Guide to Implementation Groups (IG)

CIS Critical Security Controls v8.1

November 2024

Center for Internet Security®

CIS Controls™

Acknowledgments

The Center for Internet Security® (CIS®) would like to thank the many security experts who volunteer their time and talent to support the CIS Critical Security Controls (CIS Controls) and other CIS work. CIS products represent the effort of a veritable army of volunteers from across the industry, generously giving their time and talent in the name of a more secure online experience for everyone.

As a nonprofit organization driven by its volunteers, we are always in the process of looking for new topics and assistance in creating cybersecurity guidance. If you are interested in volunteering and/or have questions, comments, or have identified ways to improve this guide, please write us at: controlsinfo@cisecurity.org.

All references to tools or other products in this guide are provided for informational purposes only, and do not represent the endorsement by CIS of any particular company, product, or technology.

Editor
Valecia Stocchetti, CIS

Contributors
Josh Franklin, CIS
Robin Regnier, CIS

Contents

Introduction

In a world faced with varying degrees of cyber attacks, implementing a cybersecurity framework can be a logical, but daunting, task. An enterprise needs a way to prioritize the implementation of security controls. For those using or wanting to use the CIS Critical Security Controls (CIS Controls) in their cybersecurity journeys, CIS has developed Implementation Groups (IGs) to help prioritize the implementation of the CIS Controls—divided into IG1, IG2, and IG3. IGs are based on several factors—*Size and/or Complexity*, *Data Types*, *Resources and Technology*, *Threat Types*, and *Risk*. Each IG identifies a set of Safeguards[1] that the enterprise should implement.

So where does an enterprise start? Every enterprise should begin with IG1, as it represents a minimum standard of information security that is the on-ramp to implementation of the CIS Controls. Referred to as *essential cyber hygiene,* IG1 provides effective security value with technology and processes that are generally already available, while providing a basis for more tailored and sophisticated action, if warranted. Once IG1 has been implemented, enterprises can move to Safeguards in IG2 and IG3, based on the factors mentioned above. Keep in mind that Safeguard implementation is not a one-time activity. Instead, it is an iterative approach to protecting an enterprise from cyber threats. Remember—environments change, threats change, and business objectives change.

These IGs provide a simple and accessible way to help enterprises of different classes focus their efforts on a specific set of best practices that will maximize the value (i.e., protection) when it comes to defending against cyber attacks. *This brings us to the question of which IG does an enterprise leverage?* This guide helps provide enterprises with a way to efficiently and less subjectively determine their IG.

Figure 1 | **Implementation Groups**

1 The CIS Controls are made up of 18 top-level Controls and 153 Safeguards, or actions that are taken to implement a specific Control.

Factors Impacting Implementation Groups

For adopters of the CIS Controls, one of the most important steps in building a cybersecurity program is selecting the most appropriate IG for the enterprise. Since each enterprise is unique, there is not a single approach that works for everyone. However, CIS recommends the following factors as a basis for determining your IG: *Size and/or Complexity*, *Data Types*, *Resources and Technology*, *Threat Types*, and *Risk*. Most cybersecurity decisions come down to one or more of these five factors.

Figure 2 | **Factors that impact IGs**

Size and/or Complexity

The size/and or complexity of an enterprise can vary based on many criteria. For example, the Small Business Administration (SBA) defines a small business as having fewer than 500 employees.[2] However, even then there are exceptions to that rule, based on average annual receipts and/or number of employees for a specific industry. There may also be state-specific factors in determining what constitutes a small business, such as in California.[3]

Sometimes it can be difficult to select an IG simply based on size though. Complexity can also be a variable in selecting an IG. Complexity can run concurrently with the size of an enterprise. For example, a small enterprise is simpler in terms of complexity, while larger enterprises are much more operationally complex. However, just because you are a smaller enterprise does not automatically mean that you are less complex and fall under a lower IG (e.g., IG1). For example, a doctor's office or a small hospital may only employ 50-100 people, but they are responsible for the health information of more than 1,000 patients, which would place them at a higher IG: IG2 and/or IG3. Regulations and other variables can impact the IG that an enterprise selects to implement, which will be

