  | X | X |
| Tested Backup and Restore |  | X | X |

## Third-Party & Vendor Risk Program

There are times when a business may lose sight of the risk introduced by failing to understand the security impact third-party and vendor partners bring into the organization. This playbook will show the value in having a vendor risk program and provide guidance and direction for establishing, managing, and maintaining this program within your organization.

| MSP Level | Fundamentals | Advanced | Master |
|---|---|---|---|

| | | | |
|---|---|---|---|
| Vendor Contract Mgmt | I | X | X |
| Vendor Risk Assessments | | X | X |

# Incident Management Program

Is your MSP organization prepared to respond to a data breach or a cyber-attack? Having a working incident management program is the best chance your organization has in defending itself from suffering any long-term damage or loss of reputation from a cyber incident. Creating an incident response program for your organization does not have to be a drawn-out, daunting process. An incident management program must start with a plan. According to the National Institute of Standards and Technology (NIST), an incident response plan simply provides "the instructions and procedures an organization can use to identify, respond to, and mitigate the effects of a cyber incident." (Source:  NIST SP800-34r1, Contingency Planning Guide for Federal Information Systems).

## Incident Management Terminology

- Security event, Security incident -  Often used interchangeably, a security event is a change in the everyday operations of a network or information technology service, indicating that a security policy may have been violated or a security safeguard may have failed.

- Security breach - Any incident that results in unauthorized access of data, applications, services, networks and/or devices by bypassing their underlying security mechanisms. A security breach occurs when an individual or an application illegitimately enters a private, confidential, or unauthorized logical IT perimeter. A security breach is also known as a security violation.

- Data breach - a security incident in which sensitive, protected, or confidential data is copied, transmitted, viewed, stolen, or used by an individual unauthorized to do so. Data breaches may involve financial information such as credit card or bank details, personal health information (PHI), Personally identifiable information (PII), trade secrets of corporations or intellectual property.

When properly implemented across an MSP organization, an incident management program will help reduce the time and expense associated with an incident. With the primary focus on the protection of data and critical assets, an incident management program response process will include many different activities, such as:

- Performing secure backups of data and critical systems
- Leveraging system logs and security alerts to detect malicious activity
- Maintaining identity and access management standards to avoid compromise
- Devoting attention to patch management

Every MSP organization must have proper processes and procedures in place in order to reduce the risk of cyber threats. An incident management program will include the planning and processes of business functions and activities, identify, and establish workforce personnel roles, and include written and shared documentation in order to be used to mitigate cybersecurity risks across the organization. Your incident management program must have clearly outlined, actionable steps a response team can quickly follow when an incident occurs. However, your response plans also need to be flexible to support a wide range of incidents. If a rigid, complex process must be followed, any unplanned scenarios may result in the response team unable to properly deal with the new problem.

Additionally, frequent updates to your incident response program and plans help your flexibility to adapt, address, and manage new threats. If your organization formally reviews their incident response plans every six months, then the stakeholders and response teams will be better prepared to adapt to emerging cybersecurity issues and attacks that may target your organization and your clients. Having a strategy and processes in place with a proper method to assess risk and threats to the organization, will serve as the driver for the adoption of new technology and services to deal with those threats that may harm your business or your customers.

## Executive / Board / Owner Oversight

Poor communications, lack of leadership, and lack of board oversight are often the primary hinderance when building an effective incident management program. Successfully raising executive, board, owner, and leadership awareness on the critical importance of adopting and championing an incident management program. Response planning should elevate the importance across your entire MSP organization. Having the top-level involved and supporting senior management will allow you to recruit the most qualified candidates and workforce personnel for your security and response teams and foster the creation of processes and information channels that will help you manage an incident effectively. The security culture of your MSP organization will be driven from the attitudes, examples, and tone provided at the top and cascading throughout the rest of your department leaders and individual team members.

| MSP Level | Fundamentals | Advanced | Master |
|---|---|---|---|
| Partially Aware of IR needs | X | | |
| Realized need for IR | | X | |
| Promoted IR Plan | | | X |

## Roles & Responsibilities

Know the key stakeholders and what key roles within the MSP organization who should care and be involved in a security incident. The responsible stakeholders and roles may change depending on the type of incident and the targeted resources of the organization. Stakeholders likely include department managers, senior management, partners, customers, and legal. With the involvement of diverse responsibilities, roles, and individual personalities, there addition of business politics, resistance, negotiation, and ignorance may blend into the overall response activities. A fully functioning security incident management program should involve the following roles:

- **Legal Counsel** to provide oversight and legally sound guidance on activities to perform or avoid as well as produce any legal briefs and proceedings.
- **Executive Management** for the highest-level decision-making from the executive, board, and owner.
- **Program or Project Management** to provide oversight and application of knowledge of data, information, processes, organizational structure, workforce skills, and analytical expertise, as well as systems, networks, and data flows to manage the incident response lifecycle.
- **IT and Security** teams for technical knowledge, experience, guidance, and execution of the initial incident response and containment actions.
- **Compliance** to assist with incident oversight and follow up activities, as well as any breach notification or incident reporting that may be required to regulation entities.
- **Business Operations** for business direction and communications across business units, departments, and teams
- **Human Resources** for enabling internal communications and assisting with workforce personnel security policies that may have been violated during the incident.
- **Public Relations** (internal role or external firm) with expertise and experience in dealing with cybersecurity incidents and with preparing messaging for both internal and external communications.
- **Outside Consultants** with specialized skills and expertise who can provide support for digital forensics, incident response, and security testing.
- **Vendors** such as internet service providers (ISPs), cloud service providers, hosting providers, software as a service (SaaS) providers, and managed security service providers (MSSPs).
- **Business Partners and Stakeholders** that depend and rely upon your services or have integrated technical ties to your service data or IT environment.

