Governance, Risk, and Compliance

How to Construct a Sustainable GRC Program in 8 Steps

January 2023

CIS Center for Internet Security®

CIS SecureSuite®

Contents

Executive Summary

Change is a constant… and it can be costly trying to keep up. In a report, for instance, 90% of compliance leaders told Accenture they expected their compliance-related costs to increase amidst evolving business, regulatory, and customer demands.

These findings underscore the importance of taking a holistic approach using a sustainable governance, risk, and compliance (GRC) program. To do this, you first need to know what each of these terms means to you and your organization. Let's take a moment to do just that:

- Governance is the process by which decisions are made about risks. It also covers the programs you establish to manage risk to a degree that is acceptable to your organization and that aligns with your organizational mission and goals.
- Risk is enabling your organization to address uncertainty through identifying, categorizing, assessing, and enacting strategies.
- Compliance consists of the mechanisms by which your organization can illustrate integrity and a level of adherence to standards, laws, regulations, and best practices.

There are many moving parts to a successful GRC program. How do you get started? The purpose of this guide is to walk you through the process of setting up a sustainable GRC program and demonstrate how a CIS SecureSuite Membership can help you along the way.

Step 1

How to Create an Efficient Governance Control Program

Your first step along the path of establishing a sustainable governance, risk, and compliance program is implementing a robust governance control program. This program needs to do two things. First, it must help you to address the current control environment. Second, it must help you prepare for the future risk environment.

In this section, we'll discuss what goes into a robust governance control program, the challenges you might face, the steps you can use to overcome those challenges, and how a CIS SecureSuite Membership can help you along the way.

Fundamentals and Challenges of Governance

At its heart, governance should be about security practices and focus on risk mitigation as a security concept rather than as a compliance driver. Governance is the process by which decisions are made. It is designed to formalize processes, assign roles and responsibilities, and understand indicators for decisions and adaptations; it should not be focused on compliance only. You can monitor risks, but without a governance framework, you can't know if you are measuring the right risks for you.

When focusing solely on compliance, you miss understanding the foundation on which your security is built and how to mitigate the risk. Compliance will ultimately be a by-product of good security practices that can be guided by security governance frameworks. These include the National Institute of Standards and Technology's Cybersecurity Framework (NIST CSF), the Health Insurance Portability and Accountability Act (HIPAA), and the Payment Card Industry's Data Security Standard (PCI DSS) v4.0, among others to which our security best practices map.

Frameworks Provided with CIS Controls Mapping

Australian Signals Directorate Essential Eight	FFIEC-CAT	NERC-CIP	SOC 2
Azure Security Benchmark v3	GSMA FS 31 Baseline Security Controls	New Zealand Information Security Manual v3.5	TSA Security Defense Directive Pipeline
CISA Cybersecurity Performance Goals (CPGs)	HIPAA	NYS Department of Financial Services 23 NYCRR Part 500	UK Cyber Essentials
CMMC	ISACA COBIT 19	NIST CSF	UK NCSC Cyber Assessment v3.1
Criminal Justice Information Services (CJIS)	ISO 27001:2022	NIST SP 800-53 R5	
CSA Cloud Controls Matrix v4	ISO/IEC 27002:2022	NIST SP 800-171	
Cyber Risk Institute (CRI) Profile v1.2	MITRE ATT&CK v8.2	PCI DSS	

Industry Frameworks Referencing CIS Benchmarks

DISA STIGs	FISMA
FedRAMP	PCI DSS
FFIEC	

But you may face challenges along the way. The most prominent obstacles are time, resources, and engagement. A program is only as good as its weakest link, and things are always changing. In a chain of events, something that is your strongest element one day can with a single vulnerability become a top priority the next. Building a robust governance control program is about agility and adaptation. It's a journey, not a destination.

A Process for Sustainable Governance

Addressing risks is not just about the capabilities of today but forward-looking approaches to assess the business context of strategic decisions and their impact on operational controls. Failing to plan is planning to fail. That's why we've established a four-step process that can ensure success in building a governance program founded on sustainability.

Establishing a Foundation. Your journey toward robust governance control begins with establishing a solid foundation. A house built on a shaky foundation will collapse over time. The framework of foundational practices and addressing the cultural shift to security as a business concept, not a technology problem, is key. We all have roles to play; we all utilize technology to further enhance organizations and programs. Human error accounts for the majority of social engineering attacks, after all. If we as people do not understand what needs to be protected and what basic safeguards we need to implement, we are doing everyone a disservice. Technology is everywhere, and it is not going away. Ignorance is not bliss. There are casualties when security is not embedded in the culture from both a professional and personal level.

Foundational practices and a cultural shift rooted in your business constitute proven practices by which you can start gauging your overall maturity and path to continuous improvement. You will need to measure and plan for today and look ahead to where you want to be. To get this view, you need to stand on solid ground, and that starts off with your governance program.

While navigating this step, it's important for you to understand your regulatory environment and build capabilities to support the compliance of your internal program to that of your sector. Let's look at a few examples. Some organizations that do contractual work with the United States government are required to align to FISMA NIST 800-53, for instance. Meanwhile, if you are dealing with Controlled Unclassified Information (CUI), you should be aligning to NIST 800-171. When it comes to protecting data in the healthcare sector, you may fall under HIPAA, whereas the processing of credit card data puts you under PCI DSS.

Bringing stakeholder and business context in at this step will help you to align practices to support risk management and compliance. The controls in place will have the benefit of being informed of the requirements for control as well as a capability that will enforce a by-product of compliance. Context and business alignment are key, not the implementation of a control for no reason other than compliance.

Standardizing Configurations. Standardizing the configuration of your systems is a foundational step to controlling and managing your applications and data. The house analogy works here, as we need the foundational elements strong enough to support the respective application and data being processed within them. A baseline level 1 configuration is a good practice for all types of processing. If you have systems with highly sensitive data and controlled application process activities, a more resilient and restrictive configuration profile is needed. Not all systems require a foundation fit for a skyscraper. Nor should skyscrapers be built on bare ground.

Consistency and continuous assessment are key to completing this step. Some organizations are inclined to approach system configuration with a "set it and forget it" mentality. In reality, system configuration fits into change management; as such, you need to address any deviation from the set image for system configuration as part of a process of continuous review and assessment. If you don't, you risk not understanding the overall impact of deviations when it comes time to integrating and updating.

Some organizations are inclined to approach system configuration with a "set it and forget it" mentality. In reality, system configuration fits into change management; as such, you need to address any deviation from the set image for system configuration as part of a process of continuous review and assessment.

Continuous Monitoring and Assessment. As with any program over time, your governance program needs maintenance, as it will face many structural stresses, including organizational growth, strategic focus, upgrades, and new systems/applications. Addressing these as a program of continuous assessment requires care and attention, for risks, regulatory requirements and frameworks, and the technology to conduct business operations change over time. Each change is part of the intake process to assess the viability and sustainability of the current governance controls program.

During this step, technology is less of an issue. The process here is one of alignment and change management. It may be upgrades or add-ons that help to assist in providing a continuous assessment capability, but the planning and preparation of the program should have built-in checks and balances for the program itself. The checks involve the controls' effectiveness in assessing a risk posture, while the balances represent the ability to utilize the information those checks are creating. In other words, there needs to be a cause and effect in place, a continuous assessment to establish a credible control but a balance that the control is working and not taxing systems or degrading functionality business value.

Much like assessing controls that change over time, the overarching governance program should have the same assessment. It may have started as an internal program to perform self-assessments, but over time, it is required to comply with privacy regulations, changes in business dynamics, or even new regulations for your sector.

Implementing Controls Using the Assessment of Threat-Based Intelligence. Context is consistently mentioned, and we have a few avenues for applying context. One of the most important is the threat landscape. Why address specific threats when a cyber threat actor (CTA) is not specifically targeting your industry? You should focus on those threats that are most likely to target your organization and thus have the greatest impact.

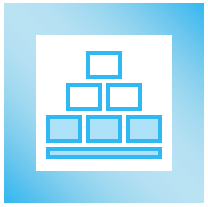
For this step, control with context and do not overvalue the control in light of the asset being controlled. The simple example here is to not pay $1,000 to control a $1 asset. Distribution of the resources for controls should be distributed in the same context. Put the most resources where respective threats exist but not all your eggs in one basket.

Building a Governance Program with CIS SecureSuite

The process of establishing a foundation, standardizing configurations, continuous monitoring and assessment, and implementing controls using the assessment of threat-based intelligence can be difficult to do on your own. But you don't have to do it alone. CIS SecureSuite offers a variety of resources designed to aid you in safeguarding your systems and data. It comprises benefits, tools, and resources that can help you implement adequate security measures and control governance using our consensus-driven security best practices.

Let's now take a look at how you can use a CIS SecureSuite Membership to navigate the four-step process we discussed above.

CIS SecureSuite offers a variety of resources designed to aid you in safeguarding your systems and data. It comprises benefits, tools, and resources that can help you implement adequate security measures and control governance using our consensus-driven security best practices.



1 Establish a Foundation with CIS Controls

The CIS Critical Security Controls (CIS Controls) consist of 18 prioritized best practices based on your risk profile and available resources that you can use to improve your cybersecurity defenses. They encompass various areas like inventory and control of hardware assets, continuous vulnerability management, secure configuration for hardware and software, incident response, and more.

Each CIS Control breaks down into individual Safeguards, think of them as sub-steps which help you work your way through implementing a Control in a way that supports your unique goals and cybersecurity maturity. For ease of use, we've also organized the CIS Controls and Safeguards into different Implementation Groups (IGs). We recommend that you start with Implementation Group 1 (IG1), as you can use this subset of Controls and Safeguards to achieve essential cyber hygiene and defend against today's most common threats. As your cybersecurity posture matures, you can then move on to Implementation Group (IG2) and Implementation Group 3 (IG3), the latter of which encompasses all 18 Controls and 153 Safeguards.

The number of Safeguards an enterprise is expected to implement increases based on which group the enterprise falls into.

