



From checklist to management system

Getting value from the NIST Cybersecurity Framework and ISO 27001:2022

In November 2018, the 'Written testimony of NPPD Office of Cybersecurity and Communication Assistant Secretary, Jeanette Manfra' for a hearing titled 'Interagency Cyber Cooperation: Roles, Responsibilities and Authorities of the Department of Defense & the Department of Homeland Security' mentioned that "only a more integrated approach to managing risk would enable the Nation to counter malicious cyber activity targeting our critical infrastructure".



WHAT IS AN INTEGRATED APPROACH TO MANAGING RISK?

Until recently, we've seen a controls or compliance-based approach to managing cyber risk and information security. However, there are blind spots in our current digital world that only an integrated risk-based approach can adequately address.

By adopting 'an integrated approach to managing risk', organizations can deliver efficient and actionable risk mitigation strategies that align with business objectives. More importantly, this puts focus on the unique set of risks faced by the organization – something that a compliance-based approach does not. All of this supports effective prioritization of risks and can help justify cybersecurity budgets and resource spend, bringing cybersecurity to the forefront of management attention.

Furthermore, in October 2022, the Biden-Harris administration made a commitment to supporting improvements in dealing with cybersecurity concerns: "The State and Local Cybersecurity Grant Program will provide \$1 billion in funding to SLT partners over four years, with \$185 million available for fiscal year 2022, to support SLT efforts to address cyber risk to their information systems and critical infrastructure" (source: [whitehouse.gov](https://www.whitehouse.gov)).

Cybersecurity, the NIST CSF and ISO 27001:2022

[Check Point Research \(CPR\) has found that global attacks increased by 28% in the third quarter of 2022 compared to the same period in 2021.](#) As we start to see the full impact of insufficient cybersecurity, and while governments and regulators increase their pressure on organizations to demonstrate that their measures against cyberattacks are 'sufficient' and fit-for-purpose, it has become increasingly evident that traditional ways of managing cyber risk and information security compliance in the Digital Era are not enough. To improve resilience and achieve long term objectives, organizations require a holistic view of risk and compliance across all business units as well as the supply chain.

There are two widely used frameworks for cyber and information security management, the NIST Cyber Security Framework (CSF) and ISO 27001. What are the differences, when should you use them and how can you get value from them?

The NIST CSF is a framework containing guidance and best practice for organizations looking to better protect themselves and guard customers' and suppliers' data against malicious cyberattacks. It "helps businesses of all sizes better understand, manage, and reduce their cybersecurity risk and protect their networks and data" (source: [the United States' Federal Trade Commission](#)).

The CSF provides the guidance to assess your cybersecurity program on a maturity basis, and its 'Core' focuses on five functions: identify, protect, detect, respond, recover. "The Core is not a checklist of actions to perform. It presents key cybersecurity outcomes identified by industry as helpful in managing cybersecurity risk." (source: [NIST CSF](#)). The CSF maps a lot of its recommended controls to other frameworks and standards and provides a solid starting point for organizations initiating a cybersecurity program.

“ The ISO 27001 offers a good certification choice for organizations that have operational maturity while the NIST CSF may be best suited for organizations that are in the initial stages of developing a cybersecurity risk program or attempting to mitigate breaches.

(Source: tugboatlogic)

”

An Information Security Management System (ISMS) is a framework for securing information assets, with international standard [ISO 27001:2022](#) being one of the most recognizable examples. A certified ISO 27001 ISMS helps organizations streamline processes and protect information in accordance with international best-practice, and certifications are recognized worldwide.

Both NIST CSF and ISO 27001 offer recommended controls, in the case of ISO 27001, these are summarised in Annex A and included in ISO 27002.

The frameworks differ, in that the CSF is a controls-based framework while ISO 27001 is a standard that requires a risk-based management system.



CONTROLS VERSUS RISK-BASED APPROACHES

Many organizations initiate cybersecurity projects by demonstrating that controls have been implemented and are mature for various assets and processes. This can be an unwieldy approach which can result in an ever-growing backlog of controls to implement and test by a limited number of security specialists. Teams can quickly get overwhelmed with increased risk of error or missing key vulnerabilities.

Some organizations employing a controls-led approach view security risk as an afterthought and not a key foundation or building block. They may then implement controls as a 'box-ticking' exercise to become compliant – and perhaps certified – to a standard. They are reactive organizations hoping that they will not be the next to be attacked, only acting at that stage. By contrast, as an industry we need to assume that we will be targeted and attacked. It is not a question of if but when.

Organizations with a more sophisticated approach to cyber risk management have developed a risk-based approach as the norm, where the priority is to reduce risk over time against appetite or tolerance. This typically follows a prescribed framework where controls are implemented to target key risks or vulnerabilities to the project or organization. The approach allows companies to justify spending and show clear return on investment for implemented controls. It relies on a holistic view where all risk attributes are centralized as an integrated mechanism, including risk, vulnerabilities, incidents, findings, remediations, controls, etc.

The McKinsey group has pushed for several years the importance of moving to a risk-based approach or, better still, a proactive approach. A proactive approach is an enhancement to the risk-based approach, which builds on these integrated themes by forming linkages to wider technologies to provide a real-time view of risk and reduce risk by increasing automation. This may include tooling to identify threat actors, monitor attack surfaces and highlight poor technology configurations, for both your own technologies and those of your vendors.



From checklist to ‘living, breathing’ management system

Comparing controls/compliance-based versus risk-based approaches to managing cyber and information security should only constitute a part of the discussion, however.

