THE AUGUSTA GROUP

Why adopting a CyberSecurity Framework (CSF) profile is the best decision for cyber regulatory compliance.

March 2023

Andy Watkin-Child, Ted Dziekanowski

Introduction - Strategy, Mission and Business Objectives

The objective of most organizations is to optimize shareholder value by developing products and services that meet the needs of all their stakeholders. Stakeholders that can include customers, suppliers, investors, employees, communities, governments, and regulators. To meet these objectives organizations need to develop and deliver strategies that have the appropriate governance, oversight and assurance. The delivery of the organization's strategy is accomplished through well-defined and measurable business and mission objectives. These objectives should have the characteristics of being specific, measurable, achievable, relevant, and time-bound, enabling the organization to fulfil its business strategy.

Business and mission objectives also provide direction and focus to the organization's strategy, operations, and decision-making processes. These business and mission objectives are reviewed regularly and updated to ensure they remain relevant and achievable, as market forces may render objectives inappropriate in addressing the organizations strategy as organisational risks. Business and mission objectives could include increasing revenue or profitability, expanding market share, improving customer satisfaction, launching new products or services, reducing costs or improving efficiency, increasing employee satisfaction or retention, enhancing the company's brand reputation and delivering secure products and services.

The role of the board, executive management and business management team is to articulate the business strategy into clearly define and measurable business and mission objectives. That can be evaluated through corporate governance to assess the effectiveness of the organization in delivering its strategy.

Managing enterprise-wide risk is now an important business objective, under which Cybersecurity risk management is an objective that is being addressed by regulators. Cybersecurity risk management is an objective that relates to the adequate protection of the Confidentiality, Integrity and Availability (CIA) of the information types utilised and owned by organizations.

Cyber Challenges to the achievement of mission and business objectives

The frequency, complexity and severity of cyber-attacks is increasing. Creating challenges for industry, insurers, regulators and risk owners. The direct impact of cyber-attacks has been amply demonstrated by direct attacks on businesses including Medibank, Optus, Latitude, Colonial Pipeline, JBS Meat, SolarWinds, Kaseya, Microsoft, Nvidia, and Samsung to name a few. Some of these attacks have indirectly affected organizations through increased supply chain risks and Software Development Life Cycle processes. Ransomware attacks were the most significant cyber threat vector in 2021[1]. Alongside cyber threats created by geopolitics and the cost-of-living crisis cyber is predicted to be one of the largest non-financial threats that organizations faced in 2022[2,3].

Since 2017 we have seen a significant increase in the frequency, complexity and severity of cyber-attacks. While attacks were in general terms a low probability event prior to 2017, cyber-attacks are now a major concern affecting cyber insurance pricing and coverage, corporate capital and have identified the failure of companies to manage cybersecurity risk[4]. This has driven US and European Union regulators to implement cybersecurity risk management regulations. Chris Inglis, the national cyber director at The White House, has stated several times, as recently as January 2023[5], that market forces have not yet addressed cybersecurity, and that regulation will therefore be used as the means to do so. We can therefore expect more cyber regulation in 2023 and beyond. (Fig 1: The trajectory and impact of cyber-attacks)

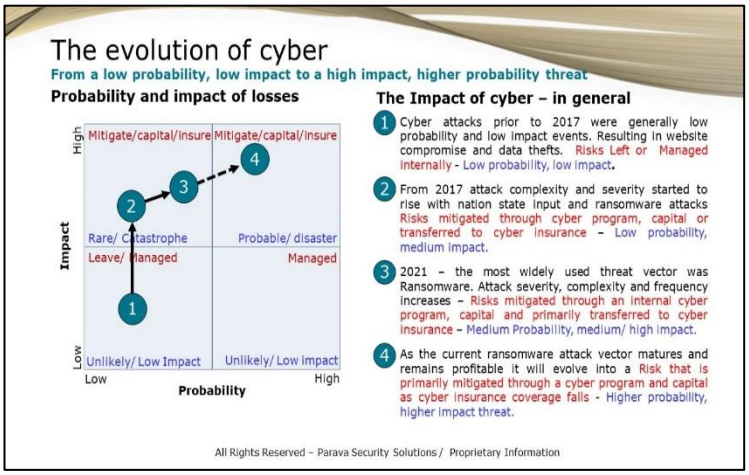

Fig 1: The trajectory and impact of cyber attacks.

[1] https://www.marsh.com/us/about/media/global-insurance-market-index-q1-2022.html?bsrc=marsh
[2] https://www.insurancejournal.com/news/international/2023/02/27/709604.htm
[3] https://www.weforum.org/events/world-economic-forum-annual-meeting-2023/sessions/press-conference-global-cybersecurity-outlook-2023
[4] https://augustagrp.com/is-cyber-insurable%3F
[5] https://www.washingtonpost.com/politics/2023/01/06/biden-national-cyber-strategy-is-unlike-any-before-it/

Compliance risks with current and potential cybersecurity risk management regulations.