| MSP Level | Fundamentals | Advanced | Master |
|---|---|---|---|
| Ad Hoc Workforce Assignments | X | | |
| Identified Personnel | | X | X |

## Team Training for Incident Response

An incident response plan is not worth much if it's only on paper. It must be put to the test. Conducting a planned (or unplanned) security exercise, running through the plan, and identifying weak spots will go a long way to validating that your incident response team is ready and able to handle a real incident. Creating and managing an incident response plan for your MSP organization involves regular program updates and workforce personnel training. Based upon the Payment Card Industry (PCI-DSS), at a minimum your organization should take the following steps for training workforce personnel responsible for incident response:

- Test your incident response plans at least once every year.
- Assign certain workforce personnel to be available 24/7 in order to work with "off-hours" incidents.
- Appropriately and frequently train your staff responsible for handling incident response activities.
- Set up alerts from intrusion-detection systems (IDS), intrusion-prevention systems (IPS), and file-integrity monitoring systems.
- Implement an internal review process to update and manage your incident response plan to address any recent industry or organizational changes.

Training your workforce personnel in both the tools and business processes they need will help your IT professionals and staff identify, diagnose, and respond to a cybersecurity incident. In addition to training your team on any existing technology solutions you may have in your organization for logging, monitoring, and alerting, there are many vendors that offer specialized training programs and courses in the art of threat hunting and digital forensics. These courses allow your team to better learn how to analyze, protect, and defend both your business operations and those of your customers.

| MSP Level | Fundamentals | Advanced | Master |
|---|---|---|---|
| Limited Training | X | X | |
| Limited Preparation | | X | |
| Formal Training and Prep | | | X |

## Communications Plan

The plan should make it clear who the incident team should communicate with, via which communication channels, and what information should be conveyed. This is a critical and sometimes overlooked part of the response process. For example, there should be clear guidelines on what level of detail should be communicated to IT management, to senior management, to affected departments, to affected customers, and to the press.

| MSP Level | Fundamentals | Advanced | Master |
|---|---|---|---|
| Communication Plan | | X | X |

## Incident Response Lifecycle

No plan survives contact with the enemy. However, having a flexible incident response program with documented and well-practiced plans should allow your MSP organization to address most any suspected cyber incident throughout a logical series of phases. Within each phase, there are specific areas of need that should be considered.

The incident response lifecycle can be broken down into the following phases:

- **Preparation**
  Preparing is one of the most essential incident response activities that an MSP organization must undertake. You need to be prepared to respond to the worst thing that can happen to your business. Preparation is the key to the survival of your business and involves investing work into identifying the start of an incident, how to recover, how to get everything back to normal, and how to create and established security policies. Additionally, part of your preparation is properly training your workforce personnel and incident response teams in the IT systems, technology, tools, investigative techniques, business processes, and procedures required for their role and responsibilities.

- **Identification**
  The next stage of incident response is identifying the actual incident and determining whether your systems or data has been breached. In order to stop an incident, you first need to detect and identify any irregular indicators of activity within your environment and analyze and determine the exact nature and scope of the incident. The alerting, identification, and analysis process can be considerably faster if you have security monitoring deployed and filtering logs and events into a central location, such as a Security Information and Event Management (SIEM) solution or Endpoint Detection and Response (EDR) solution.

- **Containment**
  The activities you take to encompass any number of concurrent actions after the initial investigation of the incident. Your response should include steps to immediately stop any minimize identified damage, exploitation, or breach in order to limit any possible spread to other networks and hosts within your MSP environment and to those of your customers. Collecting and preserving evidence, blocking firewall ports, logging access, isolating, and patching systems may play a large part of your containment phase. It is also good practice to perform further analysis on the cybersecurity incident while you also continue monitoring for the effectiveness of your containment measures.

- **Eradication**
  Once an incident has been contained, further eradication efforts are often required in order to completely remove the underlying components of the incident and to mitigate

any identified vulnerabilities exposed during the incident. If the incident resulted in an attacker gaining access and entry from one system and then spreading into other systems across your connected MSP infrastructure, the you will have more actions to take. Both containment and eradication efforts must be applied with speed and accuracy as to not allow an attacker to regain access to disrupt your activities and maintain their presence within your networked systems. As with containment, part of eradication involves a sufficient time of monitoring to ensure the security and integrity of your networked systems and the successful implementation of your eradication efforts.

- **Recovery**
  The process your MSP organization must take in order to restore and return any compromised hosts, applications, or networks back to normal operations. As part of the recovery planning efforts, your MSP organization will need to have an appropriate recovery plan that detail the actions needed to rebuild infected systems, replace compromised files, reset passwords, patch systems, and secure network perimeters. It is a best practice to include steps for confirmation and verification in order to validate that any vulnerabilities identified from the initial attack and compromise have been properly patched or remediated. Such validation may be conducted as part of an independent (third-party) penetration assessment, or pen test, of the removed systems.

- **Lessons Learned**
  An essential part of responding to a cybersecurity incident is to document, communicate and build upon lessons learned. This step provides the opportunity for your MSP organization's key stakeholders and workforce personnel to collaborate and learn from the overall experience to better respond to future security events and incidents. Look for areas of the experience to improve your incident response plan. No process is perfect for absolutely every possible scenario. Some scenarios cannot even be fathomed until they have occurred. The threat landscape is also ever evolving so your incident response process will naturally need the occasional update. You should also document and use any lessons learned to share any significant issues and best practice across all areas of your MSP business units and possibly with your customers as well.

| MSP Level | Fundamentals | Advanced | Master |
|---|---|---|---|
| Reactive Lifecycle Response | X | | |
| Partially Documented Aspects | | X | |
| Formal IR Lifecycle | | | X |

## Security Architecture

Your organization must work from the top down to instill the concept that security belongs to everyone and should be integrated as part of the culture. Relating to the overall IT Architecture and business strategy of an MSP organization, Security Architecture can best be defined as the planned assembly policies, standards, best practices, technology solutions, and security controls. These are intended to preserve and maintain the confidentiality, integrity, availability, accountability, and assurance of systems and data. Additionally, a well-designed security architecture not only considers security risks and mitigations but also includes the blending of people, processes, and technology.