153
TOTAL SAFEGUARDS

IG3 IG3 assists enterprises with IT security experts to secure sensitive and confidential data. IG3 aims to prevent and/or lessen the impact of sophisticated attacks.

23
SAFEGUARDS

IG2 IG2 assists enterprises managing IT infrastructure of multiple departments with differing risk profiles. IG2 aims to help enterprises cope with increased operational complexity.

74
SAFEGUARDS

IG1 IG1 is the definition of essential cyber hygiene and represents a minimum standard of information security for all enterprises. IG1 assists enterprises with limited cybersecurity expertise thwart general, non-targeted attacks.

56
SAFEGUARDS

Applying these Controls ensures that you're addressing the most significant threats first and doing so in a controlled, measured manner. As a governance tool, the Controls also establish consistent rules for security measures across your organization.

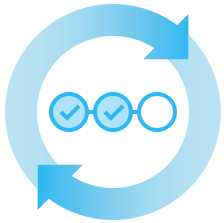
Applying these Controls ensures that you're addressing the most significant threats first and doing so in a controlled, measured manner. As a governance tool, the Controls also establish consistent rules for security measures across your organization.

2 Standardize Configurations with CIS Benchmarks

Employing CIS Benchmarks ensures that your systems are configured securely. These guidelines help you configure various aspects of your IT infrastructure—from operating systems and software applications to network devices. What's more, the Benchmarks map to the Controls, which means you can extend the fundamentals of a cyber defense program across individual operating systems that you've deployed in your environments.

The CIS Benchmarks are consensus-based and developed with input from a vast community of security professionals. This means your configuration standards will be current and align with industry best practices. Standardization is a crucial governance principle; CIS Benchmarks help you to achieve this by providing clear configuration guidelines for your organization based upon the level of protection you need. Most Benchmarks contain multiple configuration profiles, with the Level 1 profile providing base-level recommendations. For added security, you can implement the Level 2 profile or the STIG profile that contains all recommendations specific to the Defense Information Systems Agency Security Technical Implementation Guide (DISA STIG).

CIS Benchmarks are available for free to everyone, but in this form, they require you to manually implement each of their hardening recommendations. This changes when you become a CIS SecureSuite Member and receive access to the CIS Build Kits. Available as Group Policy Objects (GPOs) on Windows devices and Bash shell scripts on Linux machines, CIS Build Kits automate the remediation section of the CIS Benchmarks,saving you time and money in applying secure configurations on your systems.



3 Continuous Monitoring and Assessment with CIS-CAT Pro

As we discussed above, monitoring and assessment form the core of a robust governance control program. The pro version of the CIS Configuration Assessment Tool (CIS-CAT Pro) helps you compare your system configurations and settings against the secure recommendation of the CIS Benchmarks. It provides real-time and continuous assessment, enabling you to understand your security posture accurately and make necessary adjustments promptly. CIS-CAT Pro also comes with its Dashboard functionality, which helps you track your compliance over a recent period of time so that you can measure your progress and plan ahead. This ensures that you've not only implemented but also followed your security measures. As a governance tool, this allows for transparency, accuracy, and accountability in your security management.

SecureSuite's impact on monitoring and assessment doesn't end there. As a Member, you also receive access to the pro version of the CIS Controls Self Assessment Tool (CIS CSAT Pro). You can use this resource to track and prioritize your implementation of the Controls over time, including identifying gaps and planning out tasks for the future. As a result, you can take a strategic approach to strengthening your cyber defenses in a way that works for your organization.

4 Utilizing the Community Defense Model

Lastly, the CIS Community Defense Model (CDM) v2.0 emphasizes the value of implementing the Controls using the assessment of threat-based intelligence along with attack tactics and techniques. When paired with CIS CSAT Pro, CDM v2.0 provides you with a plan for defending against today's most common cyber threats. In fact, it shows how you can defend against at least three-quarters of the MITRE ATT&CK (sub-) techniques associated with malware, ransomware, phishing, and other top cyber attacks by implementing the IG1 Safeguards.

In the context of your operations, by incorporating this model into your governance control program, you will be able to protect your organization, introduce a capability to assess threat-based strategies, and complement an approach to the continuous alignment of control and threat vector prevention.

Get Your Governance Control Program Going

Leveraging CIS SecureSuite helps you to build a comprehensive and efficient governance control program. It provides you with a blueprint to design, implement, and monitor cybersecurity controls, aiding you in managing digital risks better and fostering a robust cybersecurity culture.

Top 5 Attacks		IG1 CIS Safeguards IG1 can defend against XX% of ATT&CK (Sub-)Techniques		All CIS Safeguards CIS Safeguards can defend against XX% of ATT&CK (Sub-)Techniques
Malware	→	77%	→	94%
Ransomware	→	78%	→	92%
Web Application Hacking	→	86%	→	98%
Insider and Privilege Misuse	→	86%	→	90%
Targeted Intrusions	→	83%	→	95%

All percentages are based on ATT&CK (sub-)techniques assigned to an ATT&CK mitigation.

Cybersecurity isn't just a technical issue; it's a governance issue. By effectively using CIS SecureSuite's complement of practical guidance, you can lay the groundwork for a robust governance control program that ensures security measures are in place, adhered to, and continuously improved.

To-Do List

- ☐ Understand how time, resources, and engagement complicate your governance efforts amid constant change.
- ☐ Embrace our four-step process for sustainable governance using a CIS SecureSuite Membership.
- ☐ Establish a foundation with the CIS Controls, starting with IG1.
- ☐ Standardize your system configurations with the CIS Benchmarks.
- ☐ To automate your application of the CIS Benchmarks' security recommendations, deploy a CIS Build Kit.
- ☐ Engage in continuous monitoring and assessment through CIS-CAT Pro and CIS CSAT Pro.
- ☐ Strengthen your defenses against today's most common threats using CIS CDM v2.0.

Step 2

Risk Mitigation: The Cornerstone of Your Audit Preparations

If you're getting ready for an audit, you might feel that the preparation and continuous assessment criteria feel like a rehearsal and/or "extra" work, especially if your compliance program has been operational and successful for a few years.

Audit preparations don't have to be so onerous, however. In this section, we'll discuss several steps that you can use to embed risk mitigation strategies into your audit preparations with the help of CIS SecureSuite. Doing so will help you to transform potential challenges into opportunities for growth and improvement.

Understanding the Importance of Risk Mitigation

Risk is inherent in every facet of the business. When we talk about trouble in terms of audit preparations, it covers a broad spectrum: financial discrepancies, non-compliance with laws and regulations, operational inefficiencies, reputational damage, and more.

Each auditor also looks at audits differently. Each has their own specialties, and there is always the unknown of what an auditor wants to see in terms of controls and evidence. As a result, disruptions may occur within the organization to pull in subject matter experts from various business units.

To preempt these risks, you can adopt a proactive approach. This is where risk mitigation comes into play. It's not just about managing the risks; it's about understanding them, planning for them, and creating systems to reduce their potential impact.

Incorporating Risk Mitigation in Your Audit Preparations

Here are several steps that you can use to incorporate risk mitigation into your audit preparations.

Risk Identification and Assessment. The first step towards effective risk mitigation is identifying and assessing potential risks. This process should involve stakeholders from across your organization to ensure that you have a comprehensive understanding of all potential operational and strategic risks. Risk identification can be as quick as a minute, while an assessment can take weeks or months dependening on the context. What is important at the start is to ask the right questions and use scenario analysis to address the risk in the context of your business and operations. Indeed, you need to understand your environment and the acceptable risk level for your organization. Risk identification and assessment are dependent on your organization and its mission/goals. As such, context is very important; your questions need to address this to ensure appropriate scoping.

Developing a Risk Management Plan. Once you've identified and assessed your risks, you can create a risk management plan detailing how you will address each risk. This could involve avoiding the risk, reducing the negative effect of the risk, transferring the risk to another party, or accepting some or all of the consequences of a particular risk.

Quick Tip

Alignment to a common framework can help you assess risk during this step. Your starting point should be to discuss organizational activities in terms of risk and use that context to assess the structural approach that you can take to build a risk management plan. Risk is often in the eye of the beholder; high risk to some is low to others. Calibration of the plan and the methods of risk identification are key components.

Incorporating Risk Mitigation into Internal Controls. Implementing robust internal controls is a crucial part of risk mitigation. These controls safeguard your organization by ensuring the integrity of financial and accounting information, meeting operational efficiency, and complying with laws and regulations.

Regular Monitoring and Review. Risk mitigation is an ongoing process. Monitoring and reviewing the risks and the effectiveness of the control measures no less frequently than on an annual basis are crucial to managing the changing landscape.

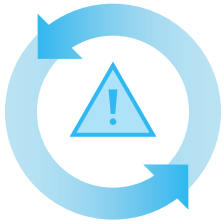
Communicating and Reporting. Clear, timely communication of your risk mitigation strategies and their progress to all relevant stakeholders helps ensure that everyone is on the same page so that they can contribute effectively to your risk mitigation efforts. If everyone does not align with the risk mitigation efforts, then risk mitigation becomes ineffective and hard to implement. This is one reason why you need a single person accountable; it is their decision as risk owner that the organization will commit no matter the outcome of the assessment.

Training and Education. Invest in training your team on risk awareness and mitigation strategies. When your team understands the importance of risk management in audit preparation, they are more likely to uphold the procedures and controls set in place.

Leveraging Technology. Consider using technology solutions to automate and streamline risk management processes. Software tools can help in risk identification, management, monitoring, and reporting, reducing the potential for human error and improving efficiency.

Instituting Risk Mitigation with CIS SecureSuite

If you're just starting off with risk mitigation, you might not know how to put the steps I discussed above into action. Fortunately, a CIS SecureSuite Membership has everything you need to get things moving. Here's a brief overview of how.

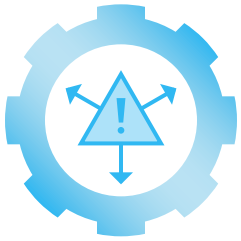


1 Fulfilling Risk Mitigation with the CIS Controls

As mentioned, the CIS Critical Security Controls (CIS Controls) are robust internal controls that you can use for risk assessments and risk mitigation. But let's take a closer look. Say you want to ensure the integrity of financial and accounting information. You can use CIS Control 10.5: Enable Anti-Exploitation Features to prevent malware from tampering with your systems and data.