US and EU regulators have released several cybersecurity risk management regulations and proposals in 2022 and 2023. These include the Securities and Exchange Commission (SEC) cybersecurity risk management, strategy, governance, and incident reporting proposal[6], affecting firms on US capital markets. The US Department of Defense (DoD) reaffirmed its plans to implement the Cybersecurity Maturity Model Certification (CMMC) regime on the global Defense Industry Base (DIB)[7]. The EU released an update to its Network and Infrastructure Security (EU NIS 2.0) Directive[8], affecting the suppliers of Critical National Infrastructure and the Digital Operational Resilience Act (DORA)[9] that impacts Financial Institutions. In 2022 US and EU regulators proposed that manufacturers of ICT products and services certify to cybersecurity risk management standards[10, 11], before products and services can be sold in the EU or US. The White House Office of the National Cyber Director (ONCD) released the U.S national cybersecurity strategy on the 2nd of March 2023[12], reaffirming Chris Inglis' statement that cyber regulation is required to manage cyber risk. It is anticipated that these regulations are the start of cybersecurity regulatory proposals for the US and EU.

Common regulatory themes

U.S and EU regulatory regimes have similar requirements, and their impact extends beyond their national boundaries, impacting both national and international organizations. They drive cybersecurity '*Left of Bang*'[13] requiring boards to take a proactive approach to managing cybersecurity risks. Current U.S and EU cyber risk management regulation requires boards to demonstrate their 'situational awareness' of cybersecurity and risk management. Through the implementation of a cybersecurity strategy, governance, risk management framework (RMF), cybersecurity programme, board oversight and assurance, and for boards to attest to their organization's cybersecurity risks. Holding boards accountable and responsible for cyber risk management and increasing board legal and compliance risk.

Regulation removes the influence of commercial market forces, and shapes compliance through regulatory enforcement regimes. U.S and EU regulations share common themes, that include, but are not limited to:

- The management of cybersecurity risk.
- Reporting cybersecurity policies and procedures.
- Confirming whether covered entities consider cybersecurity risks as part their business strategy, financial planning, and capital allocation.
- Confirming the cybersecurity risk management knowledge and experience of board members.
- The implementation of cybersecurity risk management governance processes.
- Implementing a cybersecurity Risk Management Framework and associated cybersecurity program.
- Reporting material cybersecurity incidents within a defined time frame.
- Providing regulatory updates on cybersecurity risk management compliance and previously reported cybersecurity incidents.
- Undertaking independent testing of cybersecurity risk management compliance.

Addressing the risks of cyber regulatory compliance, mission and business objectives

Organizations have a range of options to reduce the impact of cyber risks. Including the use of cyber insurance, corporate capital and cyber practices to transfer, accept or mitigate cyber risks at an enterprise and operational level. However cyber regulation changes the options available to boards for the management of cyber risks. While boards can accept cyber risk, they will be required to demonstrate to regulators how boards reached the appropriate conclusions and what data they used for regulatory reporting. Organizations can transfer the responsibility for managing risks through contracts, but they cannot transfer the accountability for cybersecurity

[6] https://www.sec.gov/news/press-release/2022-39
[7] https://dodcio.defense.gov/CMMC/
[8] https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333
[9] https://www.consilium.europa.eu/en/press/press-releases/2022/11/28/digital-finance-council-adopts-digital-operational-resilience-act/
[10] https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act
[11] https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/11/fact-sheet-biden-harris-administration-delivers-on-strengthening-americas-cybersecurity/
[12] https://www.whitehouse.gov/oncd/#:~:text=ONCD%20coordinates%20a%20whole%2Dof,innovation%20through%20cybersecurity%20policy%20leadership.
[13] https://augustagrp.com/left-of-bang-cyber-2-0

risk management. Cyber insurance is no longer a backstop for organizations, as cyber regulation transfers risk 'left of bang', requiring boards to directly manage cybersecurity risks. Boards will no longer be able to 'ignore' cyber risk as they will be required to present their organisations cyber compliance, in some instances to bid and receive contractual awards and to demonstrate to market regulators that they managed cyber risks in the event of a cyber-attack.

Cybersecurity risk management regulation requires boards to demonstrate they are managing the difference between inherent and residual risk, as economically as possible or leave the regulated market. Managing 'residual risk' requires an organization to implement an appropriate cyber practices regime. There are no shortage of cyber control frameworks and standards to choose from. They include NIST SP 800–171, NIST SP 800-53, NIST Cybersecurity Framework (*CSF*) Profiles, Cloud Security Alliance, ISO 27001 and cyber essentials. While they share similarities, most frameworks and standards lack business integration. Failing to address the integration with corporate governance, strategy and risk management or the flexibility to adapt to changes in business or mission objectives. It is why we have chosen the *CSF* profile as the most appropriate general purpose cyber framework and standard. The successful implementation of the *CSF* requires an organization to build the foundations of risk management.