According to the National Institute of Standards and Technology (NIST) Special Publication 800-53, *Security and Privacy Controls for Information Systems and Organizations*, an organization should undertake the design and development of a security architecture for information systems that:

- Describes the overall philosophy, requirements, and approach to be taken regarding protecting the confidentiality, integrity, and availability of organizational information.
- Describes how the information security architecture is integrated into and supports the enterprise architecture.
- Describes any information security assumptions about, and dependencies on, external services.

Additionally, an organization must perform periodic reviews of their security architecture and provide updates to mitigate any issues or to address any future business initiatives. Any changes to the overall security architecture are to be reflected as revisions within supporting documentation.

An MSP is in the business to provide access to technology and services for their clients. An MSP that understands the relationship between their own business strategy and technology will be in an ideal position to design, implement, and mature their own security architecture to better protect their internal operations and the services provided to their clients. This understanding leads into the strategy of security architecture design by way of the creation of policies, standards, and procedures, detailed technical design documents, vendor product evaluation and selection, development and testing, production implementation, support documentation and training, as well as the ongoing need to monitor, manage and measure the multiple components against the MSP business needs and vision.

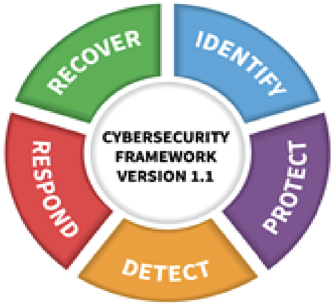
Making the selection of a point product to “bolt-on” and address a specific security need is easy. However, an MSP that has insight into their business goals, object, and vision will be able to justify and implement proper security controls linked directly to identified risks and serve to mitigate such risk. By aligning security needs with business needs, the roadmap to the creation of a robust security architecture is “built-in” to the organization.

## Reference Architectures / Case Studies

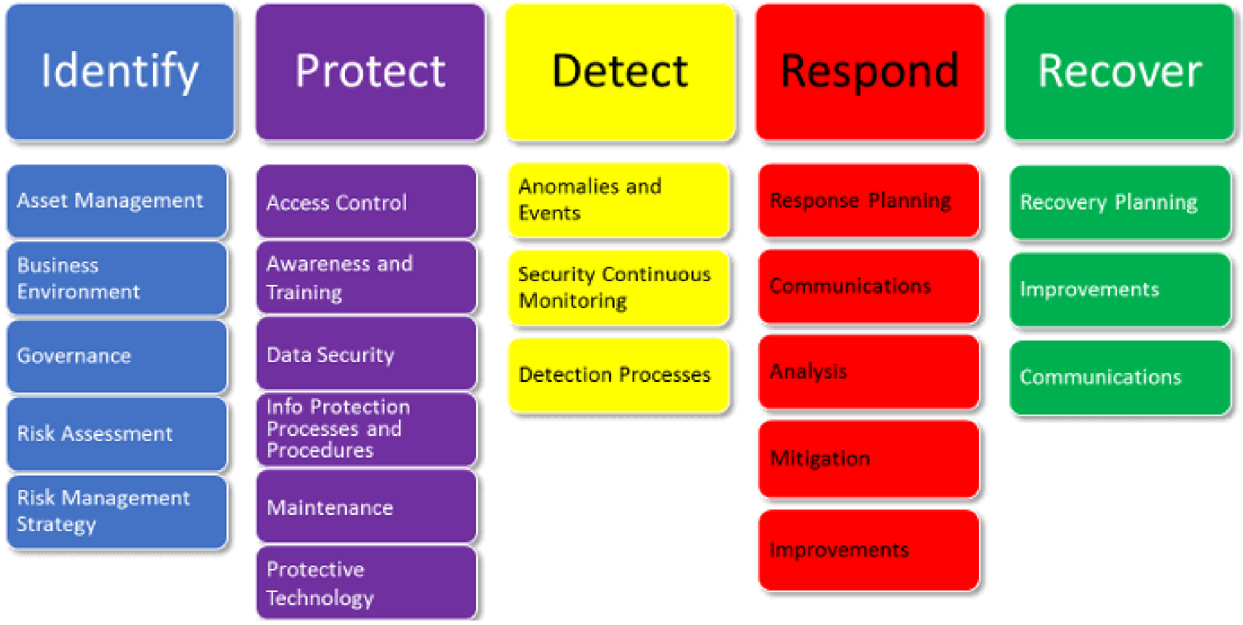
Every MSP organization has employees and workforce personnel with varying levels of security knowledge, but each MSP organization will likely have a diverse cybersecurity vision and a unique technology infrastructure to meet the needs of their business in service to their clients. An MSP that provides services to a hospital or medical provider will almost certainly have a more focused security model than an MSP that provides services to a chain of restaurants. For all MSPs, their specific security and privacy requirements revolve around ensuring that the systems and data of their clients remains protected and secure while also ensuring that their own administrators and engineers do not unintentionally put that protection and security at risk.

Historically, security architecture has been focused upon protecting network perimeters with minimal focus upon the internal applications and data. With the rise of cloud computing and a remote workforce that falls outside the traditional confines of an organizations' network boundaries, the intricacy and complexity of implementing security controls across all access points, systems, and services from any work location has grown more difficult over time. With a standards-based implementation of a Zero Trust architecture, the complexity of planning an architecture model that should improve overall cybersecurity without sacrificing the experience of the end user from any location. Zero Trust is a security architecture concept of isolation, segmentation, or compartmentalization of the different parts that make up the interconnected assembly of technology and services to limit the effects from external cyber-attacks or unintentional configuration changes. Conceptually, a Zero Trust architecture strongly rests upon a collection of components and capabilities for identity management, asset management, application authentication, network segmentation, and threat intelligence.

