tripwire by HelpSystems

WHITE PAPER

Mind the Cybersecurity Gap

Why Compliance Isn't Enough

FOUNDATIONAL CONTROLS FOR
SECURITY, COMPLIANCE & IT OPERATIONS

Foreword

Every organization wants to be secure in the long term, but compliance might order them to focus on implementing certain safeguards within a short period. Given this situation, some organizations might elect to focus on compliance now and look at security later. This might involve designating budget for compliance before allocating additional funds for security at some point in the future.

This approach can be a slippery slope. Compliance frameworks and standards are always changing. Subsequently, organizations might need to spend additional budget to align with those new versions each time they become publicly available.

Such an approach doesn't align with the interests of CISOs and other security leaders. Saving on costs is an important motivation here. On a related note, they want to keep things as simple as possible. They don't want to have their teams go out and baseline their systems for each set of standards and each framework that applies to their organization. They also don't want the burden of purchasing one compliance tool for Windows systems and another tool for Linux machines. They want to save that time and do it once for all their environments so that their personnel can focus on more important things such as responding to potential incidents.

The truth is that it can be this way. Organizations can avoid the vicious cycle of always being one step behind their ever-evolving compliance obligations and never giving enough attention to their security needs. By approaching both their security and compliance obligations through a security lens, organizations can save both time and money. The question is: how?

To find out, Tripwire reached out to multiple experts with insight into managing security and compliance programs. It asked them to share how they might use security to streamline both their compliance and security efforts. This white paper shares their recommendations. It also discusses how using a trusted security and compliance solutions provider like Tripwire can make things easier for organizations going forward.

Dean Ferrando
Systems Engineering Manager, EMEA Tripwire

Introduction

Compliance is a necessity so long as organizations want to avoid paying non-compliance fees. By contrast, security is optional—at least to the extent that they won't face any direct penalties for not securing their systems. That's not to say a lack of security won't cost them anything. Without security, organizations leave themselves exposed to a breach or a hack, security incidents which can damage their reputations, rack up legal fees from angry customers, as well as tie up IT and security personnel with time-consuming cleanups.

Organizations must create a partnership between compliance and security if they want to protect their systems and data. An either/or situation won't work. Today's technology solutions and digital threat landscape demand that organizations realize both using a robust security strategy.

Compliance, Security, and the Difference Between the Two

In the words of Gartner, compliance is "the process of adhering to policies and decisions." Organizations can create those policies using internal resources such as directives and procedures or by drawing from external laws and regulations. As such, compliance doesn't stay the same. Designating bodies update their standards periodically; organizations' hardening solutions and policies change. Compliance is simply a state at a given point in time.

Meanwhile, Gartner views security as "the combination of people, policies, processes, and technologies employed by an enterprise to protect its cyber and physical assets." Business leaders define optimal levels of security for their organizations. It's then up to technical teams to implement controls in support of those requirements.

"Security has at its core the themes of Confidentiality, Integrity, and Availability," (known as the CIA Triad) Stuart Coulson, a manager of business engagement, points out. "The implementation of security comes down to a technical team within the organization who puts in place appropriate controls to mitigate risks if one or more of those themes becomes compromised. The key word is 'appropriate'."

Compliance and security are not the same thing. The latter is rooted in the dynamic world of technology. This implies a continuous process of evaluating risks. "Security is about dealing with alerts consistently and as they show up, making sure that any risks opened up with business-as-usual activities are dealt with immediately rather than only being discovered during an annual scan," noted Dean Ferrando, EMEA systems engineering manager. In contrast, compliance lives in words of rules. And it takes a while to develop those guidelines or specifications.

Angus Macrae, a head of cybersecurity, agrees with this assessment. "Compliance is much more of a rigid, disciplined, point-in-time exercise that by its nature requires some longevity to make it worthwhile," he clarified. "It takes time, effort, and money for determining bodies to create, consult, and agree upon standards, publish accompanying guidance, and implement all the necessary accreditation processes to go with them. It likewise takes time, effort, and money for applicant organizations to become accredited with those standards, and they want to know that all that cost and effort won't simply be null and void a few months later."

Standards change, and new ones are emerging all the time. By the time an organization achieves compliance with a specific version of a set of standards, they might need to start again to comply with any changes that took effect in the meantime. Acknowledging this possibility, organizations could end up losing themselves in the accreditation process. At best, they might always be one step behind in their compliance journeys. At worst, they might develop a skewed picture of the digital risks confronting the business, leaving them exposed to attack.