Building foundations – Framing, Assessing and Responding to Risk – *NIST SP 800-39*[14]

For organizations to effectively manage cybersecurity risks, they require the organizational foundations that addresses how they will frame, assess, respond to, and monitor cyber risk. This is described by NIST SP 800-39 (*Managing Information Security Risk Organization, Mission, and Information System View*). Managing cyber risk is a complex multifaceted activity requiring the involvement of the entire organization from senior leaders and executives, that provided the strategic vision and top-level goals and objectives for the organization. Mid-level leaders that plan, execute, and manage projects and staff on the shop floor that operate the information systems, supporting the organization's mission and business functions.

Risk management is a comprehensive process that requires organizations to: (i) frame risk; (ii) assess risk; (iii) respond to risk once determined; and (iv) monitor risk on an ongoing basis using effective organizational communications, and a feedback loop for continuous improvement in the risk-related activities of organizations (Fig 2: Foundations for cybersecurity risk management). Risk management is carried out as a holistic and organization wide activity that addresses risk from the strategic to the tactical level, ensuring that risk-based decision making is integrated into every aspect of the organization. U.S Federal Information Security Risk Management Regulation (FISMA)[15] outlines an appropriate suite of tools for the implementation, oversight and assurance of cybersecurity risks. That includes NIST SP 800-39 (*Managing Information Security Risk Organization, Mission, and Information System View),* NIST SP 800-30[16] *(*Guide for Conducting Risk Assessments) and NIST SP 800-37[17] (*Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*). That are appropriate for any organization that adopts cybersecurity risk management.

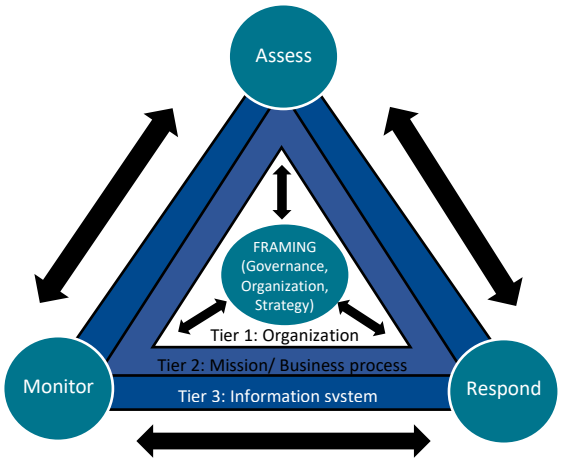

Fig 2: Foundations for Cyber risk management.

NIST SP 800-39 - Managing Information Security Risk

1. *Framing risk:* Requires and organization to build the environment in which risk based decisions are made. Produce a risk management strategy that addressess how organization intend to assess risk, respond to risk and monitor risk. Risk framing establishes a foundation for managing risk and delineates the boundaries for risk-based decisions within organizations. Establishing a realistic and credible risk framing requires that organizations identify: (i) risk assumptions (ii) risk constraints (iii) risk tolerance and (iv) priorities and trade-

[14] https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-39.pdf
[15] https://www.congress.gov/bill/113th-congress/senate-bill/2521
[16] https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final
[17] https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final

offs. Risk framing and the associated risk management strategy include strategic-level decisions on how risks to organizational operations and assets, individuals, and across the supply chain are to be managed by senior leaders and executives.

2. *Assessing risk* **:** Defines how an organization assesses risk within the context of the organizational risk framing. The purpose of risk assessment is to identify: (i) threats to the organization or threats directed through its supply chain against the organization; (ii) internal and external vulnerabilities to the organization (iii) the harm (i.e., consequences/impact) to the organization that may occur given the potential for threats exploiting vulnerabilities; (iv) the likelihood that harm will occur and the end result that is a determination of risk (i.e., the degree of harm and likelihood of harm occurring).
3. *Responding:* The organization agrees how it will respond to risk, once risks are determined based on the results of risk assessments. The purpose of risk response is to provide a consistent organization-wide response to risk in accordance with the organizational risk framing by: (i) developing alternative courses of action for responding to risk; (ii) evaluating the alternative courses of action; (iii) determining appropriate courses of action consistent with organizational risk tolerance; and (iv) implementing risk responses based on selected courses of action.
4. *Monitoring risks:* The purpose of risk monitoring is to implement appropriate oversight and assurance over risks and to (i) verify that planned risk response measures are implemented and information security requirements derived from/traceable to organizational mission and business functions, federal legislation, directives, regulations, policies, and standards, and guidelines, are satisfied; (ii) determine the ongoing effectiveness of risk response measures following implementation; and (iii) identify risk-impacting changes to organizational information systems and the environments in which the systems operate.

Organizations need to address the foundations of cybersecurity risk management to ensure the successful implementation of a Risk Management Framework (RMF). Cybersecurity risk management requires changes to organizational design and culture, embedding cybersecurity risk management into an organization from the board room to the shop floor. Across all aspects of the organizational architecture inclusive of people, process, systems, data and geographic locations. Cybersecurity risk management foundations are required to enable an organisation to move ahead and adopt an appropriate cybersecurity Risk Management Framework such as NIST SP 800-37.