A standards-based approach to implementing a Zero Trust architecture should begin with a nod to the U.S. National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). The NIST CSF can serve as a reference model for many Zero Trust architecture elements that an MSP can use to better understand, manage, and reduce its cyber security risks. NIST CSF assists organizations in determining which activities are most important to assure critical operations and maintain service delivery, which, in turn, helps prioritize investments and maximize the impact of each dollar the business spends on cybersecurity. The NIST CSF framework has a common language to address cybersecurity risk management and is especially helpful in communicating both inside and outside the organization. Improving communications, awareness, and understanding between and among IT planning and operations, as well as senior executives of organizations, is crucial to establishing a vision for security architecture and planning.



# NIST Cybersecurity Framework



| Identify | Protect | Detect | Respond | Recover |
|---|---|---|---|---|
| Asset Management | Access Control | Anomalies and Events | Response Planning | Recovery Planning |
| Business Environment | Awareness and Training | Security Continuous Monitoring | Communications | Improvements |
| Governance | Data Security | Detection Processes | Analysis | Communications |
| Risk Assessment | Info Protection Processes and Procedures | | Mitigation | |
| Risk Management Strategy | Maintenance | | Improvements | |
| | Protective Technology | | | |

NIST Cybersecurity Framework (CSF)

The NIST CSF is flexible by design and can evolve to address shifting trends with cybersecurity threats, business processes, and emerging technologies. Effectively, the NIST CSF sees successful cybersecurity as an active, continuous loop of response to both threats and solutions. Additionally, the NIST CSF works great for smaller or unregulated businesses across many different industries and verticals. Since the five high-level categories of NIST CSF (Identify, Detect, Protect, Respond, & Recover) allow for easier understanding and reporting of complex topics, NIST CSF is often used as a business reporting tool to inform senior leadership of security activities.

Many of the aspects of the IT Nation Secure MSP+ Cybersecurity Framework and Zero Trust architecture models are derived from the NIST CSF and have been customized to specifically address the business and security needs of the MSP and the services they provide to their clients.  Additionally, the government of the United Kingdom (HMG) adopted a Minimum Cyber

Security Standard that was incorporated into its overall Government Functional Standard for Security for departmental security and (de facto) government contractors. The structure of the HMG Security Policy Framework (SPF), referenced by the Minimum Cyber Security Standard, is almost identical to the U.S. NIST CSF with five primary functions – Identify, Protect, Detect, Respond, and Recover. Both U.S. and HMG frameworks emphasize the importance of data protection and provisioning access to a last-privileged (zero-trust) model, as well as the drive to continuous improvement in order to be ready for the next cyber-attack. To help security with the HMG's dependency upon its supply chain, the Minimum Cyber Security Standard asserts that vendors and suppliers meet the requirements defined within the U.K. Cyber Essentials. Operated through the U.K. National Cyber Security Center (NCSC) Cyber Essentials is an assurance and controls framework program designed to protect business from the most common internet-based threats and demonstrated their commitment to cybersecurity. If a company or MSP intends to do business with the U.K. Government, and the company or MSP manages any aspect of personal and sensitive information, then that company or MSP cannot even bid on the contract without having completed Cyber Essentials certification.

Another influencer on the creation of the IT Nation Secure MSP+ Cybersecurity Framework and certification is Australia's Essential Eight. The Australian Cyber Security Centre (ACSC) compiled a list of thorough, research-based mitigation strategies that organizations can use as starting points to improve their overall cybersecurity and flexibility. While there is no single mitigation strategy that is guaranteed to prevent cybersecurity incidents, the Essential Eight identified eight essential mitigation strategies that should be implemented as a baseline where practicable thereby making it more difficult for cyber attackers to compromise systems. The Essential Eight offers guidance through a maturity model that steps through the mitigation strategies of application control, application hardening, patching applications, patching operating systems, configuring Microsoft Office, administrative controls, multi-factor authentication (MFA), and performing daily backups. The Essential Eight is focused more on the day-to-day use of most office workers and serves as suggestion of the minimal activities an organization should start doing. When compared to the NIST CSF, the Essential Eight does not really offer the more significant guidance NIST CSF provides to organizations for developing, testing, and communicating policies and procedures around network access and management, end-user education, and many other critical cybersecurity functions.

There is no such thing as a one-size-fits-all approach to security, and each framework feeds into an overall security architecture based upon the needs of your MSP business and the specific needs of your customers. The core of the security architecture needs to one of the zero trust model. The U.S. National Institute of Standards and Technology (NIST) offers the following definitions of zero trust and zero trust architecture:

> ***Zero Trust*** provides a collection of concepts and ideas designed to reduce the uncertainty in enforcing accurate, per-request access decisions in information systems and services in the face of a network viewed as compromised. ***Zero Trust Architecture*** is

an enterprise's cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies. Therefore, a ***Zero Trust Enterprise*** is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a zero-trust architecture plan.

Across the internet, there are many publications, guides, and vendors attempting to document and define the doctrines of deploying a zero-trust architecture across an organization. According to the UK National Cyber Security Centre, much of this guidance can be distilled down into the following principles:

- **Know, Understand, and Document Your Assets and Architecture**
  In order to establish the foundation and harvest the benefits from a zero trust model, each resource and component of your architecture from users and their devices must be mapped throughout the computing services and data accessed. This includes all users, devices, services, and data sources that access or traverse your network.