"Being compliant limits your approach to security to the narrow confines of the standard you are using," noted Gary Hibberd, The Professor of Communicating Cyber at The Cyberfort Group. "Like looking through 'rose-tinted-glasses,' everything will appear okay because that is the lens you are using. But in fact, your approach could be one-dimensional and miss important aspects of cybersecurity. The result is that you may be compliant but not necessarily secure."

Key Challenges in Achieving Security and Compliance

Budgets

Organizations can run into issues when they don't balance budgets for compliance and security. While a large majority of compliance projects receive budget, security remains an afterthought. By contrast, compliance tends to get more of a share of budget even though failing to be compliant would result in a much smaller fine than the loss of revenue and/or reputation given a breach.

There's an interesting dichotomy with compliance. On the one hand, it is oftentimes too general in that it forces organizations with varying ways of doing business to adopt standards that fit the lowest common denominator of situations. On the other hand, it's too specific in that it only applies to certain environments, certain assets, and/or certain types of data. It's this specificity that prevents organizations from using different compliance obligations to achieve security, thus making budgeting even more of a challenge.

"Some compliance standards do not integrate with each other either, so it's possible to be fully compliant with one standard (e.g., Cyber Essentials) but still be way off other regulations and standards (ISO2700x)," Stuart Coulson stated. "Equally likely is that you can try to cover multiple compliance requirements, only to find you've duplicated your efforts and unnecessarily drawn down on your internal resources to provide evidence. So, my first point is that compliance is not coordinated. It's so hard to ensure you are fully compliant."

Audits

Just as compliance frameworks can fail to account for different business models, so too can auditors overlook what's important to certain organizations.

"I have a long debate with auditors about 'enforcement of a clear desk,'" Christian Toon, a CISO, cites as an example. "Paper is far from dead in many organizations. Even with significant technical, administrative, and physical controls, it's just not on our agenda to 'clear a desk,' and that's been sufficiently documented with the appropriate business and client approvals. Yet there are still auditors chasing full compliance to this."

That's assuming organizations understand what they need to do to pass an audit in the first place, as it's not always clear whether standards are mandatory or advised. Some frameworks include sentences that use "must" and "shall" to emphasize the need for organizations to implement certain controls. Others lack that verbiage and read more like helpful security governance documents filled with recommendations, while others still explicitly refer to only some measures as real and enforced. The latter are the most misleading, as they force organizations into a position where they need to interpret which measures are required and which are optional. Subsequently, organizations might waste time and money on working towards a perceived state of compliance that doesn't actually cohere with the intent of a specified framework.

Risk Management

Organizations are concerned with the following question: "How much risk is tolerable?" The issue is that compliance doesn't necessarily involve robust risk management. Here's Sarah Clarke, a security governance, risk, and compliance specialist, with more on this challenge.

"Compliance efforts are too often aimed at just securing cyber insurance or dealing with regulated industry customers instead of understanding risk," she said. "The disconnect between the compliance line and a robust threat and risk assessment can result in significant levels of misinformed spending. Not only that, but continuing immaturity in risk management also affects most businesses. (It is still incredibly tough to draw a useful line between an implemented measure and a movement in the assessed risk position.) In short, compliance is transient comfort, while robust risk management is persistent (but better informed) discomfort."

Of course, risk management doesn't extend just to one's own systems. In the age of incidents like SolarWinds and ProxyLogon, organizations also need to concern themselves with evaluating third-party vendors for risks. Many compliance frameworks don't require this function, however. Such an oversight creates a false sense of protection—even in situations where organizations have implemented all the required controls.

Checkbox Compliance

Many organizations practice what's known as "checkbox compliance." This is where they implement what's necessary in a compliance framework not because they see any value in it but because they are mandated to do so in order to trade with other organizations. They tick off the required policies and use those compliance efforts to claim that they're secure and protected against a variety of threats.

This is problematic for a few reasons. First, no compliance framework is comprehensive—or an accurate representation of what organizations are deploying across their entire networks, for that matter. That's because technology and the digital threat landscape are always changing. "Due to the changes in technology, one limitation of compliance is that it does not align or lags behind the latest trends in cybersecurity," agreed Caryll Arcales, a global security specialist.

Second, checkbox compliance sends a specific kind of message. Organizations essentially tell regulators that they understand the importance of security but are just unwilling to prioritize it. So, they'll just do certain measures and nothing else. This limits organizations' ability to explain what they've implemented and why to regulators and/or customers in the event of a breach.

How Organizations Can Overcome These Challenges

First and foremost, organizations need to recognize the limits of compliance. They need to see compliance standards as lowest common denominators—helpful but not comprehensive.