NIST SP 800-37[17] - Assessing cybersecurity risks using a Risk Management Framework (RMF)

All public and private sector organizations depend on IT systems for the design, manufacturer, service, support, communications, sales and marketing of their products and services and successfully carry out their mission and business objectives. Systems that are subject to serious threats from nation-state, proxy, criminal, terrorist, hacktivists or script kiddies. Threats that exploit both known and unknown vulnerabilities to compromise the confidentiality, integrity and availability of the information being processed, stored or transmitted by those systems.

Risk assessment is one of the fundamental components of an organizational risk management process (NIST SP 800-39). Risk assessments are used to identify, estimate, and prioritize risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals and supply chains, resulting from the operation and use of information systems. The end result is a determination of risk (i.e., typically a function of the degree of harm and likelihood of harm occurring).

NIST SP 800-37 is a Risk Management Framework. It provides a process that integrates security, privacy, and cyber supply chain risk management activities, into the system development life cycle. The risk-based approach cybersecurity risk management required by cyber regulations required an evaluation of an organization inherent risk, its practices and control effectiveness and an assessment of residual risk. With control selection and specification considering effectiveness, efficiency, and constraints due to applicable laws, directives, policies, standards, or regulations.

The RMF aims to emphasize risk management by promoting the development of security and privacy capabilities into information systems, throughout the system development life cycle (SDLC). By maintaining situational awareness of the security and privacy posture of those organisational systems on an ongoing basis, through continuous monitoring processes. Providing information to senior leaders and executives to facilitate decisions,

through corporate governance, regarding the acceptance of risk to organizational operations, assets and individuals.

There are seven steps in the RMF; a preparatory step to ensure that organizations are ready to execute the risk management process and six main steps. All seven steps are essential for the successful execution of the RMF (Fig 3: Risk Management Framework – NIST SP 800-37).

- Prepare: to execute the RMF from an organization and a system-level perspective by establishing a context and priorities for managing security and privacy risk.
- Categorize: the system and the information processed, stored, and transmitted by the system based on an analysis of the impact of loss.
- Select: an initial set of practices for the system and tailor the practices as needed to reduce risk to an acceptable level based on an assessment of risk.
- Implement: the practices and describe how the practices are employed within the system and its environment of operation.

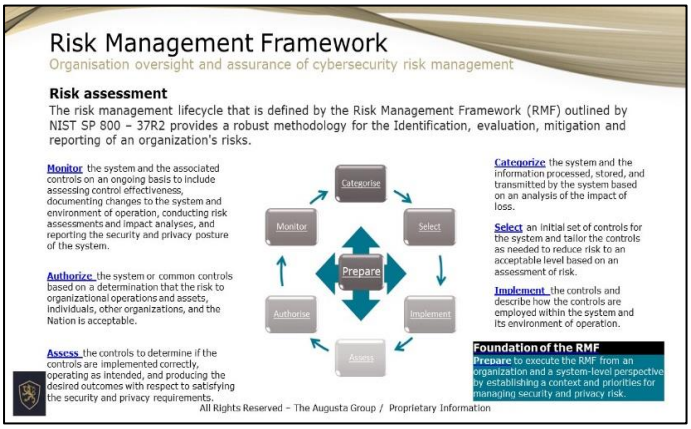

Fig 3: Risk Management Framework – NISP SP 800-37

- Assess: the practices to determine if the practices are implemented correctly, operating as intended, and producing the desired outcomes with respect to satisfying the security and privacy requirements.
- Authorize: the system or common practices based on a determination that the risk to organizational operations and assets, individuals, other organizations, and the Nation is acceptable.
- Monitor: the system and the associated practices on an ongoing basis to include assessing control effectiveness, documenting changes to the system and environment of operation, conducting risk assessments and impact analyses, and reporting the security and privacy posture of the system.

For organizations to implement an RMF they should carry out the essential activities to 'Prepare' the organization to manage its security and privacy risks. Activities that include. (Fig 4: RMF Preparation).

TASK P-1 (Risk management roles) - Individuals are identified and assigned key roles for executing the RMF. [*Cybersecurity Framework: ID.AM-6; ID.GV-2*]

TASK P-2 (Risk management strategy) - A risk management strategy for the organization that includes a determination and expression of organizational risk tolerance is established. [*Cybersecurity Framework: ID.RM; ID.SC*]

TASK P-3 (Risk assessment – organization) - An organization-wide risk assessment is completed, or an existing risk assessment is updated. [*Cybersecurity Framework: ID.RA; ID.SC-2*]

TASK P-4 (Organizationally tailored control baselines and cybersecurity framework profiles) - Organizationally-tailored control baselines and/or Cybersecurity Framework Profiles are established and made available. [*Cybersecurity Framework: Profile*]