“

A key point to highlight is the Management System (MS) part of the Information Security Management System (ISMS). The NIST CSF, NIST 800-171, PCI DSS etc. are all control frameworks - as is ISO 27002 / Annex A of ISO 27001. But the MS part of ISO 27001 wraps around it the policies, processes, governance, change management, action management etc. necessary for information security to be properly managed.

It’s pointless implementing controls from a framework if we don’t have the assurance that they will be kept up to date, strengthened if the threat changes, and that identified remediations are properly implemented and shown to be reducing risk.

Simon Marvell, Acuity CEO


”

On the same note as Simon, an article from [DNV](#) titled ‘The three-pillar approach to cyber security: processes are crucial’ aptly points out that “cyber threats change quickly, and processes need to adapt with them”. The article goes on to detail the importance of the second pillar – process, the first being people and the third data and information.

“Processes are key to the implementation of an effective cyber security strategy. They are crucial in defining how an organization’s activities, roles and documentation are used to mitigate information risks. Processes also need to be continually reviewed.

The process pillar is made up of multiple parts: management systems, governance, policies and procedures and managing third parties. All of these parts must be addressed for the process pillar to be effective.

Management systems are key - to strengthen the second pillar in your cyber security strategy, a proper management system must be put in place”.



Ultimately, whether aligned to a framework such as the NIST CSF, or a standard such as ISO 27001, a good cyber and information security program provides the overarching management system that enables desired information security outcomes. It should bring together cyber and IT risk management, controls assurance and compliance, incident, policy and audit management.

Information security management is an ongoing process, not a one-time activity. Furthermore, compared to an information security management system, a checklist approach cannot deliver the necessary centralization of all relevant information and visibility over activity, actions, responsibilities, etc.

Whichever framework you decide to use for cyber and information security, we recommend that you wrap a risk-based management system around it.

An integrated, risk-based management system approach to cybersecurity has many benefits, including:

1. Better visibility of risks

Given that all of the data is stored in one place, this approach offers better accuracy and greater visibility of risk and compliance status. This means that risks can be easily identified, addressed, tracked and reviewed – reducing the likelihood of adverse outcomes and improving decision making.

2. Enhanced accuracy

Again, due to the centralization, platforms that support an integrated, risk-based management system approach can offer a higher degree of automation. When configured appropriately, such a platform recognizes the complex relationships between the data sets (for example: risks and controls, or vulnerabilities and incidents) – not only does this save a substantial amount of time (where there's a skills shortage) but it also reduces the likelihood of human error.

3. Effective reporting

The right tool and approach can provide actionable, risk-based insights and streamline the reporting process. It takes minutes to pull meaningful reports - such as risk-based prioritization of control improvements, aggregate risks compared to tolerance, return on investment (ROI) for new controls - unlike traditional approaches which can take weeks, or days at the best of times.

4. Improved efficiency and cost savings

Platforms based on traditional, controls-based approaches tend to be quite modular and therefore require individual customization. This makes it difficult to make sense of the information as it is often spread across different platforms in different forms. It is therefore difficult to update and maintain.

On the other hand, platforms championing an integrated, risk-based management system approach fully integrate the different data sets needed to truly understand risk – with access permissions restricting the activity to designated individuals only. Furthermore, they are designed to scale.

With Acuity STREAM's risk-based management system approach, customers have seen results including:

- Information security risks remain within tolerance
- Information security programs and investments are cost-justified
- Incidents are managed effectively
- Assurance is provided for management, customers and auditors
- Compliance and certification for ISO 27001 is done effectively and efficiently

 STREAM



At Acuity, we are supporting many customers whose ISO 27001-certified information security management systems (ISMS) 'live' in STREAM, or who are just starting their journey to ISO 27001 certification. Likewise, our customers who came to us looking for compliance to the NIST CSF chose an integrated, risk-based approach to managing their cybersecurity, and have been delighted with the level of confidence a 'living, breathing' management system provides them versus a 'box-ticking' compliance-led approach.

"Our initial use case for STREAM was ISO 27001, but then we expanded to various other ISO certification models and beyond, such as 45001, 50001, and PCI DSS. Our Information Security Management System (ISMS) was lauded in the auditing process for ISO 27001 certification, and we are now certified to this Standard with the help of STREAM. (...) The main benefits of using STREAM for ATPI have been: centralization of information, so getting an overview of everything in one place; adaptability - the fact that it isn't difficult to navigate, and very customizable; and that the more you learn about it, and about how to expand the functionality, the better the product gets".

If you'd like more detail on how an integrated, risk-based management system approach could help your organization, [contact us](#) or [request a demo of STREAM](#).

Take Control of Risk

A risk-based approach to cyber security is increasingly being mandated by regulations and standards and provides significant benefits to organizations by: reducing the risk of damaging security breaches; optimizing cyber security activities and in the event of a breach, mitigating damages through demonstration of a diligent approach.

A risk-based approach can be complex, but luckily, is not impossible. The 7 key requirements described in this paper form the basis for a practical risk-based approach to cyber security.

Acuity Risk Management helps businesses worldwide effectively manage, prioritize and report on their risks to inform strategic decision-making and build long-term resilience.

Its powerful STREAM platform provides rapid time to value to reassure stakeholders that risks are under control and compliance is maintained with increasingly complex standards and regulations. With STREAM, Acuity eliminates the guesswork around risk to support strategic decision-making, prioritization of resources and justification of expenditure to maximize ROI. With customers worldwide, Acuity has proven success supporting customers in highly regulated and targeted industries such as finance, IT, telecommunications, healthcare, defense and government.



Email: info@cybersec.solutions
Web: <https://cybersec.solutions>
Tel: 01494 936696