- **Trust No Device**
  Uniquely identify, manage, and patch devices owned by your organization in order to foster secure asset management and vibrant visibility into the services and data the devices access. When connecting to resources or services provided by your organization, devices that are discovered to be compromised, have known vulnerabilities, and not managed by your organization may be treated in a different manner than those devices owned, managed, and secured by your organization. Within a bring your own device (BYOD) model, the security confidence and trust of the personal device is much lower, such that it may only be allowed to access some resources and services, but not others.

- **Trust No Network**
  Don't trust any network between the device and the service it's accessing. This includes your local company network. Assume that you have a malicious actor or device on your internal network. Incorporate policies and a network design where communication occurs in the most secure manner available through the authentication of all connections and the encryption of all network traffic.

- **Create Accounts Linked to Individuals**
  From within a single directory or identity service, enable granular access controls and create specific roles for each user. Ensure the directory or identity service can also be utilized by all resources, services, and data - both internal and external to your organization.

- **Authenticate and Authorize Prior to Access**
  Systems and services, both internal and external to your organization, may be available for access directly over the internet, so the authentication of user requests requires a

much stronger mechanism as opposed to the use of a simple username and password combination. A zero trust model requires the use of multi-factor authentication (MFA) and continuous monitoring with possible reauthentication and reauthorization throughout user interaction, as defined and enforced by policy that attempts to attain a blended balance of security, availability, usability, and funding.

- **Define Data Access Policies**
  Control access requests to your services and data resources with policies. Resource access and action permissions policies can vary based on the sensitivity of the resource/data. A least privilege principle should be applied in order to limit both visibility and accessibility while protecting your data in transit with encryption.

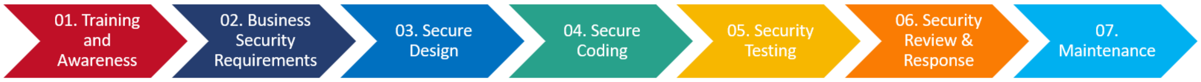
- **Monitor Devices and Services to Improve Security**
  Devices and services are more exposed to network attack. As such, an organization should not only monitor and collect device logs and network traffic data to ensure availability and performance, but also analyze the collected data to identify rogue devices and malicious activity. The collected data and analytics can serve to help you improve security policy creation and enforcement.

| MSP Level | Fundamentals | Advanced | Master |
|---|---|---|---|
| Documented Architecture | I | X | X |
| Management Awareness | I | X | X |
| Published Reference | | | X |
| Periodic Review | | | X |

## Product Security

MSP organizations utilize a myriad of in-house / on premise software and cloud-based SaaS. Additionally, there are many MSP organizations that develop and produce their own software solutions, appliances, or services. The functions of product security across your organization should be incorporated within a software development life cycle (SDLC) practice which includes the concepts of existing design control, coding standards, quality testing, and release processes. Bringing your software development life cycle (SDLC) in alignment with your adopted security policies, standards, and practices will allow your organization to produce solutions to better protect, not only your own business interests, but also the business and data security needs of your customers.

| Core Security Concepts | Gathering Security Requirements | Secure Design Principles | Secure Coding Practices | Security Testing Tools & Techniques | Final Security Review Plan | Security Patch Management |
|---|---|---|---|---|---|---|
| Assurance Methodologies | Building Checklists & Defining Security Gages | Design Level Security Controls | Code Security Analysis | Security Defect Handling | Security Review & Response Processes | Handling 3rd Party Library Upgrades |
| Standards & Frameworks | Product Security Baseline | Threat Modeling | Secure Code Review | Security Metrics Development | Supply Chain Risk Mgmt. | Disposal Policy |


01. Training and Awareness
02. Business Security Requirements
03. Secure Design
04. Secure Coding
05. Security Testing
06. Security Review & Response
07. Maintenance

- **Security Training and Awareness**
  Confirm that every person in your organization understands the security best practices and policies that your organization has adopted. Developers, engineers, and product managers will need specific training and guidance on security standards and requirements to write secure code and to implement security by design.

- **Security Requirements Review**
  In addition to the business requirements and functional needs necessary for development, it is also essential to define any security requirements during the early stages of development as part of the life cycle practice adopted by your organization. Keep in mind that security requirements will always need to be updated in response to functional changes, additional product features, updated regulatory requirements, or the evolving threat landscape.

- **Asset Catalog and Management**
  Identifying and documenting your applications and supporting assets remains a core life cycle practice and one of the first steps to securing your software and services infrastructures. As many applications rely upon support from authentication domains, databases, IT infrastructure, third-party plugins, APIs, etc. in order to properly function, an understanding of the application and its dependences remains principal to its success, operation, and future development.

- **Security Design Review**
  Software and service design reviews remain a methodical, comprehensive, and well-documented examination process of all the components that have gone into the development of a product or solution. Such reviews are regularly scheduled throughout the development process in order to validate the design against specified requirements and previous development activities. The design review also helps with identifying any problems that may impact further development or meeting requirements.

- **Manual Code Review**
  With respect to security, a manual code review is the time-consuming process of reading source code line-by-line in order to potentially identify vulnerabilities. A manual review of source code is a tedious process performed by a software developer that must be trained in the review process and has the knowledge, experience, perseverance, and endurance required to complete the task. Throughout the manual review process, any flaws or vulnerabilities discovered will need to be documented and addressed in order to improve the security posture of your application or services provided.

- **Automated Vulnerability Testing**
  There are several common off-the-shelf and open source tools that can be used to perform an analysis of the code you develop for you product and services offerings. As a baseline security practice, your organization should include the use of automated tools to perform vulnerability assessments of your code in order to discover any issues with injection, cross-site scripting, outdated libraries, broken authentication, or exposed data. Any identified vulnerabilities should be fixed or surrounded with mitigating controls.

- **Patch Management**
  Software maintenance, updates and patches are all part of a life cycle practice. Your developers and product managers will need to actively prioritize the balance between the release of new features (enhancements) with that of patching security vulnerabilities (bug fixes).