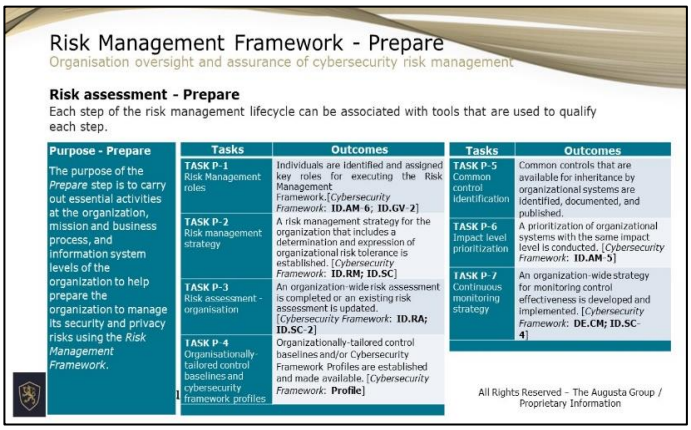

Fig 4: RMF Preparation

TASK P-5 (Common control identification) - Common practices that are available for inheritance by organizational systems are identified, documented, and published.

TASK P-6 (Impact level prioritization) - A prioritization of organizational systems with the same impact level is conducted. [*Cybersecurity Framework*: ID.AM-5]

TASK P-7 (Continuous monitoring strategy) - An organization-wide strategy for monitoring control effectiveness is developed and implemented. [*Cybersecurity Framework: DE.CM; ID.SC-4*]

Tasks P1 – P7 leverage activities that will already be conducted within an organization's security, privacy, and supply chain programs. Emphasizing the importance of having organization-wide governance, and the appropriate resources in place to enable the execution of cost-effective and consistent risk management processes across the organization. Brining these activities together with NIST SP 800-39 to form the basis for the cybersecurity risk management program.

A program that relies on a cybersecurity standard to define the baseline practices an organization should adopt for the mitigation of an organization's inherent risks. Cybersecurity regulation requires board to continually evaluate the effectiveness of their cybersecurity risk management, as business and mission objectives change in line with changes in business strategy, financial planning and operational performance.

The Cybersecurity Practices

The risk management process enables an organization to manage its risk profile, reducing its inherent risk down to a manageable residual level. It does this through the application of cybersecurity practices, practices that are documented by several informative references that include NIST, ISO, the Cloud Security Alliance, and the Centre for Internet Security.

It is the application of cybersecurity practices and the evaluation of control effectiveness that is the most expensive and time-consuming aspect of cybersecurity risk management. By way of example a typical cybersecurity standard can consist of over 100 cybersecurity practices for the management of cybersecurity risk. It can take between 12 and 18 months to implement a cybersecurity program and appropriate cybersecurity standard for an organization with low cyber maturity and require continual oversight and assurance thereafter.

The significant challenge organizations face with cybersecurity frameworks and standards is that they are generally a one-size fits all suite of practices. For example, the DoDs DFARS program requires organizations to adopt 110 cybersecurity practices from NIST SP 800-171, that includes over 300 control objectives. Control objectives that the DoD reserves the right to evaluate for covered entities, and here lies the problem. The regulation applies to large and small defense contractors and does not account for the size of the organization or the cost of compliance. Nor should it, as the aim of cybersecurity is to secure data, irrespective of its class from cyber-attacks.

We believe that a CSF profile[18] is the most appropriate cybersecurity standard to adopt in a cybersecurity risk management framework. Tailoring the *CSF* profile through the risk assessment process, to create a bespoke cybersecurity framework profile based upon the organizations risk profile, mission and business objectives.

Tailoring the *CSF* to evolving threats, mission and business requirements

Cybersecurity risk management regulation such as the SEC proposal, sets out requirements for organizations to disclose whether cybersecurity risk management is integral to its business strategy, financial planning and capital allocation. In addition to evaluating the effect of cybersecurity-related incidents have, or are reasonably likely to have, on a registrant's strategy, business model, operations, or financial condition.

Making cybersecurity risk management a near real time activity, requiring the re-evaluation of cybersecurity risks, with the potential to affect the practices an organization adopts to manage cyber risks. Practices that will change as a result of evaluating the threats and risks to an organization, in line with the organizations strategy, financial performance, business and mission objectives.

[18] https://www.nist.gov/cyberframework

The *CSF* profile is the cybersecurity standard adopted by FISMA and the RMF

The Cybersecurity Framework (CSF) was created with an understanding that all organizations are different, they have unique risks, different threats, vulnerabilities, risk tolerances and their implementation of cyber practices, that mitigate risks will vary. The Framework was created with continuous improvement in mind, to be updated and improved as industry provides feedback on implementation, ensuring it meets the needs of organizations as cyber threats evolve. Creating new risks and requiring new solutions. It also aligns with the cybersecurity process for oversight, assurance and management by adopting a cybersecurity program work breakdown structure of Identify, Protect, Detect, Respond and Recover.