The Controls work in a number of other use cases involving risk mitigation, too. For instance, you can enact all Safeguards in CIS Control 14 to increase your employees' risk awareness and understanding of mitigation strategies. Additionally, you can use our CIS Controls Navigator to map your use of the Controls to frameworks and regulations with which you're looking to comply.

The Controls and the Controls Navigator are free to use. With a CIS SecureSuite Membership, you gain access to CIS CSAT Pro along with other benefits, tools, and resources that make your implementation program even simpler.



2 Planning Risk Mitigation with CIS CSAT Pro

You need a plan to manage your organization's risks. You can formulate one using the pro version of the CIS Controls Self Assessment Tool (CIS CSAT Pro), which comes with a SecureSuite Membership. CIS CSAT helps you to formalize your implementation of the Controls so that you can track your implementation of individual CIS Safeguards in accordance with your risk management plan. You can even create and assign implementation tasks, thereby communicating to your team and to other stakeholders how they can support your organization's risk mitigation efforts.

3 Achieving Visibility with CIS-CAT Pro

CIS SecureSuite Members receive access to the pro version of the CIS Configuration Assessment Tool (CIS-CAT Pro). It comes with two main components, CIS-CAT Pro Assessor and CIS-CAT Pro Dashboard.

With CIS-CAT Pro Assessor, you can automate your scans against the security recommendations of the CIS Benchmarks, our secure configuration guidelines developed through consensus with IT professionals around the world. This component saves you time and money in visualizing the state of your system hardening efforts.

CIS-CAT Pro Dashboard graphically displays your scan results with CIS-CAT Pro Assessor in a dashboard. Not only that, but you can use this component to review your scan results over a recent period of time so that you can appreciate how far you've come with your risk mitigation program and where you still need to go. Try CIS-CAT Lite for Microsoft Windows 10, Ubuntu, or Google Chrome.

4 Streamlining with the CIS Build Kits

CIS-CAT Pro helps you to automate your evaluation of your systems against the CIS Benchmarks. The CIS Build Kits — another CIS SecureSuite Membership benefit — help you to automate the implementation of the Benchmarks' hardening guidelines themselves.

Available as Group Policy Objects (GPOs) for Windows and Bash shell scripts for Linux Machines, the Build Kits automate the "Remediation" section of the CIS Benchmarks so that you can automatically harden a system of your choosing. This saves you even more time and money when you're mitigating risks, as it helps you to minimize instances of human error as well as respond to risks more quickly. Try a sample CIS Build Kit today!

CIS Build Kits automate the "Remediation" section of the CIS Benchmarks so that you can automatically harden a system of your choosing. This saves you even more time and money when you're mitigating risks, as it helps you to minimize instances of human error as well as respond to risks more quickly.

5 BONUS: Using CIS RAM for Assessing Risks

A CIS SecureSuite Membership provides benefits, tools, and resources that you can use to maximize your implementation of CIS security best practices, including the CIS Controls. If you're already working to implement the Controls, you can build on the progress you've already made by using our CIS Risk Assessment Method (CIS RAM) v2.1.

Freely available to everyone — including SecureSuite Members — CIS RAM v2.1 guides you through the process of assessing your cybersecurity posture against the Controls. CIS RAM features a family of documents consisting of instructions, examples, templates, and exercises for conducting a cyber risk assessment. Together, these resources make it easy for you to assess security risks as you work your way

through the Controls, from establishing essential cyber hygiene with Implementation Group 1 (IG1) to implementing most if not all of the Controls under Implementation Group 3 (IG3).

Fostering a Risk-Aware Culture with CIS SecureSuite

Risk mitigation is not just about navigating through the storm; it's about anticipating it and ensuring you are well-prepared when it arrives. By incorporating a risk mitigation strategy into your audit preparations, you transform audits from potentially stressful events into a robust organizational improvement and success tool.

By doing so, you foster a risk-aware culture that will not only stand up to the scrutiny of an audit but will also improve decision-making, strategic planning, and overall business resilience. In a world of uncertainties, effective risk mitigation is your guiding compass, helping you to steer clear of potential pitfalls and navigate toward success.

To-do List

- ☐ **Recognize how a reactive approach to audit preparation can leave you vulnerable to reputational damage, non-compliance with laws, and other consequences.**
- ☐ **Incorporate risk mitigation into your audit preparations using a CIS SecureSuite Membership.**
- ☐ **Mitigate common risks by implementing specific CIS Controls.**
- ☐ **Create and assign implementation tasks through CIS CSAT Pro to help you manage your organization's risks.**
- ☐ **Visualize the state of your risk mitigation efforts with the Assessor and Dashboard components of CIS-CAT Pro.**
- ☐ **Minimize human error as you mitigate risk by deploying a CIS Build Kit.**
- ☐ **Leverage CIS RAM v2.1 to assess risks as you make your way through the Controls.**

Step 3

Why Assessments Are Key to Your Governance Audits

Assessments and governance audits are two sides of the same governance coin, working in tandem to ensure the credibility and integrity of your organization. The latter help you to objectively evaluate processes, controls, and risks within your organization, while the former provides valuable insights and evidence to support the audit process.

In this section, I'll discuss how assessments naturally complement your audits. I'll also explain how you can use the benefits, resources, and tools of a CIS SecureSuite Membership to conduct assessments in support of your audits.

The Multifaceted Impact of Assessments

Below are four reasons why assessments are key to successful audits.

Unveiling Hidden Risks. Assessments act as a spotlight, uncovering risks that might have gone unnoticed. They help you to identify gaps in your organization's processes, systems, or controls that could lead to non-compliance with regulations or standards, financial discrepancies, or even reputational damage. By identifying these risks early through assessments, you can preemptively take action to mitigate them, enabling smoother and more effective audits.

Quick Tip

When you're looking to unveil hidden risks, make sure that you break down the requirements. You might feel tempted to go straight to addressing high-level requirements, but to be effective, you need to spend some time exploring the details and understanding the technical elements.

Verifying Compliance and Effectiveness. An integral part of any audit is verifying compliance with relevant laws, regulations, and standards. Assessments provide the necessary evidence to demonstrate this compliance, showing that controls are not just in place but are also effectively addressing the intended risks. Furthermore, assessments can verify that processes are working and achieving their objectives. They offer

a methodical way to validate the efficacy of your organization's operations and governance, supporting the audit findings.

Facilitating Continuous Improvement. Assessments don't just provide a snapshot of the current state of affairs; they also offer insights into potential areas for improvement. By identifying weaknesses and areas of non-compliance, assessments can guide strategic decisions on where to allocate resources to improve processes and controls. This continual improvement is beneficial for achieving strategic objectives and is also looked upon favorably in audits, demonstrating a proactive commitment to good governance.

Promoting a Culture of Accountability. Assessments encourage accountability throughout your organization. They demand involvement from all levels, from executive management to frontline staff, promoting a shared responsibility for governance and compliance. This culture of accountability is a significant asset during audits, as it demonstrates that governance is not just a management concern but is also embedded throughout your organization.

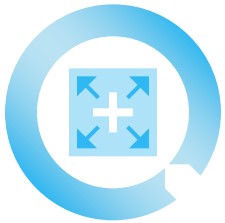
Quick Tip

If you're looking to develop a culture of accountability from scratch, you might want to consider sitting down with business owners and stakeholders to develop a Responsible Accountable Consulted Informed (RACI) matrix. In doing so, you'll be able to specify everyone's responsibilities and identify the true owners of a governance audit at your organization.

How CIS SecureSuite Supports Audits with Assessments

CIS SecureSuite provides you access to two assessment tools: the pro version of the CIS Controls Self Assessment Tool (CIS CSAT Pro) and the pro version of the CIS Configuration Assessment Tool (CIS-CAT Pro). Both will help you take a strategic approach to implementing CIS security best practices. They will also save you time and money when preparing for an audit.

Let's look at how these tools satisfy the four benefits of assessments discussed above.



1 Spotting Areas of Improvement

Both CIS CSAT Pro and CIS-CAT Pro can help you identify where you can strengthen your cybersecurity maturity. The former helps you track your implementation of the CIS Critical Security Controls, vendor-agnostic security measures that you can use to strengthen your cyber defenses. With CIS CSAT Pro, you can determine which Controls you've already enacted, identify security gaps, and map out future implementation efforts before your next audit.

It's a similar story for CIS-CAT Pro. This tool enables you to automate scans of your systems' settings against the recommendations of the CIS Benchmarks, secure configuration guidelines developed by IT professionals around the world using a consensus process. Using CIS-CAT Pro and its HTML output report, you can see to which recommendations each of your operating systems align and to which they don't. You can then identify steps that you can use to further harden your systems in preparation for an audit.

2 Snapshotting Your Compliance Efforts

The CIS Controls and CIS Benchmarks map to numerous security regulations and frameworks. This is by design. You can use these mappings to implement the Controls and Benchmarks in a way that not only accords with your unique needs but also fulfills your compliance objectives at the same time. You can therefore implement our security best practices once and not worry about duplicating your efforts.

Frameworks Provided with CIS Controls Mapping

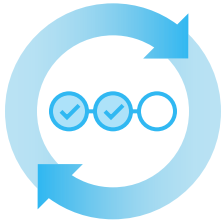
Australian Signals Directorate Essential Eight	FFIEC-CAT	NERC-CIP	SOC 2
Azure Security Benchmark v3	GSMA FS 31 Baseline Security Controls	New Zealand Information Security Manual v3.5	TSA Security Defense Directive Pipeline
CISA Cybersecurity Performance Goals (CPGs)	HIPAA	NYS Department of Financial Services 23 NYCRR Part 500	UK Cyber Essentials
CMMC	ISACA COBIT 19	NIST CSF	UK NCSC Cyber Assessment v3.1
Criminal Justice Information Services (CJIS)	ISO 27001:2022	NIST SP 800-53 R5	
CSA Cloud Controls Matrix v4	ISO/IEC 27002:2022	NIST SP 800-171	
Cyber Risk Institute (CRI) Profile v1.2	MITRE ATT&CK v8.2	PCI DSS	

Industry Frameworks Referencing CIS Benchmarks

DISA STIGs	FISMA
FedRAMP	PCI DSS
FFIEC	

As discussed above, CIS CSAT Pro and CIS-CAT Pro help you to streamline your implementation of the Controls and the Benchmarks, respectively. They simplify your compliance program even further by reducing manual effort (in the case of CIS-CAT Pro), improving your visibility, and providing you with resources to plan for the future. In that sense, they empower you to take a proactive approach to your audits by planning and building upon your compliance objectives.