- **Integration and Deployment**
  Application and service code development has a life cycle and your code will need to be protected and controlled throughout its development and deployment. You will need a system in place to maintain version control. Such validation may be managed by documenting a provable chain of custody or utilizing code signing or hashing. Additionally, your organization may run a testing or staging environment that mirrors your production environment where code can be promoted from development into testing into production after passing the requirements for each stage.

- **Secrets Management**
  To secure your product, application, or services, Account IDs, passwords, tokens, security sensitive data, and controls need to be protected with encryption during storage and while in transit. Access to such information should be limited to only certain developers and engineers on a need to know basis. For example, your developers may not need access to the production accounts and password, but your support engineers may need to have production access for troubleshooting. Additionally, it is a good security practice to expire and rotate any keys, tokens, or passwords on a regular basis as well as logging

any changes for monitoring and auditing.

- **Third-Party Libraries**
  The use of third-party code or open-source libraries for development is a great way to save a good deal of time. However, by adding such libraries and lines of code to your own product you may introduce unforeseen vulnerabilities as there is no way to assure that the third-party entity that developed the code followed good security practices. Additionally, an organization will need to consider the licensing of third-party or open-source libraries and how they may be used within and resold as part of your own product. The use of third-party or open-source libraries should be part of your asset catalog to be monitored and managed for risks as appropriate.

- **Security and Risk Assessment**
  Prior to production launch and periodically, it is good security practice to hire a security professional to simulate the actions of a malicious hacker in order to perform an analysis of your software and systems via a penetration test (Pen Test). This type of assessment is conducted to discover potential vulnerabilities (e.g. coding errors, system configuration issues, buffer overflows, memory faults, or other environmental weaknesses) and can provide useful feedback on elements that may have been missed during development. Additionally, penetration tests and assessments are frequently conducted in conjunction with automated vulnerability testing tools and manual code reviews in order to provide a more comprehensive analysis.

- **Incident Response / Vulnerability Management**
  Everything eventually breaks. As part of your product security program, you will want to prepare an incident response plan in order to properly address new and emerging threats and vulnerabilities that are discovered over time. Your organization should create a standardized playbook with identified points of contact that outlines the protocols and procedures for responding to an incident. Once the incident is addressed, any software maintenance, updates, and patches should fall under the established patch management process in migrating a fix from development, to testing, and into production.

- **Documentation and Training**
  Documentation in the form of a User's Guide or Administrator's Guide is standard as part of a delivery package for most software products and services. Your organization may also want to publish additional whitepapers designed to highlight best practices, certain features or case studies to further expand the knowledge of the user of your offering. Training curriculum and classes may also be developed to deliver to your users. In addition to basic security awareness training, developers, engineers, and product managers will need specific security training and guidance on the backend operations

and integrations.

- **Security Champions / Stakeholder Review**
  The best way to cultivate a security culture within your organization is to have security representatives from all departments across of your organization come together as a stakeholders or champions group. Your security champions need an established channel of communications and should meet regularly to share new ideas, receive training, review projects, and report information back into their own departments. By establishing a partnership between development, engineering, and other business units, each security champion brings certain knowledge to the table as part of a feedback loop to help bridge any gaps in communication and foster a better understanding of business needs and priorities.

- **Establish Metrics**
  The success of a product security program is defined by the metrics your organization deems important to the program. It is important to establish criteria that allows developers and engineers to fully understand the risks associated with common security issues. Also, it is important to establish how to easily identify and properly correct security flaws found during development, and how to follow security and secure coding standards throughout the entire life cycle of the project.

- **Strategic Roadmap**
  Producing a roadmap of future, more mature versions, and patch releases of your product allows your organization to present and prioritize any capital, initiatives, time and resources needed. Roadmaps are a tool for the business to use in order to help ascertain their return on investment (ROI) and to help identify any additional risk the product vision may bring when aligned with other business initiatives.

| MSP Level | Fundamentals | Advanced | Master |
|---|---|---|---|
| Implemented Application Security | I | X | X |
| Secure Application Development |  | O |  |
| Secure Coding and Practiced SDLC |  |  | O |

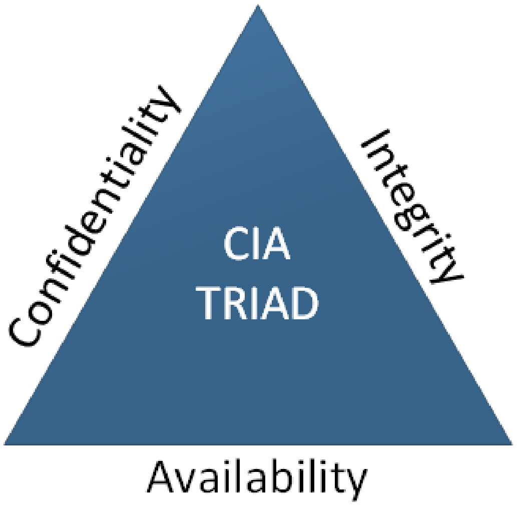
## Product Compliance

MSP organizations utilize a myriad of in-house / on premise software and cloud-based SaaS. Additionally, there are many MSP organizations that develop and produce their own software solutions, appliances, or services. Depending upon the nation, state, or industry in which the product or service is being sold or utilized, there will be several laws and regulations to which you must comply in order to operate.  In short, your product compliance program should cover and monitor your policies, legal regulations, established standards, and documented requirements that apply to your solutions.