2 https://advocacy.sba.gov/wp-content/uploads/2023/03/Frequently-Asked-Questions-About-Small-Business-March-2023-508c.pdf

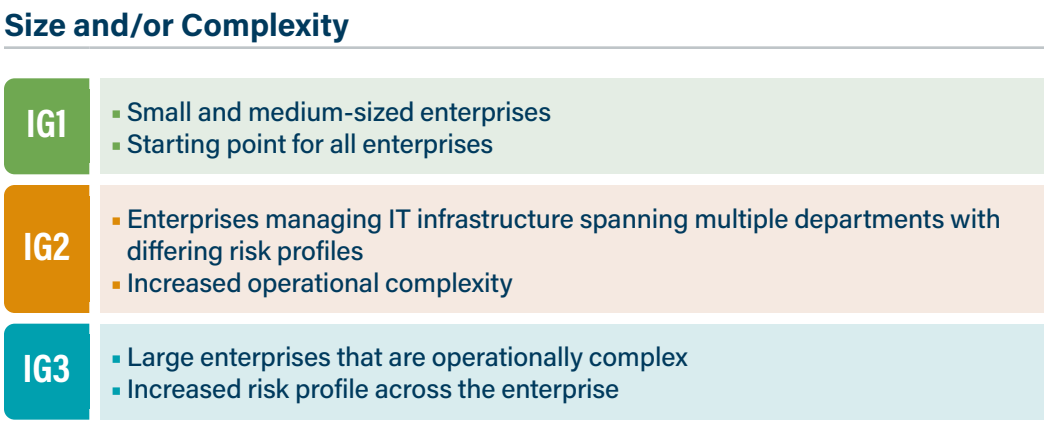
3 https://www.dgs.ca.gov/PD/Services/Page-Content/Procurement-Division-Services-List-Folder/Certify-or-Re-apply-as-Small-Business-Disabled-Veteran-Business-Enterprise

addressed more in-depth under Data Types below. Bottom line: It is the culmination of factors that can determine an IG and not any one factor. As the complexity increases, so may the corresponding Safeguards that are needed to defend against cyber attacks, and sometimes regardless of size.

In terms of the CIS Controls, IG1 is intended for small and medium-sized enterprises (SMEs). If an enterprise fits into a unique situation, as outlined above, then it may warrant IG2 and/or IG3 Safeguards to be implemented to demonstrate compliance. Regardless of which IG an enterprise selects, IG1 is the starting point for all enterprises. It is why we have classified it as a minimum standard of information security and why we refer to it as *essential cyber hygiene*. A well-built cybersecurity program must rest on a solid foundation, which IG1 addresses.

Determining when an enterprise moves to IG2 will depend on the size and complexity of the enterprise. IG2 is for enterprises managing Information Technology (IT) infrastructure that spans multiple departments with differing risk profiles and increased operational complexity. An IG3 enterprise often includes large enterprises that are operationally complex and have an increased risk profile that is widespread across the enterprise, not just in a few areas of the enterprise. Shown below in Figure 3 is a summary of the Size and/or Complexity factors that may impact IG selection.