The same can be said about assessing your risks. With CIS CSAT Pro specifically, you can focus on the strategy of evaluating your cybersecurity posture against the Controls using the CIS Risk Assessment Method (CIS RAM) v2.1. This is important, as you may need to communicate this strategy and demonstrate how you've taken "due care" in the event of a security incident. CIS CSAT Pro helps you to formalize your risk assessments; you're able to document what you've done and why those controls are "reasonable" based on your understanding of the risks at your organization.



3 Enabling Continuous Assessments

With CIS CSAT Pro and CIS-CAT Pro, you don't need to stop assessing your cybersecurity posture. You can continue to evaluate your systems and data to identify how you can continue to grow.

Take CIS CSAT Pro. It lets you prioritize your implementation of the Controls, which are themselves prioritized into three Implementation Groups (IGs). If you're new to the Controls, you can begin by enacting Implementation Group 1 (IG1) and laying a foundation of essential cyber hygiene in the process. From there, you can use CIS CSAT Pro to work your way through relevant CIS Safeguards in Implementation Group 2 (IG2) and Implementation Group 3 (IG3) in a way that works with your security requirements, your evolving technology, and the changing threat landscape facing your organization.

CIS-CAT Pro provides similar functionality. Each scan yields insight into how you can harden the settings of your operating systems in ways that will more closely align them to the security recommendations of the CIS Benchmarks and to your unique needs. CIS Benchmarks come in three different configuration profiles – Level 1 (base hardening), Level 2 (for defense-in-depth), and versions that include all recommendations set forth in the Defense Information Systems Agency Security Technical Implementation Guides (DISA STIG). As a result, you can use CIS-CAT Pro to gauge your hardening efforts based on the level of security you need for each of your systems.

4 Engaging the Team and Stakeholders

Finally, you can use the functionality of CIS CSAT Pro and CIS-CAT Pro to engage your team and stakeholders ahead of the next audit. CIS CSAT Pro enables you to assign implementation tasks to your team members and communicate timelines to your stakeholders so that everyone can collaborate on preparing for the next audit. Along those same lines, CIS-CAT Pro comes with a Dashboard component that graphically displays your scan results over a recent period of time. You can use these results to coordinate with team members, frame your results and goals in a business context, seek executive buy-in for future hardening, and map out the next steps for securely configuring your systems.

CIS-CAT Pro comes with a Dashboard component that graphically displays your scan results over a recent period of time. You can use these results to coordinate with team members, frame your results and goals in a business context, seek executive buy-in for future hardening, and map out the next steps for securely configuring your systems.

Assessments and Governance Audits: A Symbiotic Relationship

Assessments are a vital tool in the governance toolbox. They unlock the full potential of audits by revealing risks, verifying compliance and effectiveness, facilitating continuous improvement, and promoting a culture of accountability. Essentially, they transform audits from a necessary obligation into a strategic asset. By understanding the symbiotic relationship between assessments and audits, you can leverage both to their full potential, achieving compliance, improved governance, reduced risk, and enhanced performance along the way.

To-do List

- ☐ See that governance consists of two components: assessments and audits.
- ☐ Use a CIS SecureSuite Membership, specifically CIS CSAT Pro and CIS-CAT Pro, to take a strategic approach to your audits.
- ☐ Determine which CIS Safeguards and CIS Benchmarks recommendations you still need to implement.
- ☐ Reduce manual (and duplicated) effort complying with standards and frameworks that are relevant to your organization.
- ☐ Conduct ongoing assessments to move through the IGs and to improve your conformance score in the CIS-CAT Pro HTML output report.
- ☐ Assign implementation tasks and use graphic representations to enlist the support and buy-in of both team members and stakeholders.

Step 4

Quantitative Risk Analysis: Its Importance and Implications

In an increasingly volatile, uncertain, complex, and ambiguous (VUCA) world, you must take the time to address risk as a business issue and not treat it as something that can be ignored. A critical part of this ongoing process is risk analysis. While there are several methods for approaching risk analysis, quantitative risk analysis stands out as it is both precise and objective. In this section, we'll explain what quantitative risk analysis entails and and why it is so important.

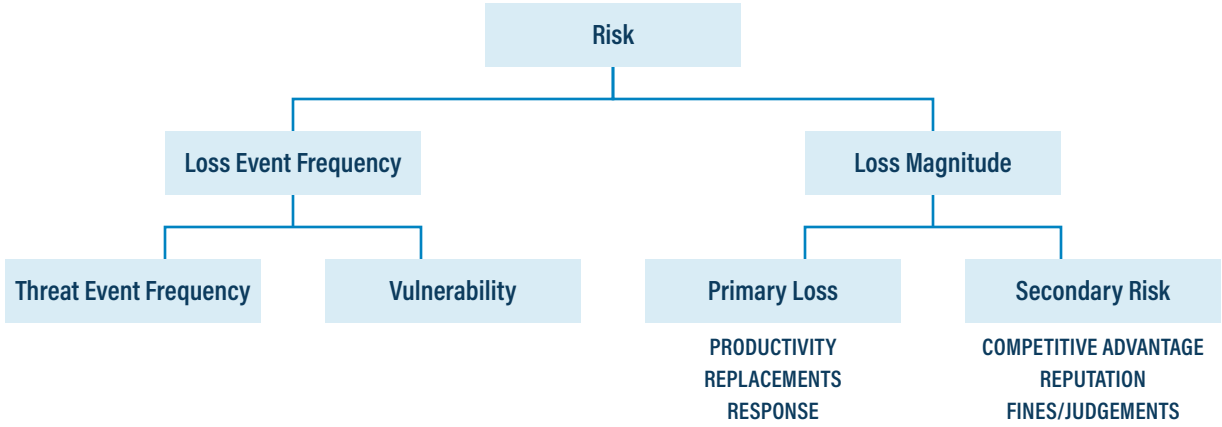
You must take the time to address risk as a business issue and not treat it as something that can be ignored.

Understanding Quantitative Risk Analysis

Quantitative risk analysis is a statistical technique for understanding financial uncertainty or risk in a project or business venture. It uses numerical values and complex data to determine the probability of a specific event and the potential impact that event could have on the organization.

This method involves collecting data about specific, measurable quantities of risk using mathematical models and simulations to analyze them. From there, you can forecast the probability of various outcomes, including the best-case and worst-case scenarios.

The following flow chart provides a helpful example. As explained by the Factor Analysis of Information Risk (FAIR) Institute, the financial value you assign to a specific risk depends on the loss event frequency, which is the time frame during which someone like a cyber threat actor (CTA) could affect an identified asset; and the loss magnitude, which encapsulates the losses that could stem from the loss event. Loss event frequency breaks down even further into threat event frequency, which is the number of attempts a CTA could try to target an asset, and vulnerability, which represents the percentage of threat events that turn into loss events. Similarly, loss magnitude breaks down into primary losses (such as productivity declines, the cost of replacements, and response times) and secondary losses (such as missed competitive advantages, reputational damages, and fines/judgments).



Source: FAIR Insitute

The Importance of Quantitative Risk Analysis

Below are some general benefits of using quantitative risk analysis in your organization:

Provides Numeric Data. Unlike qualitative risk analysis that uses judgments, intuition, and ordinal scales (e.g., high, medium, low), quantitative research relies on empirical assessments to provide specific numeric values associated with risk. It's about fostering consistency around numbers and complex data. We have to build up our capability in FAIR analysis and use it to continuously assess internal capability, as an example, so we start out with a major risk, address the adaptation of the qualitative assessment, and transfer it to quantitative.

You can do this sequentially. Start by understanding to which quantitative framework your organization aligns. Next, get the necessary education to implement the framework properly in context with your organization's missions and goals. You can then start small and expand. This is not a "one size fits all" effort; it will take time and patience to build and operate. As you build competency and your organization understands the approach, you remove the complexity of the process, enabling you to ultimately face more complex risks.

Facilitates Objective Decision-Making. Quantitative risk analysis eliminates ambiguity and facilitates more objective decision-making by providing a clear, numeric picture of the risk landscape. It reduces the element of subjective bias that can be associated with qualitative methods, leading to more rational and robust decisions.

Helps in Risk Prioritization. Quantitative risk analysis assists in prioritizing risks based on their potential impact on your organization's objectives. Quantifying risks enables you to focus your resources on the most significant risks first, ensuring a more efficient and effective risk management strategy.

Enables Financial Planning. This method also assists in financial planning by quantifying the potential impact of risks. It can help determine the contingency reserves needed for identified risks and supports cost-benefit analysis for proposed risk mitigation strategies.

Enhances Stakeholder Communication. Quantitative risk analysis provides a common language of 'numbers' that enhances stakeholder communication. It allows for clear, precise communication about risks and their potential impacts, which can help gain stakeholder buy-in for necessary risk management actions. Numbers will be the starting domino in securing that buy-in. It's followed by the assessment of the risk with factual statements of treating the risk. If you address specific risks early, you will help to ensure a greater return on treating the risk. Therefore, it is the opening line for organizational review.

Supports Continuous Risk Monitoring. Finally, quantitative risk analysis supports continuous risk monitoring by providing a baseline for comparison as new data emerges. This can help you to identify trends, track risk mitigation effectiveness, and support adjustments to risk management strategies as needed.

CIS RAM: A Quantitative Risk Analysis Tool in Your Toolbox

As discussed above, you can revolutionize the way your organization measures and addresses risk by embracing quantitative risk analysis. You just might not know how to get started.