"Compliance tries to help in considering areas that could be of concern," Dean Ferrando concedes. "This is OK for the generic organization, but what about bespoke devices, multi geo connectivity restrictions, translation tools, and other areas that are specific to an organization that the compliance framework does not consider? It just doesn't account for all possible use cases."

With this understanding, organizations can get more strategic with their compliance efforts. Stuart Coulson put it a different way. "Don't do compliance for compliance's sake," he warned. "Instead, ensure you work to meaningful outcomes and seek improvements. Compliance comes with a cost, so make sure you emphasize return on investment."

When done in this way, compliance can add value to the business. The same is true of security. This presents organizations with an opportunity with which they can pursue both compliance and security at the same time, not either/or.

"Whilst there are certainly gaps and differences in thinking, this doesn't make the two things incompatible," noted Angus Macrae. "It just means that at times, you must view security and compliance as slightly different journeys to a similar destination. Compliance is a good way of otherwise disparate parties demonstrating to each other that they have the commitment to meet certain non-negotiables with a similar if not equivalent level of rigor. This can then form the first pillars of credible trust."

Organizations can create those pillars of credible trust by using the CIS Controls to drive both their compliance and security efforts. The CIS Controls are unique in that they map into a number of different compliance frameworks and simultaneously act as security guidelines. Hence, organizations can use those standards to perform double duty.

The CIS Controls represent just one way by which organizations can approach compliance within the bounds of a robust internal security program.

"A thorough business impact analysis and risk assessment with your security team and senior teams should identify your threat landscape and go some way to identify your control requirements," explained Christian Toon. "In doing so, you create your own control framework. This is what makes the difference. It's relevant to the organization, so this is what your teams get behind. Your narrative changes from 'We need to do this for the standards or legal requirements' to 'We're doing this for us because this is what we expect and who we are.' This creates a more visceral response, a sense of purpose that all people will buy into." That buy-in won't be forthcoming unless security teams lay the groundwork. In those situations, the security basics can be particularly useful.

For Sarah Clarke, there's no fundamental control more useful than creating

Relevant Security and Compliance Standards Overview

- **UK GDPR:** This law entered into force on January 1, 2021. It's based on the European Union's General Data Protection Regulation (EU GDPR), which took effect several years prior, though it does reflect certain changes to make EU GDPR work in a UK context.
- **DPA 2018:** The Data Protection Act (DPA) 2018 outlines a framework for data protection in the United Kingdom. It replaces the Data Protection Act 1998, and it both sits alongside and supplements the UK GDPR.
- **Cyber Essentials:** Driven by the National Cyber Security Centre (NCSC), Cyber Essentials is a certification program that UK organizations can use to protect the confidentiality, integrity, and availability of their information against digital threats.
- **GDPR:** Short for the General Data Protection Regulation, GDPR is a European Union law that creates a single data protection regime across 28 EU member states.
- **PCI DSS:** The Payment Card Industry Data Security Standard (PCI) consists of 12 high-level requirements for protecting information in organizations' cardholder data environments (CDEs). Each high-level requirement consists of low-level requirements, and each one of those leverages one or more testing procedures.
- **HIPAA:** The Health Insurance Portability and Accountability Act, HIPAA is a regulation that outlines data privacy and security provisions with which organizations must comply to safeguard healthcare information.
- **CIS Controls:** Developed by the Center for Internet Security, these Critical Security Controls consist of 18 top-level security measures along with supporting Safeguards that organizations can use to defend themselves against some of the most pervasive attacks in the threat landscape today.
- **ISO 27001:** This standard uses a top-down, risk-based approach to information security management systems. It's not technology-specific. But it does dive into the specifics of security techniques like password management.
- **SWIFT:** Short for the Society for Worldwide Interbank Financial Telecommunications, SWIFT is a messaging system that facilitates the exchange of information such as money transfer instructions between banks and other financial institutions.
- **BSI IT-Grundschutz:** Developed by Germany's Bundesamt für Sicherheit (BSI), IT-Grundschutz offers organizations with a systematic approach to ISO 27001. It provides information that suits anyone from CISOs at large enterprises to security personnel working at small- to medium-sized businesses (SMBs).
- **IEC 62443:** Initially created for organizations with industrial processes, IEC 62443 is a standard through which organizations can take a risk-based approach to securing their industrial automation and control systems (IACS).
- **Basel III:** The Basel Committee on Banking Supervision created Basel III following the financial crisis of 2007-09. The set of measures are designed to help banks strengthen their risk management, supervision, and regulation efforts.
- **SOX:** Short for the Sarbanes-Oxley Act, SOX has security implications for companies. In particular, Sections 302, 404, and 409 reference internal controls, governance, and disclosure for organizations' information security programs.
- **NCA:** The NCA refers to the National Cybersecurity Authority, or the government entity in charge of cybersecurity in Saudi Arabia. The entity created the Essential Cybersecurity Controls (ECC) to provide national organizations with minimum security requirements.
- **CSCC:** NCA developed the Critical Systems Cybersecurity Controls (CSCC) as an extension of and complement to the ECC. CSCC consists of 32 main controls and 73 subcontrols that address cybersecurity governance and defense, among other domains.
- **CCC:** Functioning as another extension of and complement to the ECC, the Cloud Cybersecurity Controls (CCC) consist of 37 main controls and 96 sub-controls that apply to Cloud Service Providers (CSPs) along with 18 main controls and 26 sub-controls that pertain to Cloud Service Tenants (CSTs).