Figure 3 | **Size and/or Complexity factors impacting IG selection**



Data Types

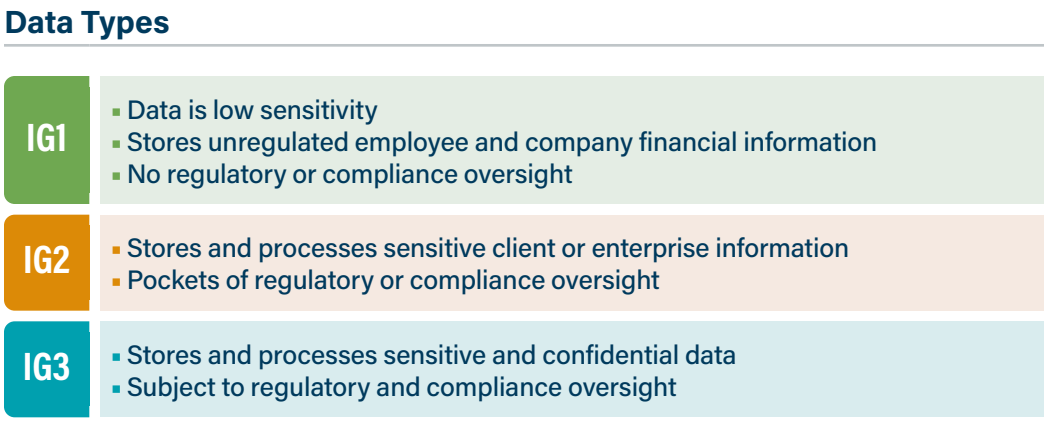
The types of data an enterprise handles and stores will also impact which IG it selects. The first step in determining which types of data an enterprise handles and stores is to take an inventory of the data and then classify it. The classification scheme will differ between enterprises. For example, an enterprise may have a classification scheme that groups data by public, internal, confidential (including sensitive and proprietary data), and restricted. However, there are many other categories that can be used to classify data, including private, critical, and regulatory data. Whichever classification scheme an enterprise chooses, ensure that it is defined and consistently

used throughout the enterprise. Once classified, data labeling can also be used to provide meaningful context about the data, as well as provide added protections around more sensitive data (e.g., business confidential data). Some enterprises will find that they already have this capability built into existing technologies, or it can be easily added (e.g., Microsoft 365®).

Some data types have special considerations due to specific laws and/or regulations that are put in place to protect and secure that data. The applicable laws and regulations that an enterprise is subject to may be determined by variables such as the sector they are classified as, the types of entities they work with (e.g., federal), or the types of data that are handled (e.g., health, credit card). For example, health insurance companies and health care providers are just some of the entities that are regulated under the Health Insurance Portability and Accountability Act (HIPAA). Another example is when an enterprise collecting data on European Union (EU) citizens and residents is subject to regulation under the General Data Protection Regulation (GDPR).

Most IG1 enterprises handle data with low sensitivity and no regulatory or compliance oversight (e.g., an enterprise that handles unregulated employee and company financial information). To understand what data is regulated, go back to the first step of inventorying data. When an enterprise moves to IG2, this is where they often begin to move into compliance and regulations. It may not be widespread, but some departments/systems/data can be regulated, require additional Safeguards to be implemented, and be subject to external audits. If not regulated, it could mean that the enterprise handles more sensitive data, which requires additional protections found in IG2. An IG3 enterprise deals with the highest regulatory burdens and is subject to external audits to ensure compliance on a recurring basis (e.g., annually). They also store and process sensitive and confidential data and, therefore, must uphold the confidentiality, integrity, and availability (CIA) of that data, as is the case with any data. Shown in Figure 4 below is a summary of how Data Types impact the selection of an IG. It is worth noting that the types of data an enterprise handles are one of the more heavily weighted factors when it comes to selecting an IG.

Figure 4 | **Data Type factors impacting IG selection**



Resources and Technology

Aside from the size, complexity, and data types that can factor into IG selection, resources and technology will also play a role. The three main resources that often impact implementation in an enterprise are time, budget, and skill set. Some enterprises can face challenges in one or more of these areas. For example, an enterprise may have the time to implement a technology, but not the budget or skill set. Likewise, they have the skill set and budget, but no time due to competing priorities. In these cases, enterprises should determine which areas (time, budget, skill set) need more focus to succeed at implementation. Technology may also play a role in implementation. For example, some enterprises use existing or no-cost technology, commercial off-the-shelf (COTS) products, or they also use proprietary/custom-built software. Again, this comes back to the question of resources, which will determine the type(s) of software used.