CIS SecureSuite can help you. It provides you with benefits, resources, and tools that you can use to plan out and build upon your implementation of security best practices, including the CIS Critical Security Controls (CIS Controls). The same goes for your use of the CIS Risk Assessment Method (CIS RAM) v2.1, a free tool that enables anyone to evaluate their cybersecurity posture against the CIS Controls using quantitative risk analysis.

Take the pro version of our CIS Controls Self Assessment Tool (CIS CSAT Pro) as an example. Using CIS CSAT Pro, you can plan out which CIS Controls and CIS Safeguards you want to implement in support of your security requirements. You can then refer to CIS RAM v2.1 to understand how the security measures you've identified will help to manage the underlying risk you're seeking to address. (In doing so, you'll create documentation that you can use to demonstrate that you took "due care" around your risks.) From there, you can return to CIS CSAT Pro and use it to plan out implementation efforts, assign tasks to your team members, track their progress, and plan for the next round of implementation — all the while guided by the quantitative risk analysis inputs of CIS RAM v2.1.

Using CIS CSAT Pro, you can plan out which CIS Controls and CIS Safeguards you want to implement in support of your security requirements. You can then refer to CIS RAM v2.1 to understand how the security measures you've identified will help to manage the underlying risk you're seeking to address.

One Side of the Risk Analysis Coin

In the realm of risk management, quantitative risk analysis offers an objective, data-driven tool for understanding, prioritizing, and managing risk. By leveraging this approach, you can deepen your knowledge of your risk landscape, make more informed decisions, and ultimately enhance your resilience in uncertainty.

Even so, it's worth noting that quantitative risk analysis does not replace qualitative risk analysis but rather complements it. When used together, both provide a comprehensive view of your organization's risk environment, offering a solid foundation for effective risk management. Qualitative risk analysis takes into account factors such as geo-political environments, human capital, and reputational. Not every risk is calculatable in terms of the cost to the organization, after all. Context matters here, as well—quantitative and qualitative both have their own strengths and weaknesses.

It is up to the team to decide how you will balance quantitative and qualitative risk analysis in a way that will provide you with better data on making risk-based decisions and reviewing controls. In an uncertain world, this comprehensive, tailored approach to risk analysis is a necessity, not a luxury.

To-do List

- ☐ **Review the five factors that make quantitative risk analysis an important tool in your risk management toolbox.**
- ☐ **Use a CIS SecureSuite Membership, specifically CIS CSAT Pro, together with CIS RAM v2.1 to perform quantitative risk analysis and implement measures to mitigate your risks.**

Step 5

FAIR: A Framework for Revolutionizing Your Risk Analysis

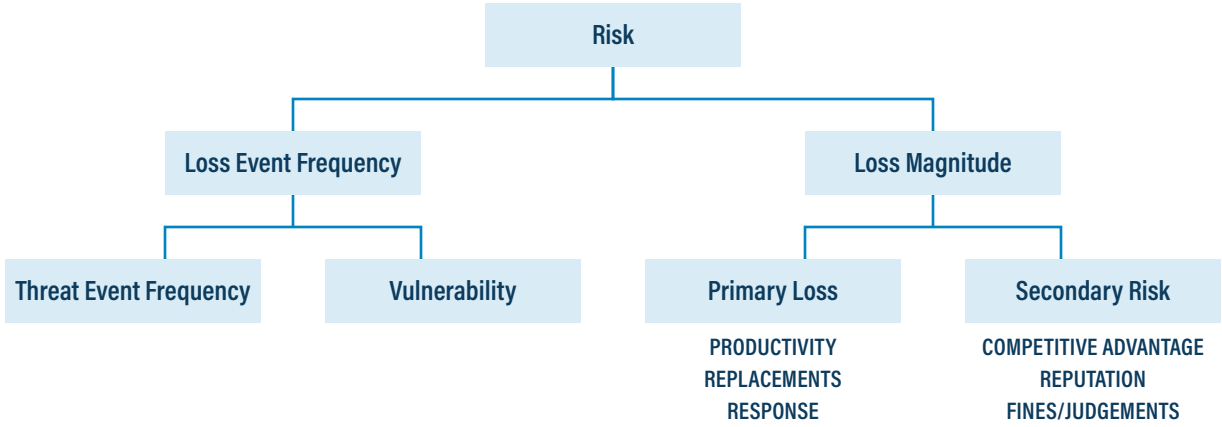
In risk management, understanding the landscape of risks, their potential impact, and the likelihood of their occurrence is the first line of defense. Many frameworks exist to aid this analysis, but the Factor Analysis of Information Risk (FAIR) has emerged as a leading methodology for quantifying and managing information risk.

In this section, we'll provide an overview of how FAIR works, discuss some of the ways in which FAIR's methodology revolutionizes risk analysis, and describe how a CIS SecureSuite Membership fits into the FAIR model.

Understanding FAIR

FAIR is a standard quantitative framework for understanding, analyzing, and quantifying information risk in financial terms. Unlike traditional risk assessments which focus on qualitative measures (e.g., high, medium, low), FAIR provides metrics about dollars and cents. In doing so, FAIR gives you a common language by which you and other stakeholders can understand what a risk means to your organization.

At a high level, FAIR's model helps you to understand the probability and magnitude of loss tied to a potential risk event. As I discussed in a blog post, the FAIR model assigns a financial value to the risk based upon two factors: the loss event frequency, or the time frame during which a cyber threat actor (CTA) could affect an identified asset; and the loss magnitude, or the losses that could stem from the loss event. Both loss event frequency and loss magnitude also break down into subcategories that enable a detailed, nuanced understanding of risk. For instance, the former comprises threat event frequency, or the number of attempts a CTA could try to target an asset, and vulnerability, or the percentage of threat events that turn into loss events. Meanwhile, the latter encapsulates primary losses (such as productivity declines, the cost of replacements, and response times) and secondary losses (such as missed competitive advantages, reputational damages, and fines/judgments).



Source: The FAIR Institute

Threat event frequency, vulnerability, and secondary losses also have their own subcategories. You can learn more with this full view of FAIR's risk analysis methodology.

Why FAIR Is Revolutionary for Risk Analysis

1 Emphasis on Quantitative Data

FAIR's primary strength lies in its ability to quantify risk. Expressing risk in financial terms enables you to make more objective and rational decisions. This quantitative data can be integrated into broader financial analysis, enhancing overall strategic planning and decision-making.

2 Prioritizing Risks Efficiently

By quantifying risks, FAIR enables you to compare and prioritize them based on potential financial impact. This allows for a more efficient allocation of resources, targeting the troubles with the most significant potential for harm.

3 Enhanced Communication

Expressing risk in financial terms enhances communication with stakeholders. It provides a common language that bridges the gap between technical risk experts and business executives. This can improve decision-making and buy-in for risk mitigation strategies.

Other means of risk analysis don't provide this level of communication. For instance, qualitative risk analysis doesn't provide actionable or prioritized input that organizations need to effectively address risk within their environment. It gives a general impression that can guide decision-making around risk, but those decisions reflect the level of context that you have around a particular risk. To see this in action, you can review the "bald tire scenario."

4 Facilitating Risk Transfer Decisions

With a clear understanding of the potential financial impact of risks, you are better equipped to make decisions about risk transfer. This is where you make a business agreement to pay/contact/direct another to take responsibility for mitigating a risk. As an example, you transfer your risk when you purchase any type of insurance. The key is to ground your risk transfer considerations on a solid foundation of what the risks mean to you. That way, you'll ensure that your decisions are cost-effective and aligned with your organization's risk tolerance.

The key is to ground your risk transfer considerations on a solid foundation of what the risks mean to you. That way, you'll ensure that your decisions are cost-effective and aligned with your organization's risk tolerance.

5 Supporting Continuous Improvement

FAIR encourages an ongoing risk analysis process, with regular updates as new data becomes available. This supports continuous improvement, enabling you to adapt your risk management strategies in response to evolving circumstances.

CIS SecureSuite: The Natural Complement to FAIR

By now, you know about the advantages of using FAIR's model to understand your risks. However, you might not know how to start applying FAIR's quantitative risk analysis to your own organization.

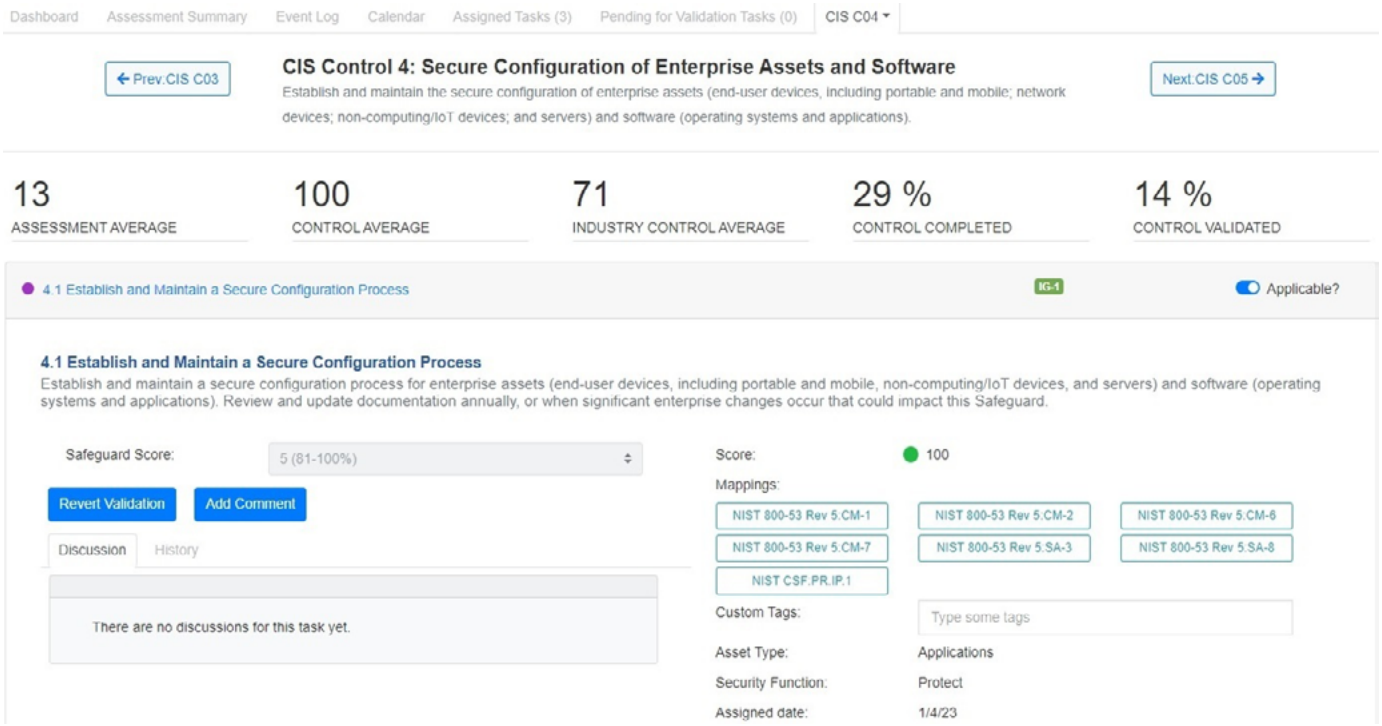
This is where a CIS SecureSuite Membership comes in. It provides benefits, tools, and resources that you can use to strengthen your cybersecurity posture by implementing CIS security best practices. Among them