an asset inventory. "My first focus is to descope low-risk assets and systems," she pointed out. "A defensible and documented process to do that is your top priority. Intelligence then allows planning and budget estimation for subsequent efforts."

Buy-in will be minimal if no one's communicating, as well. That's why organizations need to bring compliance and security teams together. "Teams need to collaborate with each other to align cybersecurity with compliance," urged Caryll Arcales. "This should be supported by management. Good management can contribute by ensuring that there's efficient communication between the two domains (or teams)." They can lend an additional hand by creating processes that bake collaboration between security and compliance into the business.

Gary Hibberd recommends developing a Governance, Risk, and Compliance (GRC) framework towards this end. "A GRC framework works best when it brings together multiple people from across the organization to focus on security together," he explained. "This cross-functional team will bring diverse knowledge, skills, and experience of compliance risks and issues related to their particular discipline together for consideration. The fresh perspective to security that this provides will ensure any gaps are quickly identified."

Security and Compliance Standards Overview (cont.)

- **NCPF:** Known as the National Cybersecurity Policy Framework, NCPF sets out policy guidelines by which the South African government can take a coherent approach to cybersecurity. It also seeks to address a lack of cybersecurity awareness in the Republic.
- **Law 05.20:** Adopted in July 2020, Law 05.20 refers to a set of objectives and provisions enacted by the Kingdom of Morocco for the purpose of strengthening the security of State-owned and critical infrastructure information systems.
- **NIA:** The National Information Assurance (NIA) policy specifies high-level information classification as well as focuses on system information and integrity for entities in the State of Qatar. Organizations can use NIA to protect their assets and defend against risks.
- **UAE NIAF:** The National Information Assurance Framework (NIAF) sets out standards by which organizations in the United Arab Emirates (UAE) must protect key information, exchange information with external actors, and engage in other required practices.
- **TISAX:** Known as the Trusted Information Security Assessment Exchange, TISAX requires all organizations that touch the German automotive supply chain to submit to audits over standards developed by the Verband Deutscher Automobilindustire (VDA).
- **ADHICS:** Issued by Abu Dhabi's Department of Health in February 2019, the Abu Dhabi Healthcare Information and Cyber Security Standards requires organizations to meet standards for asset management, access control, and other cybersecurity functions.

Conclusion

Compliance and security are not the same thing. But as noted above, they are not mutually exclusive. Organizations can use robust security controls to fulfill their compliance objectives. They can do this on their own, but they might run into challenges along the way.

Here are some additional recommendations that they can use to help them going forward:

- Put security and compliance on the Board's agenda to ensure that budget forecasts are predictable rather than having to find emergency budgets as a result of a breach or failing an audit.
- Decide what your core infrastructure is and devise a plan to ensure that those assets are covered as an absolute minimum. Talk to other members of your supply chain to ensure that they are taking cyber security seriously so as to reduce your risk.
- Map out each of the compliance standards that your organization must adhere to and check for overlap so that several policies can be addressed at the same time. (This is where the CIS Controls can help.)
- Keep abreast of changes to compliance standards and ensure you have budget, resources, technology, and processes in place to adopt changes quickly.
- Ensure that there is a clear communications policy in place to ensure that the compliance and security teams within your organization are aligned and that there is also an escalation process in place to discuss potential risks with the C-suite.

They don't have to do this all on their own, however. They can enlist the help of a vendor like Tripwire. Tripwire's solutions use file integrity monitoring (FIM), vulnerability management (VM), security configuration management (SCM), log management (LM), and other best practices to help organizations keep their systems safe both on-premises and in the cloud. Simultaneously, they can help to automate customers' compliance efforts with GDPR, SOX, PCI DSS, and many other frameworks.