It is important to note that if an enterprise is classified under a higher IG (e.g., IG3), but does not have the resources to implement those Safeguards, it does not reduce the threshold for which IG they would select. This means that if an enterprise is heavily regulated, but does not have the budget to implement IG3 Safeguards, then a deeper look into why that is happening is required. For example, it might require more work to get leadership buy-in and secure additional funding or may necessitate looking outward at a third party to take on some of the burden that the enterprise cannot handle in-house. It also means that an IG3 enterprise needs to start at IG1 regardless. If there are challenges or barriers to implementation, start small and work up from there as resources allow.

In looking at IG1, these are enterprises with limited cybersecurity expertise or resources. It is not uncommon for an IG1 enterprise to outsource its cybersecurity needs to a Managed Service Provider (MSP), Cloud Service Provider (CSP), and/or Managed Security Service Provider (MSSP). IG1 enterprises will often utilize their existing processes and technology stack, consisting of no-cost or COTS products.

Want to know more about how to determine the cost of implementing IG1? Check out our Cost of Cyber Defense: Implementation Group 1 (IG1) that can help provide a baseline of how much it could cost during implementation

Moving to IG2, enterprises are implementing enterprise-grade technology into their infrastructure. Along with that, they have specialized expertise (either in-house or a third party) in installing and properly configuring the systems. They are using COTS products, and may also be using custom-built/proprietary software, depending on the needs of the enterprise. IG2 enterprises demonstrate a higher maturity when it comes to implementation.

From there, an IG3 enterprise employs in-house expertise that specializes in various areas of technology and cybersecurity. They have a fully formed Information Technology (IT) department, an in-house information security team, an engineering team, and more. They also have other teams that support these areas, such as legal and procurement, which play a role in many enterprise processes (e.g., software procurement). In addition to the use of COTS products, they use software designed

in-house or proprietary to the enterprise. IG3 enterprises also have the ability to purchase dedicated cybersecurity software for specific tasks. Shown below in Figure 5 are the Resources and Technology factors that impact IG selection.

Figure 5 | **Resources and Technology factors impacting IG selection**

Threat Types

There are different types of threats that an enterprise can be exposed to, such as cyber attacks (e.g., ransomware), physical threats (e.g., flood), or hybrid threats (e.g., power grid attack). For the CIS Controls, the Safeguards are primarily focused on cyber threats. Cyber attacks can be opportunistic attacks, where the attacker takes advantage of an opportunity but is not necessarily targeting an enterprise. They may also be targeted and planned well in advance of the actual attack, aiming to elicit a specific result.

Additionally, cyber threats can have different motivations, such as geopolitical, financial, ideological, or dissatisfaction. The type of threat actor can change based on motivation, including nation-state threat actors, cybercriminals, terrorist groups, or insiders. There is another type of threat that is less innocuous in nature, and that is human error. While the intent is not necessarily malicious, human error still poses a threat to enterprises and can result in significant harm depending on the error. An example is a user who fails to securely configure a database, which leads to leaked data and results in a data breach.

When selecting an IG, the types of threats that an enterprise faces can vary. For enterprises that handle large amounts of intellectual property (IP), a nation-state threat actor may be one of their biggest threats. For financial institutions, a cybercriminal may be the most common threat actor they

face. In terms of the CIS Controls, enterprises that face general, non-targeted attacks are well suited to implement IG1. In fact, our CIS Community Defense Model (CDM) v2.0 stands behind this statement with data.

The CIS CDM v2.0 asserts that, independent of any specific attack type, implementing IG1 Safeguards defends against 74% of ATT&CK (sub-) techniques in the MITRE ATT&CK® framework.

Moving to IG2 provides additional protection for enterprises facing more advanced cyber threats. Threat actors target sensitive information or other data that could hurt the enterprise, potentially resulting in a loss of public trust. IG2 enterprises also face industry-specific threats. IG3 offers the highest level of protection and is geared toward enterprises that are exposed to more sophisticated and targeted attacks, such as zero-day exploits and/or nation-state threat actors. If an attack is successful on an IG3 enterprise, there will be significant harm caused to the welfare of the public. Shown below in Figure 6 are the Threat Type factors impacting IG selection.