are the pro version of our CIS Configuration Assessment Tool (CIS-CAT Pro) and the pro version of our CIS Controls Self Assessment Tool (CIS CSAT Pro). Both can help you better understand and contextualize your risks in accordance with the FAIR model. Let's explore a few examples below.

Insight into Quantitative Data. Using CIS CSAT Pro, you can track your implementation of the CIS Critical Security Controls (CIS Controls) at the level of individual CIS Safeguards. You can leverage such insight to determine your progress in implementing all of the Safeguards of a single Control or all of the Safeguards of an Implementation Group (IG). This gives you an understanding of where you are in the process of managing a certain risk.

It's a similar story with CIS-CAT Pro, which enables you to conduct automated scans of your systems' settings against the secure recommendations of the CIS Benchmarks. Each scan yields an HTML report, which includes a percentage that demonstrates your scanned system's conformance to the corresponding CIS Benchmark's guidance. This score quantifies to what extent your hardening efforts on your system fulfill a CIS Benchmark configuration profile, whether that be base-level (Level 1), defense-in-depth (Level 2), or those of the Defense Information Systems Agency Security Technical Implementation Guides (DISA STIGs).

Communication Around Prioritized Risks. The FAIR model emphasizes the importance of communicating with stakeholders about risk analysis and prioritizing risks accordingly. The same can be said about CIS CSAT Pro. It's designed to help you prioritize your implementation of the Controls from the level of individual Safeguards. With this view of your efforts, you can plan to apply all the Safeguards of an IG that match your cybersecurity maturity. You can also look to implement all the Safeguards of a Control depending on your unique security requirements and risk mitigation priorities.



A screenshot of CIS CSAT Pro showing the completion percentage of CIS Control 4: Secure Configuration of Enterprise Assets and Software.

As part of this prioritization process, you can work with your team members and other stakeholders to assign tasks for each implementation effort. Such a collaborative process enables you to streamline your communication with stakeholders around mitigating cybersecurity risk. Similarly, it improves visibility around outstanding actions, thereby creating accountability for cyber defense across the organization.

A Toolbox for Continuous Improvement. Risk analysis means nothing if you can't adapt and improve your understanding of your risks over time. CIS CSAT Pro and CIS-CAT Pro support this viewpoint. The former helps you to track your efforts so that you can move through the IGs of the Controls, growing your cybersecurity maturity along the way. Similarly, CIS-CAT Pro comes with a Dashboard component that displays your scanning results over a recent period of time. You can use these results to understand your systems' conformance to the CIS Benchmarks, including how you've improved and where you still need to go.

Enhancing Your Risk Analysis Program with FAIR

The FAIR model offers a paradigm shift in risk analysis, moving the focus from a subjective to a quantitative understanding of risk. While it may not replace other risk analysis forms, it provides another analysis capability for your organization to enhance your decision-making. It requires understanding the context of the business, gauging control depth, and adding a reality check to the number so that the calculations are not the one area assessed in risk management. By integrating FAIR into your risk management approach, you can achieve a more robust, objective, and practical understanding of your risk landscape.

Just remember that FAIR, like any model, is not a panacea. It is most effective when used as part of a broader risk management strategy, incorporating quantitative and qualitative analysis methods. Nevertheless, the value of FAIR in revolutionizing risk analysis is undeniable. It is well worth considering for your organization as you seek to enhance your approach to managing risk in today's uncertain world.

To-do List

- ☐ **Learn the elements that the FAIR methodology uses to assign a financial value to a risk. Use a CIS SecureSuite Membership, specifically CIS CSAT Pro and CIS-CAT Pro, to align withthe FAIR methodology.**
- ☐ **Determine which CIS Safeguards and CIS Benchmark recommendations you've implemented across your systems and environment.**
- ☐ **Use CIS CSAT Pro to assign implementation tasks to your team members and communicate the status of these tasks to stakeholders.**
- ☐ **Plan which Safeguards and Benchmark recommendations you plan to enact over the next 3-6 months.**

Step 6

Congratulations, You're Compliant: Charting Your Path Ahead

Navigating the labyrinth of compliance requirements is no small feat, so congratulations if you've recently achieved compliance with a particular standard or regulation! But achieving compliance is a continuous review, adjustment, and improvement cycle. What comes next after you've achieved compliance?

In this section, I'll point out seven things that you can do to capitalize on your compliance achievement. I'll also discuss how you can use the benefits, resources, and tools of a CIS SecureSuite Membership as a toolbox to help you along the way.

1 Celebrate Your Achievement

First and foremost, take a moment to appreciate your team's hard work and dedication. Compliance isn't achieved in isolation; it's a team effort involving collaboration across your organization. Celebrating this achievement fosters a positive organizational culture and motivates your team for the next phase of the journey.

2 Communicate Your Success

Compliance isn't just an internal affair. It matters to your stakeholders, too. Your customers, partners, and investors want the assurance that you're committed to good governance, and achieving compliance provides that assurance. Be sure to communicate your success to your stakeholders, demonstrating your ongoing commitment to quality, security, and privacy depending on the compliance standard you've achieved.

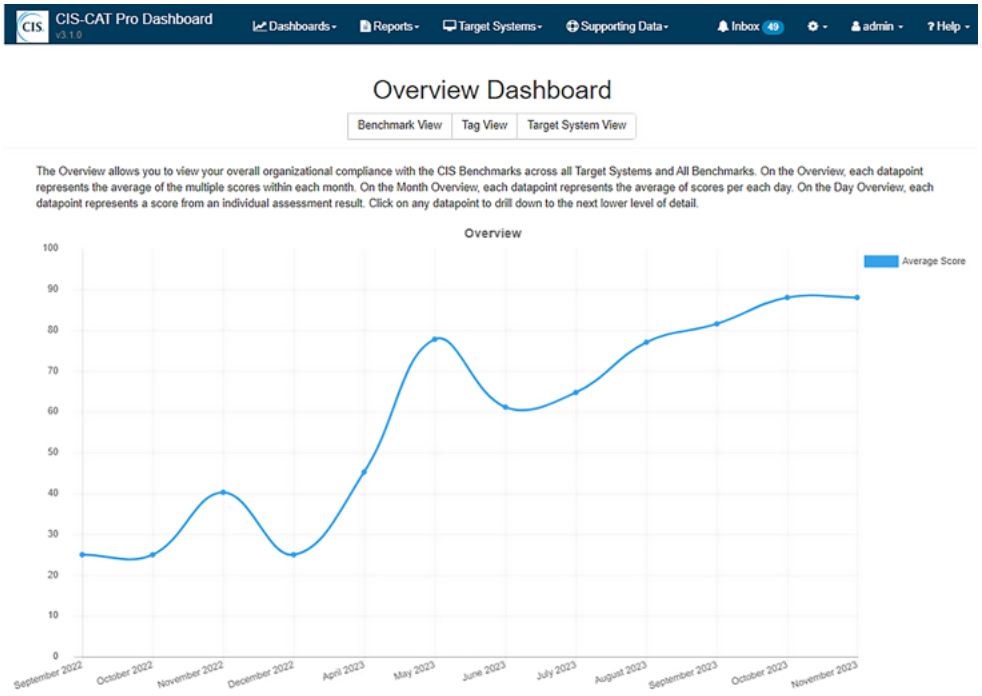
Quick Tip

One of the ways you can communicate success is to create a Trust and Security Center on your website. Its purpose is to illustrate your certifications and FAQs so that everyone — stakeholders, customers, and external visitors alike — can view your compliance and privacy achievements.

3 Monitor Continuous Compliance

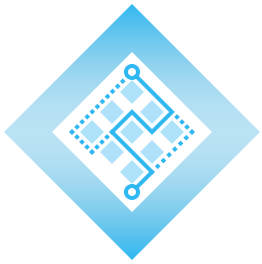
Achieving compliance is one thing; maintaining it is another. This is because environments change both from a physical and technological perspective. Every change to the environment modifies the level of compliance you've achieved. As such, you need to make compliance an ongoing effort.

Regular monitoring is crucial to ensure that you continue to meet compliance requirements. This could involve regular audits, reviews, and reporting to ensure your controls remain effective and meet compliance requirements.



A screenshot of CIS-CAT Pro showing conformance to a CIS Benchmark over the span of a year.

That's the philosophy behind the pro version of our CIS Configuration Assessment Tool (CIS-CAT Pro). Included in a CIS SecureSuite Membership, CIS-CAT Pro comes with two components, an Assessor and a Dashboard, that support you in conducting automated scans of your systems' settings against the secure recommendations of the CIS Benchmarks. The Dashboard component graphically displays your scanning results over a recent period of time. With that information, you can visualize the impact of your hardening efforts on each system and plan out what you need to do to meet your security requirements on an ongoing basis.