Framework profiles offer advantages over traditional cybersecurity standards (Fig 5: Advantages of a CSF profile). They can be developed for specific organizations, industry sectors, products, services, or data types. They can be written to encapsulate as many or as few cybersecurity practices as required, based upon the level or protection to manage cyber risks. With the flexibility to increase or decrease the number of cyber practices as the risk environment changes. For Example, should regulation develop and require boards to oversight and assurance cybersecurity risk management governance or supply chain dependencies. As we have included in the cybersecurity RMF in figure 2 below to address U.S and EU Cybersecurity risk management regulations and enforcement proposals. The *CSF* was created to integrate with existing security processes and maps to existing cyber standards such as NIST SP 800-171, NIST SP 800-53, ISO 27001 and the Cloud Security Alliance. Providing the flexibility for organizations to align cybersecurity practices with business and mission objectives, that is an important consideration for organizations wishing or being required to deploy a cybersecurity risk management framework.

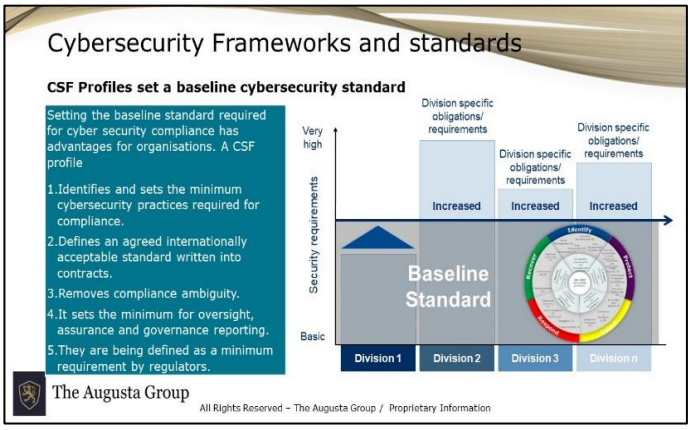

Fig 5: Advantages of a CSF profile

The Cybersecurity Framework consists of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers.

The Framework Core: is a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors. The Framework Core consists of four elements: Functions, categories, Subcategories, and informative references (Fig 6: CSF Core Framework)

- Functions: organize basic cybersecurity activities across 5 cybersecurity activities Identify, Protect, Detect, Respond, and Recover. The Functions also align with existing organizational capabilities to manage cybersecurity risks.
- Categories: are the subdivisions of a Function into groups of cybersecurity outcomes closely tied to programmatic needs and particular activities.
- Subcategories: further divide a Category into specific outcomes of technical and/or management activities. They provide a set of results that, while not exhaustive, help support achievement of the outcomes in each Category.

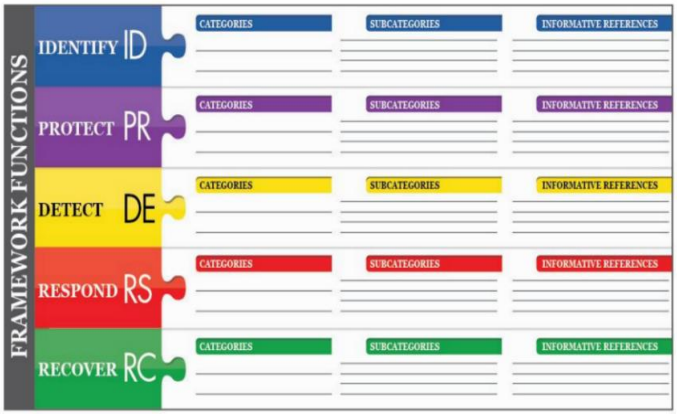

Fig 6: CSF Core Framework

- Informative References: are specific sections of standards, guidelines, and practices common among critical infrastructure sectors that illustrate a method to achieve the outcomes associated with each Subcategory.

Framework Implementation Tiers: provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. Tiers set out the degree of sophistication of cybersecurity risk management practices including Partial (Tier 1), Risk Informed (Tier 2), Repeatable (Tier 3) and Adaptive (Tier 4). Tiers describe an increasing degree of sophistication in cybersecurity risk management practices as the tiers

increase. They help determine the extent to which cybersecurity risk management is informed by business needs and is integrated into an organization's overall risk management practices. Each Tier 1, 2, 3 and 4 is broken down into threes deliverables, a Risk Management Process, Integrated Risk Management Program and External Participation.

- Risk Management Process – Describes the development of an organization's cybersecurity risk management practices in line with risk objectives, threats, and business/ mission requirements.
- Integrated Management Program – Describe the ability of the organizations cybersecurity program to mitigate an organizations risk.
- External Participation – Describes an organization knowledge and management of its role in its business environment and across its supply chains.

A typical cybersecurity framework includes functions and categories such as those described below (Fig 7: An Example CSF profile). We recommend including the Governance (GV) and Supply Chain Dependency Management (DM) functions, adopted by the Financial Services *CSF* profile, adding functions that align with cybersecurity risk management regulations.