Figure 6 | **Threat Type factors impacting IG selection**

Risk

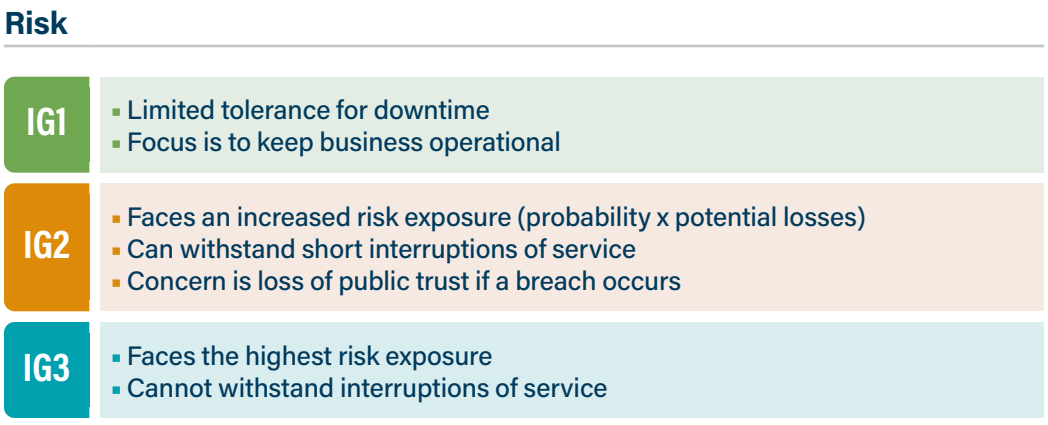
Risk management is at the center of most enterprises' business operations. There are different facets of risk management, but two key components that often factor into the selection of IGs are risk tolerance and risk appetite. Explained in basic terms, risk appetite is compared to a speed limit sign on a highway, whereas risk tolerance is how much the driver is willing to go over the speed limit. In the realm of cyber threats, an enterprise may have a risk appetite for service disruptions to their website, but one of the risk tolerance criteria indicates that the enterprise's website can be down no longer than three hours.

In terms of how risk factors into IG selection, an IG1 enterprise has limited tolerance for downtime. Its focus is to keep business operational—meaning, keeping the lights on and the doors open. A cyber attack taking out a significant portion of their infrastructure, such as a ransomware attack, could mean that they risk going out of business in some instances. This is often a result of maturity. While an SME may identify as an IG1, it may not be fully mature yet in terms of cyber protections. Therefore, if the enterprise is not prepared, an attack could bring them to a halt. This is where incident response preparation is key. If nothing else, incident response will help enterprises be prepared when an incident strikes so that they can work to return to normal business operations as soon as possible.

Ready to take the next step in determining your risk? Download CIS RAM v2.1, an information security risk assessment method that helps enterprises implement and assess their security posture against the CIS Controls.

An IG2 enterprise might face an increased risk exposure, but they can also withstand short interruptions in service. For example, they have a disaster recovery site or robust backup solution where they are able to fail over to a backup in a short amount of time. However, the loss of public trust is one of the biggest concerns with IG2 enterprises, so upholding brand reputation and communication are key during an incident. IG3 enterprises face the highest risk exposure and cannot withstand interruptions of service. An example of this would be a city government that just suffered a targeted attack on its infrastructure and has lost years of records. On top of losing public trust, they also now are faced with a data breach that is subject to certain breach notification laws requiring reporting and response. Loss of life can also play a role in incidents, impacting safety. Shown below in Figure 7 are the Risk factors impacting IG selection.