Learn more about Tripwire's cybersecurity and compliance solutions at **tripwire.com**.

A Special Thank You

We wanted to thank the following experts who shared their expertise for this white paper:

- Stuart Coulson
- Dean Ferrando
- Angus Macrae
- Gary Hibberd
- Christian Toon
- Sarah Clarke
- Caryll Arcales
- David Bisson
- Michelle Gunter

This publication would not have been possible without their input.

Further Reading

- www.tripwire.com/solutions/compliance-solutions
- www.tripwire.com/solutions
- www.tripwire.com/state-of-security/security-data-protection/security-compliance-difference/
- www.tripwire.com/solutions/compliance-solutions/gdpr
- ico.org.uk/for-organisations/guide-to-data-protection/introduction-to-dpa-2018/about-the-dpa-2018/#1
- www.tripwire.com/state-of-security/security-data-protection/cyber-essentials-certification-help-business/
- www.tripwire.com/solutions/compliance-solutions/pci-dss-compliance/pci-dss-compliance-with-tripwire-a-ul-white-paper-register
- www.tripwire.com/state-of-security/regulatory-compliance/iso-27001-matters-business/
- www.investopedia.com/articles/personal-finance/050515/how-swift-system-works.asp
- www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html
- www.iec.ch/blog/understanding-iec-62443
- www.bis.org/bcbs/basel3.htm
- www.tripwire.com/solutions/compliance-solutions/sox-it-compliance/sustaining-sox-compliance-register
- www.tripwire.com/solutions/compliance-solutions/the-national-cybersecurity-authority-compliance
- www.tripwire.com/state-of-security/featured/national-cybersecurity-authority/
- www.tripwire.com/state-of-security/featured/7-challenges-your-compliance-efforts/
- www.tripwire.com/state-of-security/featured/building-effective-cybersecurity-budgets/
- www.tripwire.com/state-of-security/regulatory-compliance/hidden-value-in-creating-cybersecurity-audit-programs/
- www.tripwire.com/state-of-security/risk-based-security-for-executives/risk-management/the-challenges-of-managing-third-party-vendor-security-risk/
- www.tripwire.com/state-of-security/regulatory-compliance/regulatory-fines-prison-time-render-check-box-security-indefensible/
- www.gov.za/documents/national-cybersecurity-policy-framework-4-dec-2015-0000
- www.dgssi.gov.ma/sites/default/files/attached_files/presentation_note_of_the_law_n_deg_05-20_on_cybersecurity_-_english_version.pdf
- www.tripwire.com/solutions/compliance-solutions/national-information-assurance-certification
- https://tdra.gov.ae/userfiles/assets/vzjmlB3CM34.pdf
- www.tripwire.com/state-of-security/regulatory-compliance/achieving-automated-tisax-compliance/
- www.lexology.com/library/detail.aspx?g=16ae068c-57b6-4604-9b56-1b890f274e02
- www.tripwire.com/state-of-security/security-data-protection/security-controls/what-is-vulnerability-management/
- www.tripwire.com/state-of-security/security-data-protection/security-controls/security-configuration-management/
- www.tripwire.com/state-of-security/security-data-protection/security-controls/what-is-log-management/
- www.tripwire.com/solutions/file-integrity-and-change-monitoring
- www.gartner.com/en/information-technology/glossary/compliance
- www.gartner.com/en/information-technology/glossary/security
- www.tripwire.com/solutions/compliance-solutions/hipaa-compliance
- www.tripwire.com/state-of-security/security-data-protection/security-controls/cis-top-20-critical-security-controls/
- https://nca.gov.sa/en/pages/cscc.html
- https://nca.gov.sa/en/pages/ccc.html
- www.tripwire.com/state-of-security/controls/how-to-fulfill-multiple-compliance-objectives-using-the-cis-controls/

tripwire®
by HelpSystems

Tripwire is the trusted leader for establishing a strong cybersecurity foundation. We protect the world's leading organizations against the most damaging cyberattacks, keeping pace with rapidly changing tech complexities to defend against ever-evolving threats for more than 20 years. On-site and in the cloud, our diverse portfolio of solutions find, monitor and mitigate risks to organizations' digital infrastructure—all without disrupting day-to-day operations or productivity. Think of us as the invisible line that keeps systems safe. **Learn more at tripwire.com**

***The State of Security*: News, trends and insights at tripwire.com/blog**
Connect with us on LinkedIn, Twitter and Facebook