The following are a few of the most common governmental laws, industry regulations, directives, and standards that have the most impact on cybersecurity controls surrounding data and systems:

- National Institute of Standards and Technology - Cybersecurity Framework (NIST CSF) (U.S.)
- National Institute of Standards and Technology - Security and Privacy Controls for Information Systems and Organizations (NIST SP 800-53 Rev. 5) (U.S.)
- National Institute of Standards and Technology - Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (NIST SP 800-171 Rev. 1) (U.S.)
- Office of the Superintendent of Financial Institutions (OSFI) Memorandum (Canada)
- Center for Internet Security Controls (CIS Controls)
- International Organization for Standardization - Standards for Information Security Management Systems (ISO/IEC 27001)
- International Organization for Standardization - Standards for Risk Management (ISO 31000)
- American Institute of CPAs (AICPA) - Service Organization Control (SOC) 2 Type II
- Health Insurance Portability and Accountability Act (HIPAA) / Health Information Technology for Economic and Clinical Health Act (HITECH) (U.S.)
- Federal Information Security Modernization Act of (FISMA) (U.S.)
- Security of Network Information Systems (NIS) Directive (EU)
- General Data Protection Regulation (GDPR) (EU)
- California Consumer Privacy Act (CCPA) (California, U.S.)
- Payment Card Industry Data Security Standard (PCI-DSS)

Confidentiality, integrity, and availability stand as the vital components of an effective cybersecurity program. Often cited as the 'CIA triad,' the concepts of confidentiality, integrity, and availability are the guiding principles that many organizations use in order to tailor their compliance programs.



**Confidentiality**
Confidentiality is achieved by preventing or limiting the disclosure of information to unauthorized individuals or entities. Confidentiality of data may be addressed through physical or logical access controls, user identity, access management, and the use of encryption.

**Integrity**
Integrity can be achieved by ensuring the accuracy and completeness of the data or systems that provide services. At a minimum, integrity checking monitors for the modification or deletion of files. Additionally, there are a variety of software tools and utilities available for integrity checking that compare hashed values and / or generate log entries upon the modification or deletion of files.

**Availability**
Availability is the concept that ensures the reliable access to data and services is there when it is needed. Implementing high availability systems throughout your security architecture is one way to safeguard availability of data and services. High availability systems are intended to be fault tolerant and designed to prevent disruptions from power outages, hardware failures and denial-of-service attacks.

Key components for an MSP to consider when assessing product compliance and designing a robust security architecture with a march towards compliance include:

- **Visibility** -- monitoring for change, performance, availability, auditability & logging
- **Access Control** -- policies, identities, groups, granular controls, authentication, MFA, SSO
- **Secure Configuration** -- lockdown based upon user profiles, consistent enforcement of policies and access controls, log management controls, user interface controls
- **Auditability** – tracking issues / vulnerabilities, reporting, security / risk scoring

Compliance stands as a critical chunk of any MSP cybersecurity strategy. While an MSP environment with baseline security controls and point solutions may not necessarily meet all the needs for regulatory compliance and may not keep the most persistent cyber attackers from penetrating the organization, such controls serve as a vital foundation for implementing a solid cybersecurity architecture and compliance program.

| MSP Level | Fundamentals | Advanced | Master |
|---|---|---|---|
| Compliance Settings | X | X | X |
| Identified Purchasing Channels | I | X | X |
| Procurement Processes |  | I | X |
| Audited & Measured Controls |  |  | X |

## People & Process

A healthy security architecture is built on three pillars—people, processes, and technology. Since technology and security architecture has been addressed within the above sections, the multiple roles of people and business processes throughout your MSP organization will need to be examined as well.

### People Are the Worst

Due to the complexity of the technology solutions (e.g., software, systems, services, and platforms) that modern companies routinely use to conduct their daily business, the operational risks posed by workforce personnel and human error are the greatest threat to your cybersecurity and the protected data across your organization. The risk from the people that make up your workforce personnel far surpasses your risk from malicious actors and cyber-attacks. However, having an experienced workforce knowledgeable about your business can also be an asset to your organization as the first line of defense against such malicious activities.

### People Can Be the Best

Regular security awareness training can serve as the foundation to help create a strong culture of cybersecurity across your organization. When senior management and executives commit to developing a positive culture around cybersecurity and investing in training for the roles and responsibilities of their personnel, the alignment with process and technology will blend to better protect your organization. Having a top-down approach for your cybersecurity culture may allow your organization to retain and rely upon those employees with the institutional knowledge and capability to maintain the security or your data and operations.

By employing the right people with a positive attitude, relevant experience, and necessary qualifications and then equipping them with the specific operational and cybersecurity training needed within their role to be successful, the security culture will grow and flourish across your organization. To support the organization, specific security roles, and responsibilities will need to be defined in order to limit access based upon the principles of least privileged in providing a person with access to systems and data only if it necessary to perform the role of their job. In your MSP organization, consider the following roles and the level of access each would need in order to function without raising the risk of exposing protected data in the event of a breach.

- End Users
- Contractors
- Helpdesk
- DEV Ops
- Server / Systems Operations

- Security Operations
- Network Operations
- Third-Parties

**No Plan Survives Contact with the Enemy**
Every MSP organization must have proper processes and procedures in place in order to reduce the risk of cyber threats. Processes define the business functions and activities, establish workforce personnel roles, and must exist in documentation in order to be used to mitigate cybersecurity risks across the organization. As cyber threats constantly evolve and change, process will need to be revisited and updated in order to address new threat vectors. Additionally, having a strategy and processes in place with a proper method to assess risk and threats to the organization, will serve as the driver for the adoption of new technology and services to deal with those threats that may harm your business or your customers.

It is paramount that every MSP organization should have a cyber incident response plan in place with repeatable procedures and a well-defined, orchestrated approach in handling a cybersecurity incident from discovery to recovery. The goal of the incident response plan and procedures is to quickly recover any disrupted business processes in the most efficient way possible. Efficient response processes are only viable if the MSP organization has invested the time and effort to fully examine and document their IT assets, security architecture and service dependencies. With prior emphasis on governance, policy development, adoption of standards, and implementation of technology aligned with risk tolerance and business objectives, everything blends into the critical processes designed to enhance the visibility and insight into your organization, shorten threat response times, and minimize the impact to your business and customers.