Figure 7 | **Risk factors impacting IG selection**



Tailoring Your Implementation

There are times where your enterprise requires a unique approach to cybersecurity. Just as you tailor your clothing, you may also tailor which Safeguards to implement. In more technical terms, while the CIS Controls address general best practices that enterprises should implement to protect their environment, some operational environments may present unique requirements. For example, if implementing a technology costs $1 million, but the enterprise's revenue is $500,000 a year, then it might not be reasonable to implement that technology as it could bankrupt the enterprise. In this case, they can choose to implement a different technology or compensating control that will still safeguard the enterprise, but not put them out of business. On the other hand, perhaps it is reasonable to implement the Safeguard with a small loan and then move forward based on the positive impact that it can have on the enterprise (e.g., mitigating a large threat). Each situation will be unique to the enterprise.

Laws, Regulations, and Compliance

It was previously mentioned under Data Types that laws and regulations can impact the selection of IGs. It is also one of the largest areas that may require tailoring. This could be due to industry-specific regulations. For example, the Federal Information Security Management Act (FISMA) applies to several organizations including federal agencies, contractors working with the federal government, service providers who handle federal data (e.g., CSPs, MSPs), state agencies, and more. NIST® SP 800-53[4] and NIST SP 800-171 play a crucial role in FISMA compliance. For IG1 and IG2 enterprises, there are likely certain systems or data that require additional protections (i.e., Safeguards from a higher IG). The CIS Controls help bridge that gap between frameworks by providing mappings to over 25 different frameworks.[5]

Auditing is another element that is often related to compliance and regulations. There are two main types of audits: internal and external. Audits in general are a great way to help facilitate growth and maturity in an enterprise in defending against cybersecurity threats while also demonstrating compliance. This could involve an internal audit, as a way to assess control implementation. It can also involve an external audit, which will consist of an independent assessor evaluating control implementation for compliance or security purposes. A common way for enterprises to prepare for an

4 National Institute of Standards and Technology (NIST)

5 CIS Controls Navigator as well as Excel versions of each mapping are available for download

external audit is by undergoing an internal audit prior to the engagement to identify any opportunities for improvement or findings that need to be resolved. It is worth noting that depending on the framework and/or regulation, not all need to undergo an external audit.

Cyber Insurance

Cyber insurance often requires a specific set of protections to be put in place in order to obtain coverage. Additionally, coverage may vary depending on the levels of protection an enterprise has in place. This may be determined by the insurer through questionnaires, assessments, or a combination of the two. Keep in mind that not all types of threats are covered by cyber insurance, so it should not act as failproof protection, but instead as a supplemental way to transfer some of the risk an enterprise holds.

Putting It All Together

For enterprises wanting to understand more about how to select an IG to implement, following the guidance from these five factors is key. The IGs provide a solid foundation for an enterprise to build a cybersecurity program.

Figure 8 | **The five factors impacting the selection of IGs**

Factors Affecting Implementation

	 Size and/or Complexity	 Data Types	 Resources and Technology	 Threat Types	 Risk
	CHARACTERISTICS				
IG1 ESSENTIAL CYBER HYGIENE	▪ Small and medium-sized enterprises ▪ Starting point for all enterprises	▪ Data is low sensitivity ▪ Stores unregulated employee and company financial information ▪ No regulatory or compliance oversight	▪ Limited cybersecurity expertise, may outsource IT/cybersecurity needs ▪ Uses existing and/or cost-effective technology and processes ▪ Uses Commercial off-the-Shelf (COTS) products	▪ Exposed to general, non-targeted attacks (e.g., Ransomware, Malware, Web Application Hacking, Insider and Privilege Misuse)	▪ Limited tolerance for downtime ▪ Focus is to keep business operational
IG2	▪ Enterprises managing IT infrastructure spanning multiple departments with differing risk profiles ▪ Increased operational complexity	▪ Stores and processes sensitive client or enterprise information ▪ Pockets of regulatory or compliance oversight	▪ Implements enterprise-grade technology ▪ Has specialized expertise to install and properly configure software ▪ Use COTS products, and may be using proprietary/ in-house software	▪ Exposed to more advanced cyber threats, resulting in a loss of public trust ▪ Exposed to industry-specific threats	▪ Faces an increased risk exposure (probability x potential losses) ▪ Can withstand short interruptions of service ▪ Concern is loss of public trust if a breach occurs
IG3	▪ Large enterprises that are operationally complex ▪ Increased risk profile across the enterprise	▪ Stores and processes sensitive and confidential data ▪ Subject to regulatory and compliance oversight	▪ Employs security experts that specialize in various areas of cybersecurity ▪ Likely using software designed in-house or proprietary to the enterprise, in addition to COTS products ▪ Ability to purchase dedicated cybersecurity software for specific tasks	▪ Exposed to sophisticated and targeted attacks, including zero-day attacks and/or nation-state threat actors ▪ Successful attacks can cause significant harm to the public welfare	▪ Faces the highest risk exposure ▪ Cannot withstand interruptions of service