Functions	Category ID	Category
GOVERNANCE (GV)	GV.SF	Strategy and Framework (GV.SF)
	GV.RM	Risk Management (GV.RM)
	GV.PL	Policy (GV.PL)
	GV.RR	Roles and Responsibilities (GV.RR)
	GV.SP	Security Program (GV.SP)
	GV.IR	Independent Risk Management Function (GV.IR)
	GV.AU	Audit (GV.AU)
	GV.TE	Technology (GV.TE)
	GV.RE	Regulation (GV.RE)
IDENTIFY (ID)	ID.AM	Asset Management (ID.AM)
	ID.BE	Business Environment (ID.BE)
	ID.GV	Governance (ID.GV)
	ID.RA	Risk Assessment (ID.RA)
	ID.RM	Risk Management Strategy (ID.RM)
	ID.SC	Supply Chain (ID.SC)
PROTECT (PR)	PR.AC	Identity Management and Access Control (PR.AC)
	PR.AT	Awareness and Training (PR.AT)
	PR.DS	Data Security (PR.DS)
	PR.IP	Information Protection Processes and Procedures (PR.IP)
	PR.MA	Maintenance (PR.MA)
	PR.PT	Protective Technology (PR.PT)
DETECT (DE)	DE.AE	Anomalies and Events (DE.AE)
	DE.CM	Security Continuous Monitoring (DE.CM)
	DE.DP	Detection Processes (DE.DP)
RESPOND (RS)	RS.RP	Response Planning (RS.RP)
	RS.CO	Communications (RS.CO)
	RS.AN	Analysis (RS.AN)
	RS.MI	Mitigation (RS.MI)
	RS.IM	Improvements (RS.IM)
RECOVER (RC)	RC.RP	Recovery Planning (RC.RP)
	RC.IM	Improvements (RC.IM)
	RC.CO	Communications (RC.CO)
Supply Chain/ Dependency Management (DM)	DM.ID	Internal Dependencies (DM.ID)
	DM.ED	External Dependencies (DM.ED)
	DM.RS	Resilience (DM.RS)

Fig 7: An example CSF Profile

Currently the Cybersecurity Framework profile has been adopted by the U.S Cybersecurity and Infrastructure Security Agency, by U.S Federal through FISMA and by several U.S agencies. Examples of baseline cybersecurity framework profiles adopted by various U.S agencies can be found in Appendix 1: Examples of CSF profiles developed by U.S Federal agencies.

Tailoring a *CSF* profile based upon the application of NIST SP 800-37

The traditional approach to managing cybersecurity has been to implement practices from a control standard. However, cybersecurity regulation focuses on the management of cybersecurity risk, requiring organization to assess cybersecurity risk and apply appropriate practices to mitigate those identified risk. This approach is more economic than the traditional approach to cybersecurity, as it recognises that organizations cannot protect everything and they should focus on securing those assets that have the highest risk, based up upon probability and impact.

The probability and impact of a cyber-attack is unique to an organization. It is as unique as an organizations data, assets, processes, products, services, markets, and cyber maturity. The mitigation of cyber risk is therefore unique to the organization, and this 'paradigm shift' in cybersecurity requires the organization to select practices from a control's framework based upon cyber risks. In this instance the *CSF* profile is the profile that has been adopted by U.S Federal governance through FISMA and the RMF.

The development of a CSF profile requires an organization to start with a baseline profile. This baseline profile is created following an assessment of cybersecurity risks using NIS SP 800-37. As the assessment of risks will identify risk mitigations and appropriate practice that can be selected from a baseline *CSF* profile and augmented with compensating practices from within the organization. The process of selecting practices from a baseline *CSF* profile and compensating practices is more efficient and cost effective than applying all practices from a given profile. As the organization strategy, financial performance, systems architecture, and cyber maturity change. Requiring an assessment of risk and a re-evaluation of the latest *CSF* baseline profile. Updating the latest baseline *CSF* profile to reflect changes in the organization risk profile.

To Conclude

To comply with U.S and EU cybersecurity risk management regulations organizations need to provide assurance that they have implemented a cybersecurity Risk Management Framework(RMF), with cybersecurity practices in line with the organizations risk profile. This will demonstrate appropriate oversight, assurance and attestation of cybersecurity risks through the organization's governance processes. Boards may also be required to inform regulators of their cybersecurity risk management experience and knowledge, along with employing external cybersecurity expertise.

As an example, the Securities and Exchange Commission (SEC) cybersecurity risk management proposal and EU NIS 2.0 and DORA require organizations to implement some form of an RMF that acts as the foundations for cybersecurity risk management program. Boards are going to be held accountable and responsible for cybersecurity risk management which requires the implementation of appropriate solutions to Frame, Assess, Respond and Monitor cyber risk. Cyber risk management needs to be integrated into all strategic, leadership and governance processes. These actions should demonstrate to regulators that an appropriate RMF has been implemented and cybersecurity risk management oversight, assurance and attestation is taking place through its governance processes.