# Secure MSP Education Program

Education specific to MSP and SMB environments combined with industry recognized certifications make for a valuable, immediately applicable, and appreciable breadth of cybersecurity knowledge. Participating in cybersecurity courses designed to focus on MSP roles allows for peer learning and knowledge sharing outside of the coursework.  When possible, pair education between the Engineers and the Sales or Owners/VCIO's in complimentary programs, rather than relying on technical cybersecurity knowledge alone to fortify the MSP.

## Certify for Engineers

**Certify Cybersecurity Fundamentals for Engineers (Yellow Book)**
This full day course covers the basics of frameworks including the MSP+ Cybersecurity Framework, review of NIST 800-53 plus the NIST for Managed Services Providers overview. You'll review the CIS 20 Controls with a deep dive into the first six basic controls; a secure onboarding process; an overview of the cybersecurity technologies and solutions ecosystem and the problems they each solve for; the principles of security architecture; understanding risk and

business impact and how the technical and physical assessment process determines outcomes for the risk conversation; a basic overview of the concepts behind malware analysis and intrusion detection; and incident response planning (before, during, and after an incident).

**Similar Courses:** CompTIA Security+, (ISC)2 SSCP, Microsoft MTA Security Fundamentals

**Certify Cybersecurity Advanced for Engineers (Green Book)**
This course takes Engineers into real-world tactical and planning exercises covering the full 36-point checklist for a secure onboarding process; conducting an assessment to determine risk and business impact; deep dive into implementing the MSP+ Cybersecurity Framework; and blue team incident response.

**Similar Courses:** CEH, ISACA CSX Technical Foundations

**Certify Cybersecurity Master for Engineers (Blue Book)**
This course takes Engineers into real-world tactical and planning exercises covering identity and access management; information classification; security operations; and security architecture and engineering.

**Similar Courses:** CompTIA CySA+, CompTIA CASP+, (ISC)2 CISSP, ISACA CSX Practitioner

| MSP Level | Fundamentals | Advanced | Master |
|---|---|---|---|
| Certify for Engineers | X | X | X |

## Certify for Sales

**Certify Cybersecurity Fundamentals for Sales (Yellow Book)**
This full day course covers the basics of frameworks including MSP+ Cybersecurity Framework and a review of NIST 800-53 plus the NIST for Managed Services Providers overview; cybersecurity controls; the fundamentals of risk conversation and the security assessment process; an overview of cybersecurity technologies and solutions in the MSP ecosystem and the business outcomes of each solution; how to build a cybersecurity sales roadmap and measure outcomes; discovering the underlying pain and risks to compel an open conversation around cybersecurity; using a risk-based or product-based conversation to convey the threat landscape and determine ownership of risk; addressing the most common objections of SMBs; delivering a live customized version of security awareness training; and business outcomes that include a review of assessment tools and reporting, essential security package recommendations and how to have the budget and priority conversation.

**Similar Courses:** CompTIA Security+, Microsoft MTA Security Fundamentals

**Certify Cybersecurity Advanced for Sales (Green Book)**
This course takes Sales Professionals into real-world reconnaissance and planning exercises

covering the full sales cycle from security assessment to profile creation and gap analysis to action plan presentation inclusive of risk and business impact to project implementation and onboarding discussion and review. We'll also cover prospecting, business outcome processes, and advanced presentation techniques related to cybersecurity.

**Similar Courses:** GIAC Information Security Fundamentals, ISACA CSX Fundamentals

### Certify Cybersecurity Advanced for VCIOs (Green Book)

This two-day course takes Owners and Security Management Professionals into real-world governance strategy planning exercises including asset value determination, scenario planning, business impact analysis, budget planning, and team/resource strategy.

**Similar Courses:** GIAC Information Security Fundamentals, ISACA CSX Fundamentals

### Certify Cybersecurity Master for VCIOs (Blue Book)

This course takes Owners/Security Program Managers into real-world management and planning exercises covering governance risk and compliance, management of full assessment process and establishing and managing to metrics.

**Similar Courses:** (ISC)2 CISSP, ISACA CISM

| MSP Level | Fundamentals | Advanced | Master |
|---|---|---|---|
| Certify for Sales | X | X | X |
| Certify for vCISO | | X | X |

# Next Steps

Now that you understand the Certification Framework, the goal is to achieve a level of certification either through self-attestation or IT Nation Secure Certification.  Remember, this is a journey that begins with the Fundamentals (Yellow) book. The sections below will help you understand the benefits for achieving these certifications and what it means for your organization and clients.

## Completing the Books in Sequence

After completing the Advanced book and the requirements associated with each of the sections, your organization is eligible to self-attest and certify that you have completed a milestone in your security journey.  Our hope is that most MSPs will achieve this level of success and security.

### MSP+ Certification

As the governing body for the IT Nation Secure MSP+ Certification, we have determined the following list of requirements must be met and attested to by an organization's owner, managing partner, or other equivalent executive level individual before receiving access to the certification logo for this achievement.

### Secure MSP Accreditation

The requirements for this achievement are outlined in the Master book.  In addition to completing the required activities, your organization will still need to self-attest as per the direction above.  Once the request for ITN Secure MSP Accreditation has been received, you will be required to provide all the necessary evidence requested by the certification team via a secure upload link. All the documented evidence provided will be destroyed upon the certification board's approval or denial decision, with a letter confirming the destruction for your records.

## Acknowledgements

### Contributing Authors

- Bryan Lowe, CISSP, CISM, CRISC, CCISO
- Frank DePrisco
- David Bork, CISSP
- Wayne Selk, CISSP
- Joy Beland, Security+, CSX|F, SSAP
- Drew Sanford
- Jay Ryerse, CISSP

If you have any questions or comments for the authors, please send an email to ITNSecure_Cert@ConnectWise.com