4 Plan for the Next Audit

While celebrating your current achievement, remember that the next audit is just around the corner. Begin planning for it early, considering any changes in your business operations or the regulatory environment that could affect your compliance status. Be proactive in identifying and addressing potential issues before your next audit. Also, make sure to review the audit requests and identify gaps that are not currently identified in your control set.

5 Identify Opportunities for Improvement

Even though you've achieved compliance, there are likely still areas where you can improve. Use the insights gained from your compliance process to identify these areas and develop a plan to address them. This could involve enhancing your controls, improving your processes, or investing in modern technologies to increase efficiency and effectiveness.

This is another area where a CIS SecureSuite Membership can help. Specifically, the pro version of our CIS Controls Self Assessment Tool (CIS CSAT Pro) helps you to track your implementation of the CIS Critical Security Controls (CIS Controls). You can use CIS CSAT to plan your journey through the different Implementation Groups (IGs) of the Controls by reviewing which individual CIS Safeguards you've implemented and which ones you'd like to prioritize toward strengthening your cyber defenses.

6 Expand Your Compliance Program

Once you've achieved compliance with one standard or regulation, consider whether there are other areas where you should seek to achieve compliance. Expanding your compliance program can further strengthen your governance and risk management practices and provide additional assurance to your stakeholders.

Once again, a CIS SecureSuite Membership can assist you with this step. Both CIS CSAT Pro and CIS-CAT Pro are designed to help you streamline your implementation of the CIS Controls and CIS Benchmarks. These security best practices map to numerous standards and regulations such that you can avoid duplicating effort. By implementing the Controls and Benchmarks, you'll save time and money on complying with multiple standards and regulations at once.

By implementing the Controls and Benchmarks, you'll save time and money on complying with multiple standards and regulations at once.

7 Foster a Culture of Compliance

Finally, continue to foster a culture of compliance within your organization. Compliance isn't just the responsibility of a single department or team — it should be embedded in the culture of your entire organization. Regular training, communication, and reinforcement can help to embed compliance into your organizational DNA.

Quick Tip

You can use newsletters, lunch and learns, and continuous training. Ongoing education will help you to create a security-first mindset and security-minded culture. By contrast, if you conduct training just once a year, your employees will quickly forget the importance of security and compliance until next year's training.

An Ongoing Commitment to Compliance

Achieving compliance is a significant milestone, but it's not the journey's end. By taking these steps after achieving compliance, you can ensure that your organization continues to benefit from your compliance efforts, maintaining a robust and effective governance and risk management program that stands up to scrutiny and delivers value for your stakeholders. Remember, compliance isn't just a box to be checked — it's an ongoing commitment to quality, security, and integrity.

To-do List

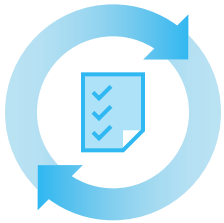
- ☐ **Commit to acting upon your compliance achievements using a CIS SecureSuite Membership. This includes the following:**
- ☐ **Leverage CIS-CAT Pro's Dashboard functionality to graphically display your system-hardening efforts.**
- ☐ **Plan out the next stage(s) of your CIS Controls implementation journey using CIS CSAT Pro.**
- ☐ **Review CIS's mapping and compliance guidelines to save time, money, and duplicated effort on fulfilling your compliance obligations.**

Step 7

How to Build a Robust Continuous Audit Program

In an increasingly dynamic and complex business environment, periodic audits don't provide timely insights for your organization to navigate risks effectively. A continuous audit program can help by offering a near real-time assessment of your organization's operational and financial performance as well as identifying control deficiencies, potential fraud, and compliance issues. But how can you build an effective continuous audit program?

In this section, I'll discuss 10 steps that you can use to build a robust continuous audit program at your organization. I'll also note how the benefits, tools, and resources of a CIS SecureSuite Membership can help you along the way. Let's get started.



1 Understand the Basics of Continuous Auditing

Continuous auditing involves the frequent or real-time assessment of your organization's operations. This doesn't mean that you need to conduct an audit every day. Instead, it's about using automation to be proactive rather than reactive with your audits.

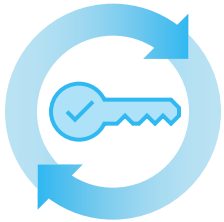
As such, continuous audits aren't the same as traditional audits. The latter involves assessing specific control requirements and technology to provide the information in a traditional sense, i.e., to store and curate the audit requirements. It also occurs annually or semi-annually.

By contrast, in continuous auditing, you use technology and tools as the assessment method to monitor processes and to understand if a control is effective. You benchmark the control to continually assess if its current condition fits within the corresponding control parameters. Understanding this shift from periodic to constant auditing is the first step in building your program.

2 Establish Your Objectives

Determine what you want to achieve with your continuous audit program. Is it to improve the effectiveness of your internal controls? Enhance compliance with regulations? Detect fraud more rapidly? Your objectives will guide the design and implementation of your program.

Not sure what your unique goals are? In general, you can use a continuous audit program to gain assurance of a control being sustainable over a period of time. Sustainability should be a reflection of the capability of the control and also its ability to manage risk. The data over time is a time series assessment of the effectiveness of the control. A continuous audit program also helps you to address exceptions to the control parameter and identify weak controls early, thus reducing the risk of exposure to a misaligned/configured control.



3 Assess Your Current Audit Process

Review your existing audit process to identify gaps and areas of improvement. Here are some ideas of where to look:

- **Current audit scope:** Are system assessments looking at all systems or just those defined as critical?
- **Method of assessment:** What timing requirement is in place? Is it just annual reviews? Should those be more often and/or take place after a major cyber event?
- **Sample size:** Does this change with growth or shrinkage within your organization?

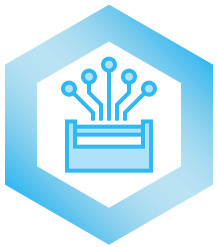
Consider the technologies, techniques, and resources currently in place and how you can leverage and/or enhance them for continuous auditing.

4 Define Key Risk Indicators

Identify the key risk indicators (KRIs) to be monitored through continuous auditing. These should align with your organization's risk appetite and strategic objectives. KRIs could include financial metrics, operational metrics, or other indicators of risk and performance.

Quick Tip

If you're looking to identify KRIs that matter to you, consider looking at risks that can be measured using the metrics discussed above along with a set of key tolerance/appetite values to measure against. Additionally, you'll want to ensure a consistent approach to measurement.



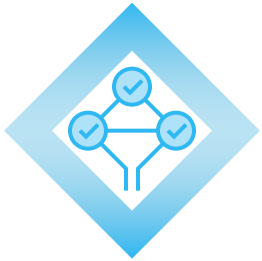
5 Leverage Technology in Your Toolbox

Continuous auditing relies heavily on technology. Automated data analysis tools, artificial intelligence, and machine learning can monitor large volumes of transactions and controls in real-time. Invest in technologies that align with your continuous audit objectives and capabilities.

This is where a CIS SecureSuite Membership can help. It enables you to streamline your implementation of security best practices by using resources such as the pro version of our CIS Configuration Assessment Tool (CIS-CAT Pro) and the CIS Build Kits. The former helps you to conduct automated scans of your systems' settings against the security recommendations of the industry-leading CIS Benchmarks. In this way, CIS-CAT Pro saves you time and money in visualizing the current state of your system hardening efforts.

From there, you can conserve even more effort by implementing one of our Build Kits. Available as Group Policy Objects (GPOs) on Windows devices and as Bash shell scripts on Linux machines, the Build Kits automate the "Remediation" section of the CIS Benchmarks. They're designed to help you apply all of the secure configurations of a Benchmark at once without having to manually apply the recommendations one by one.

Please note that your organization has unique needs and requirements, so the process of integrating technology like CIS-CAT Pro and the Build Kits into your processes will look different from another's journey. Say you're in a data-heavy industry such as eCommerce, for instance. It will be easy for you to build automated assessment tools into current processes. By contrast, if you're in a sector with less emphasis on data, you may have to adapt analytic and audit capabilities to find an approach that works for you.



6 Develop an Audit Plan

Outline your continuous audit plan, detailing the scope of the audit, the KRIs to be monitored, the technology and techniques to be used, and the frequency of reporting. Remember, continuous auditing doesn't mean continually auditing everything—it means auditing the right things at the right time.

You want to understand if your control is effective before an adversary tests it. The same thing with hygiene. You want to practice good hygiene now and not wait until it is too late. For example, you want to test your systems for up-to-date patches based on a known vulnerability. Having that assurance provides some respite against the exploitation of your systems. You want to know what patches are in place before a vulnerability is announced.

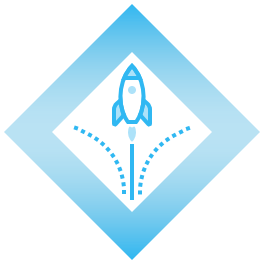
One of the ways you can practice good hygiene now is by downloading the pro version of our CIS Controls Self Assessment Tool (CIS CSAT Pro), another resource available through a CIS SecureSuite Membership. You can use CIS CSAT Pro to track and prioritize your implementation of the CIS Critical Security Controls (CIS Controls), including Implementation Group 1 (IG1)—the definition of essential cyber hygiene. With CIS CSAT

You can use CIS CSAT Pro to track and prioritize your implementation of the CIS Critical Security Controls (CIS Controls), including Implementation Group 1 (IG1)—the definition of essential cyber hygiene. With CIS CSAT Pro, you can map out a way to strengthen your defenses against common cyber threats in a way that works for you.

Pro, you can map out a way to strengthen your defenses against common cyber threats in a way that works for you.

7 Train Your Team

Your audit team will need the skills and knowledge to implement and manage the continuous audit program. This might require training in new technologies/techniques or bringing in new team members with specialized skills, including data analysis, red teaming skill sets, and skills on technologies that the organization is using.