Organizations that fail to demonstrate the implementation of a Risk Management Framework (RMF) may find their legal and compliance risk profile exceeding the organisations and stakeholders risk appetite. For example the Securities and Exchange Commission (SEC) requires covered entities to report their cybersecurity risk management compliance. Compliance information that will be passed to credit rating agencies and could affect the cost of capital. Another consideration is that Board members are required disclose and attest to their organisations cyber risk compliance and their personal knowledge and experience regarding the oversight of cyber risk.

The effectiveness of traditional risk treatments such as cyber insurance, contractual risk transfer or ignoring cyber risk will become less relevant or obsolete. Cyber regulation will force the treatment of cyber risk 'Left of Bang' into the board room of covered entities. Requiring boards to oversight, assure and attest cyber risk compliance. Regulatory compliance that will be evaluated in the case of EU NIS 2.0 ex-post and ex-ante, or when an organization reports a cyber incident as required by regulators. In which event an organizations compliance to its cyber insurance policy may be challenged at best or invalidated at worst, if an organisation has failed to take reasonable measures to manage cyber risk.

The risk management process and risk management framework rely upon a cybersecurity standard, to mitigate cyber risks. Reducing the organisations inherent risk down to an acceptable residual level using a cybersecurity standard. The CSF profile acts as a 'bucket' into which a cyber security standard can be input and be tailored to meet specific organisational risks that are identified through the risk assessment process and defined through the Risk Management Framework. Various U.S Federal Agencies have adopted the use of the CSF profile as the means by which cybersecurity practices are baselined. These include profiles for the Maritime sector, energy and nuclear energy, chemical production, manufacturing, transportation, dam infrastructure, water and waste water, small business and health and human services. An indication that cybersecurity standards have been set and could be adopted by industry.

The U.S National Association of Corporate Directors recommended (amongst other things) in March 2023 that organizations should implement Enterprise-wide Risk Management, a Cybersecurity Risk Management Framework and a 3 Line of Defence model for the oversight and assurance of cybersecurity risks [19] for the management of cyber risk. With cyber risk ownership to be established at a senior level and delivered through an organization ide cyber-risk management team, adopting a 3 Line Of Defence model. A model that we created and integrated into a cybersecurity risk Targeting Operating Model (TOM)[20].

The three line of defence model is a well-established model for the oversight and assurance of risk. The '3 Lines of Defence' model was developed in the 1990s, later adopted by the Basel Committee on Banking Supervision as a good model for internal control management and applied by successfully across Financial Services organisations globally[21]. The 3 Line of defense provides organisations with an effective framework through which

[19] https://www.nacdonline.org/insights/publications.cfm?ItemNumber=74777
[20] https://parava.org/board-cyber-risk-governance/
[21] https://www.iia.org.au/sf_docs/default-source/technical-resources/fact-sheet--3-lines-of-defence---nov-2017.pdf?sfvrsn=2

management can demonstrate appropriate oversight and assurance of cybersecurity risks. Relying separate and independent functions to oversight and assure cybersecurity risks. That enable management to demonstrate that they have taken the appropriate steps to manage cybersecurity risks prior to attesting to cybersecurity risk management compliance. Compliance that is delivered through a Cybersecurity risk management framework that adopt a cybersecurity framework profile.

Appendix 1 – Examples of *CSF* profiles developed by U.S Federal Agencies

Examples of existing NIST *CSF* profiles

- Ransomware Risk Management - NISTIR 8374
- *CSF* Profile for Manufacturing - NISTIR 8183r1
- *CSF* Profile Election Infrastructure - NISTIR 8310 (Draft)
- Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services - NISTIR 8323
- Cybersecurity Framework Smart Grid Profile - NIST TN 2051
- *CSF* Profile for Hybrid Satellite Networks (HSN) Draft Annotated Outline - Draft White Paper NIST CSWP 27
- US Coast Guard- Maritime Bulk Liquids Transfer Cybersecurity Framework Profile
- US Coast Guard - Maritime Specific Cybersecurity Framework Profiles
- Cybersecurity Coalition - Cybersecurity Framework Botnet Threat Mitigation Profile
- Cybersecurity Coalition - Cybersecurity Framework DDoS Threat Mitigation Profile
- Inland Revenue Services - Framework Payroll Profile

Profiles that have been developed into industry standards, adopted by the U.S Cybersecurity Infrastructure Security Agency (CISA).

- Chemical Framework Guidance [pdf]
- Commercial Facilities Framework Guidance [pdf]
- Critical Manufacturing Framework Guidance [pdf]
- Dams Framework Guidance [pdf]
- Defense Industrial Base Framework Guidance [pdf]
- Emergency Services Framework Guidance [pdf]
- Federal Framework Guidance DRAFT [pdf]
- Healthcare & Public Health Framework Guidance [pdf]
- Nuclear Framework Guidance [pdf]
- Transportation Systems Framework Guidance [pdf]
- Water & Wastewater Systems [link]

Federal Trade Commission - Small Business Cybersecurity Framework Profile

Department of Health and Human Services – Health Care and Public Health Sector Cybersecurity Framework