Impact and Benefits

There is one last question to consider: What impact and benefits does an enterprise receive by selecting a particular IG?

IG1

An enterprise selecting IG1 receives the most security value for the least number of "actions" (Safeguards) to implement. IG1 consists of 56 Safeguards that span across 15 (of the 18) Controls. This is backed by the CIS Community Defense Model (CDM) v2.0, where we assert that, independent of any specific attack type, implementing IG1 defends against 74% of the (sub-)techniques found in the MITRE ATT&CK® Enterprise framework.[6] Additionally, enterprises selecting IG1 can expect to implement many procedural Safeguards, along with some technical Safeguards, that have minimal impact on usability.

IG2

Enterprises selecting IG2 can expect to implement an additional 74 Safeguards, the largest group of the three IGs. They are comprised of procedural and technical defenses but lean heavily on the technical side. For example, allowlisting software, encryption, and penetration testing are some of the activities an enterprise will implement. IG2 also may have some impact on usability. In terms of defenses, IG2 provides additional protection as compared with IG1.

IG3

IG3 enterprises have 23 additional Safeguards to implement that are heavily technical. These are activities such as implementing an intrusion prevention solution, role-based access control, and a data loss prevention solution. Implementing IG3 Safeguards also provides the highest defense, defending against 86% of ATT&CK (sub-)techniques in the MITRE ATT&CK® framework. In terms of impact, these are activities that will have an impact on usability.

6 MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) v8.2

Figure 9 | **Impact and Benefits of selecting a particular IG**

Impacts and Benefits of Implementation

IG1	▪ Many procedural Safeguards ▪ Safeguards have minimal impact on usability ▪ Effective security value: independent of any specific attack type, this IG defends against 74% of ATT&CK (sub-)techniques in the MITRE ATT&CK framework
IG2	▪ Combination of procedural and technical defenses ▪ Contains the largest number of defenses ▪ Impact to usability may occur
IG3	▪ Safeguards have moderate impact on usability ▪ Leans heavily on technical defenses ▪ Implementation of all CIS Safeguards defends against 86% of ATT&CK (sub-)techniques in the framework.

Conclusion

Implementation Groups are the solution to implementing a cybersecurity framework while limiting the "drinking from a firehose" experience. An enterprise needing to implement one or more frameworks can use the CIS Controls as that bridge to reduce the need for multiple assessments and help improve inefficiencies in control implementation. Enterprises wanting to determine which IG to begin with should first focus on the five factors (*Size and/or Complexity*, *Data Types*, *Resources and Technology*, *Threat Types*, and *Risk*) that impact IG selection. Once an IG is selected, an enterprise can begin to look at specific needs that would require tailoring and start developing their cybersecurity program (i.e., laws, regulations, compliance, and cyber insurance). Keeping in mind that cybersecurity is a journey and not a destination, IG implementation is an iterative process that should be continually reassessed and improved as technology and threats advance in the globally connected world we live in.

Appendix A

About the CIS Controls

The CIS Critical Security Controls (CIS Controls) are a prioritized set of actions that collectively form a defense-in-depth set of best practices that mitigate the most common attacks against systems and networks. They are developed by a community of Information Technology (IT) experts who apply their first-hand experience as cyber defenders to create these globally adopted security best practices. The experts who develop the CIS Controls come from a wide range of sectors, including retail, manufacturing, healthcare, education, government, defense, and others.