8 Pilot and Refine

Before rolling out your continuous audit program organization-wide, consider piloting it in one area or process. This will allow you to refine your approach, troubleshoot any issues, and demonstrate the value of continuous auditing.

Quick Tip: If you're looking to create a pilot, start small and identify systems that will fit the paradigm of continuous assessment. This will help you to gain some wins in assessing how to scope the assessment of continuous control and use these as lessons for evolving the program. Continuous auditing is not a "big bang" approach.

9 Communicate and Collaborate

Continuous auditing can represent a significant change, so effective communication and collaboration are essential. Engage with stakeholders across the organization to explain the benefits of constant auditing, address any concerns—notably, the resources required to keep this program operational and the burden it imposes on systems, resources, and costing—and ensure everyone understands their role in the process.

Here's another place where a CIS SecureSuite Membership can help. Within CIS CSAT Pro, you can assign team members and stakeholders to different steps of an implementation task. That way, you can make sure that key individuals support your efforts to enact a CIS Safeguard and, by extension, contribute to your continuous auditing program over the long term.

10 Review and Adapt

Finally, remember that continuous auditing itself should be subject to constant improvement. Regularly review your program's effectiveness and adapt it as needed, considering changes in your business environment, risk landscape, and technological capabilities.

Continuous Auditing as a Journey

Building a continuous audit program is a journey that requires commitment, resources, and a willingness to adapt. However, the benefits—improved risk management, enhanced compliance, and better decision-making—can be significant. By following these steps, you can lay the foundation for a robust continuous audit program that drives value for your organization.

To-do List

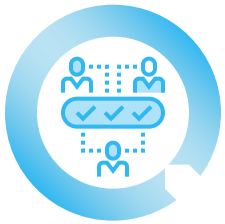
- ☐ **Leverage CIS-CAT Pro and the CIS Build Kits, two benefits of a CIS SecureSuite Membership, to automate your continuous audit journey where you can.**
- ☐ **Develop a plan to enact all the CIS Safeguards of IG1 with the help of CIS CSAT Pro.**

Step 8

Mitigation Strategies to Make the Most of Audit Results

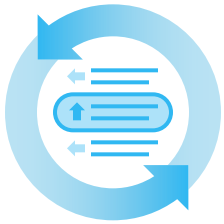
The auditing process, whether internal or external, can be daunting, but the implementation of audit findings truly makes a difference. If you don't act on your audit findings, your organization risks losing applicable certifications, suffering reputational damage, losing contracts, and incurring fines. How do you avoid these potential consequences?

In this section, I'll discuss six mitigation strategies that you can use to capitalize on your audit results. I'll also explain how you can use the benefits, resources, and tools of a CIS SecureSuite Membership to help you along the way.



1 Understand Your Audit Findings

First and foremost, it's crucial to understand your audit findings in detail. This goes beyond merely reading the audit report. Involve your team in discussions, delve into the data, and ensure that you fully comprehend the underlying issues. Understanding is the first step toward effective mitigation.



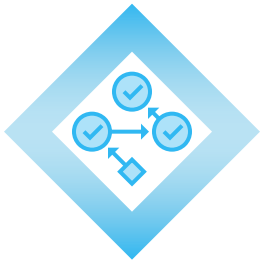
2 Prioritize Your Responses

Not all audit findings are created equal. Some issues may pose a significant risk to your organization, while others might be less critical. Prioritize your responses based on factors like potential impact, cost of mitigation, and alignment with your organization's strategic objectives.

To complete this step, you can use the pro version of the CIS Controls Self Assessment Tool (CIS CSAT Pro). This tool helps you track and prioritize your implementation of the CIS Critical Security Controls (CIS Controls), security best practices that strengthen your cyber defenses. With CIS CSAT Pro, you can use your audit results and security requirements to

Not all audit findings are created equal. Some issues may pose a significant risk to your organization, while others might be less critical. Prioritize your responses based on factors like potential impact, cost of mitigation, and alignment with your organization's strategic objectives.

identify specific CIS Safeguards that matter to your organization and determine which ones you want to implement first.

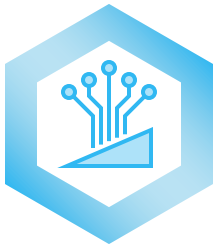


3 Develop an Action Plan

Once you have prioritized your responses, develop a clear and detailed action plan to address each issue. This should include specific steps, responsibilities, resources, and timelines. An action plan guides your mitigation efforts and demonstrates your commitment to addressing the audit findings.

This step is another opportunity for you to draw upon a SecureSuite Membership. In CIS CSAT Pro, you can create multiple users and assign them to tasks that support your implementation efforts. That way, you can make sure you hold team members, stakeholders, and others in your organization accountable to a defined action plan as you act upon your audit results.

In CIS CSAT Pro, you can create multiple users and assign them to tasks that support your implementation efforts. That way, you can make sure you hold team members, stakeholders, and others in your organization accountable to a defined action plan as you act upon your audit results.



4 Leverage Technology

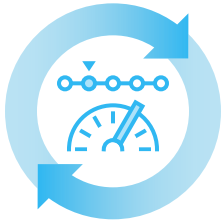
Technological tools can significantly enhance your mitigation efforts. For example, data analytics can provide deeper insights into issues, while automation can streamline processes and controls. Consider leveraging technology to address your audit findings and improve your overall operational efficiency.

At this point in the process, you can call upon two CIS SecureSuite resources: the pro version of our CIS Configuration Assessment Tool (CIS-CAT Pro) and the CIS Build Kits. With the former, you can conduct automated scans of your systems' settings against the secure recommendations of the CIS Benchmarks. CIS-CAT Pro thereby helps you to quickly determine whether you've hardened your systems against

guidelines developed by IT experts around the world using a consensus-driven process. If you choose, you can then implement the CIS Build Kits, which automate the "Remediation" section of the CIS Benchmarks. Available as Group Policy Objects (GPOs) for Windows devices and Bash shell scripts for Linux machines, the CIS Build Kits help you to implement all the recommendations of a Benchmark at once without any manual effort.

5 Foster a Culture of Continuous Improvement

Make the most of your audit results by fostering a culture of continuous improvement. Encourage your team to see audit findings as opportunities for learning and growth rather than criticisms or failures. This cultural shift can help ensure audit findings are addressed proactively and effectively.



6 Monitor Progress and Review Effectiveness

Finally, regular monitoring and review are essential to ensure that your mitigation strategies are effective. This involves tracking progress against your action plan, reviewing the effectiveness of implemented changes, and adapting your strategy as needed.

Here, you can deploy CIS-CAT Pro once again. Its Dashboard component enables you to visualize your scanning results over a recent period. With this insight, you can track the impact of your hardening efforts so that you can effectively act upon your audit results using secure configurations going forward.

Making Opportunities out of Challenges

Remember, audits are not just about identifying problems but about finding solutions. By implementing these mitigation strategies, you can transform your audit results from a challenge into an opportunity, driving improvement, enhancing risk management, and adding value to your organization. Make the most of your audit results. In doing so, you'll be able to turn insights into improvements to your cybersecurity posture as well as to your governance, risk, and compliance (GRC) program.

To-do List

- ☐ **Take the time to understand the nuances of your audit results and have conversations across your organization about the importance of acting on these results.**
- ☐ **Use the benefits of a CIS SecureSuite Membership to make the most of your audit results.**
  - ☐ **Use CIS CSAT Pro to prioritize which CIS Safeguards you can implement to strengthen your organization's cyber defenses.**
  - ☐ **Within CIS CSAT Pro, create and assign tasks to your team members so that they can effectively contribute to your action plan.**
  - ☐ **Automate and streamline where you can using CIS-CAT Pro and the CIS Build Kits.**
  - ☐ **Graphically monitor the progress of your system-hardening efforts with CIS-CAT Pro's Dashboard functionality.**

Conclusion

Sustainable governance, risk, and compliance isn't possible without a plan in place. CIS SecureSuite helps overcome this challenge with access to benefits, tools, and resources that help you to build a robust governance controls program, analyze your risks both quantitatively and qualitatively, establish a continuous auditing program, and act upon your audit results. In that way, you can continue to navigate the cybersecurity audit lifecycle and proactively keep up with the costs of change wherever your evolving business, regulatory, and customer demands take you.

Authors

Sean Atkinson
Chief Information Security Officer

Sean Atkinson is Chief Information Security Officer of CIS. He uses his broad cybersecurity expertise to direct strategy, operations, and policy to protect CIS's enterprise of information assets. His job responsibilities include risk management, communications, applications, and infrastructure. Prior to CIS, he served as the Global Information Security Compliance Officer for GLOBALFOUNDRIES, serving Governance, Risk and Compliance (GRC) across the globe.

Prior to GLOBALFOUNDRIES, Atkinson led the security implementation for the New York State Statewide Financial System (SFS) implementation from 2007 to 2014, and his last role and responsibility was as the Internal Control, Risk and Information Security Manager.

Atkinson was born in Brooklyn, N.Y. and lived in England for 18 years, graduating from Sheffield Hallam University in 2000. After moving back to the United States, he has pursued multiple degrees and certifications in the IT arena.

In addition to his work with CIS, Atkinson is also an adjunct professor of Computer Science at the College of Saint Rose.

Stephanie Gass
Director of Governance, Risk, and Compliance at CIS

Stephanie Gass is the Director of GRC for the Information Security and Privacy programs at CIS. She oversees external and internal audits along with efforts to ensure that CIS aligns to the CIS Controls v8, SOC 2 Type 2, ISO:IEC 27001/27701, NIST 800-171, and FISMA Moderate.

Prior to joining CIS, Stephanie was the US Information Security Officer and ITAR lead at GlobalFoundries, a global chip manufacturer.

Stephanie has a Master's Degree from George Washington University in Cybersecurity. She was the Lead and Contributing Author to *Managing Cyber Threats through Effective Governance: A Call to Action for Governors and Legislatures*. She also spoke about this topic at a recent MS-ISAC Annual Meeting.

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 Critical Security 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. election offices.

CIS® Center for Internet Security®

CIS SecureSuite®

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