The Implementation Group methodology was developed as a new way to prioritize the CIS Controls. These IGs provide a simple and accessible way to help enterprises of different classes focus their scarce security resources, while still leveraging the value of the CIS Controls program, community, and complementary tools and working aids.

If you would like to know more about the CIS Controls and Implementation Groups, there are many resources available on our website at https://www.cisecurity.org/controls/.

Appendix B

Acronyms and Abbreviations

CIA	Confidentiality, Integrity, Availability
CIS CDM	CIS Community Defense Model
CIS CSAT	CIS Controls Self Assessment Tool
CIS RAM	CIS Risk Assessment Method
CMMC	Cybersecurity Maturity Model Certification
COTS	Commercial off-the-Shelf
CSP	Cloud Service Provider
EU	European Union
FISMA	Federal Information Security Management Act
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
IG	Implementation Group
IP	Intellectual Property
IT	Information Technology
MITRE ATT&CK	MITRE Adversarial Tactics, Techniques, and Common Knowledge
MSP	Managed Service Provider
MSSP	Managed Security Service Provider
NIST SP	National Institute of Standards and Technology Special Publication
PCI DSS	Payment Card Industry Data Security Standard
SBA	Small Business Administration
SME	Small and medium-sized enterprises

Appendix C

Links and Resources

CIS Critical Security Controls® (CIS Controls®) v8.1 | Learn more about the CIS Controls, including how to get started, why each Control is critical, procedures and tools to use during implementation, and a complete listing of Safeguards for each Control.

CIS Community Defense Model (CDM) v2.0 | A guide published by CIS that leverages the open availability of comprehensive summaries of attacks and security incidents, and the industry-endorsed ecosystem that is developing around the MITRE ATT&CK Framework.

CIS Controls Assessment Specification | Provides an understanding of what should be measured in order to verify that the Safeguards are properly implemented.

CIS Controls Navigator | Learn more about the Controls and Safeguards and see how they map to other security standards (e.g., CMMC, NIST SP 800-53 Rev. 5, PCI DSS, MITRE ATT&CK). Available for CIS Controls versions 8.1, 8, and 7.1.

CIS Controls Self Assessment Tool (CIS CSAT) | Enables enterprises to assess and track their implementation of the CIS Controls for versions 8.1, 8, and 7.1.

CIS Cost of Cyber Defense | IG1: CIS has published The CIS Cost of Cyber Defense: Implementation Group 1 (IG1), to help you answer these questions: Which protections to start with? Which tools will be needed to implement those protections? and How much will an implementation will cost?

CIS Risk Assessment Method (CIS RAM) v2.1 | An information security risk assessment method that helps enterprises implement and assess their security posture against the CIS Controls.

Establishing Essential Cyber Hygiene | IG1 is essential cyber hygiene and represents a minimum standard of information security for all enterprises. This guide will help enterprises establish essential cyber hygiene.

Guide to Asset Classes | In v8.1, CIS restructured Asset Classes and their respective definitions to ensure consistency throughout the Controls. Learn more about our naming conventions and what they mean.

CIS WorkBench | Get involved in one of our many communities.

The Center for Internet Security, Inc. (CIS®) makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation.

We are a community-driven nonprofit, responsible for the CIS Controls® and CIS Benchmarks™, globally recognized best practices for securing IT systems and data. We lead a global community of IT professionals to continuously evolve these standards and provide products and services to proactively safeguard against emerging threats. Our CIS Hardened Images® provide secure, on-demand, scalable computing environments in the cloud.

CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), which supports the rapidly changing cybersecurity needs of U.S. elections offices.

CIS® Center for Internet Security®

www.cisecurity.org
info@cisecurity.org
518-266-3460
Center for Internet Security
CenterforIntSec
@CISecurity
TheCISecurity
cisecurity