The Journal of Supercomputing (2018) 74:5171–5186
https://doi.org/10.1007/s11227-018-2479-2

A security review of local government using NIST CSF: a case study

Ahmed Ibrahim[1] · Craig Valli[1] · Ian McAteer[1] · Junaid Chaudhry[2]

Published online: 12 July 2018

Abstract

Evaluating cyber security risk is a challenging task regardless of an organisation's nature of business or size, however, an essential activity. This paper uses the National Institute of Standards and Technology (NIST) cyber security framework (CSF) to assess the cyber security posture of a local government organisation in Western Australia. Our approach enabled the quantification of risks for specific NIST CSF core functions and respective categories and allowed making recommendations to address the gaps discovered to attain the desired level of compliance. This has led the organisation to strategically target areas related to their people, processes, and technologies, thus mitigating current and future threats.

Keywords NIST cyber security framework · Local government · Cyber security · Risk assessment

1 Introduction

The National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF) [28] is a risk-based approach to manage risks organisations face from a cyber security perspective. Similarly, several frameworks such as NIST SP 800-53 [27], COBIT5 [17], ISO/IEC 27001:2013 [23], ISA 62443-2-1:2009 [21], and ISA 62443-3-3:2013 [22] are being used to assess cyber security risk from different perspectives and outcomes are measured using different yardsticks. Often, navigating the various frameworks can be challenging for organisations, especially if such expertise are not present internally. Given the rapidly changing technology and threat landscape,

✉ Ahmed Ibrahim
ahmed.ibrahim@ecu.edu.au

[1] Security Research Institute, School of Science, Edith Cowan University, 270 Joondalup Drive, Perth, WA 6027, Australia

[2] College of Security and Intelligence, Embry-Riddle Aeronautical University, Prescott, AZ, USA

assessing the cyber security posture of an organisation, regardless of their business or size, is paramount.

Our focus of this paper is to demonstrate the application (Sect. 3) of NIST CSF in a local government organisation and provide recommendations (Sect. 5) based on our findings (Sect. 4).

The main contributions of this paper are:

- The adoption of the NIST CSF as an Assessment Tool and targeting different levels of the organisation, depending on their level of expertise and job function to obtain responses to facilitate assessment.
- Quantification of the assessment to reflect severity of actual risk, which in turn enabled the organisation to effectively address the issues to attain desired level of compliance.
- A detailed review of similar frameworks used in the industry and relevant case studies (Sect. 6).

The next section provides a background of the NIST CSF and its components. We recommend the reader to refer to NIST [28] for additional details and strategies for suitable approaches to implement, which would vary from organisation to organisation.

2 The NIST CSF

The NIST CSF [28] consists of the *Framework Core*, the *Framework Implementation Tiers*, and the *Framework Profiles*. The Framework Core consists of five concurrent and continuous functions; *Identify*, *Protect*, *Detect*, *Respond*, and *Recover*. We designed an Assessment Tool for our investigation based on these functions, which provided a systematic approach to ascertain the organisations cyber security risk management practices and processes.

The Framework Implementation Tiers describe the level an organisations cyber security risk management practices that comply with the framework. Tiers provide context and degree to which cyber security risks are managed and extent to which business needs are considered in cyber security risk management. The Assessment Tool enabled the determination of the organisations *Current Tier* based on various internal and external factors such as their risk management practices, threat environment, legal and regulatory requirements, business/mission objectives, and organisational constraints. Organisations should also determine the *Desired Tier*, provided it is feasible to implement, reduces cyber security risks, and meets the organisational goals. The following are descriptions of the tier levels [28]:

- *Tier-1 (Partial):* risk management practices are not formalised and managed in an ad hoc manner, lack awareness of cyber security risks organisation wide, and do not have processes in place to collaborate with external entities.
- *Tier-2 (Risk Informed):* risk management practices are formalised but not integrated organisation wide, but cyber security activities are prioritised based on risks with adequate means to perform related duties, with informal means to communicate cyber security information internally and externally.

- *Tier-3 (Repeatable):* risk management practices are formalised and policies are in place and are adaptable to cyber threats. Organisation-wide approach is required to manage cyber security with skilled and knowledgeable personnel to respond and understand dependencies and role of external partners.
- *Tier-4 (Adaptive):* cyber security practices are based on lessons learnt and predictive indicators, with continuous improvement, adaptability, and timely response. Organisation-wide approach to manage cyber security risks is part of the organisational culture and actively shares with external partners.

The Framework Profile represents the outcomes based on the business needs the organisation characterised from the Framework Core and determined using the Assessment Tool. Consequently, a *Current Profile* (the "as is" state) and a *Target Profile* (the "to be" state) can be used to identify opportunities for improving the cyber security of the organisation [28]. Framework profiles can be determined based on particular implementation scenarios, and therefore, the gap between Current Profile and Target Profile would vary as per scenario. In this paper, a local government-specific approach to CSF was adapted. However, industry-specific tailoring may be performed for the CSF.

3 Methodology

The NIST CSF allowed us to design an Assessment Tool targeted at three levels of participants within the organisation, i.e. executive, management and technical. The rationale was to ascertain organisation-wide understanding of cyber security risks. Hence, the Assessment Tool comprised of questions addressing the requirements outlined as per the NIST CSF.

The questions were selected based on the nature and relevance to the level of participant. This is because the NIST CSF comprised of questions that were both technical and non-technical. Therefore, it would have been unrealistic to expect deep knowledge of technical operations or implementation level details from a policy level executive.

In order to assist us determine a baseline (i.e. the Desired Tier), additional questions were included in the Assessment Tool to determine the nature of the organisation and its business. This was then followed by the remaining requirements comprised in the NIST CSF.

3.1 Determining compliance

The compliance for each measure was based on the responses provided by the participants. They were graded as either, *Complaint*, *Partially Compliant*, or *Non-Compliant*; and each was assigned scores of either 10, 5, or 0, respectively, for each core function's subcategory. Any subcategory that was not applicable depending on the Desired Tier level was excluded from the compliance score calculation.

Given the number of security requirements for each Core Function's subcategory is *N*, then the number of applicable requirements in each subcategory given the Desired

Tier level is N'. Therefore, the total compliance score C for each core function's category can be defined as:

$$C = \frac{\Sigma R}{\Sigma N' \times 10} \tag{1}$$

where R is the compliance score for each category of the respective Core Function.

Additionally, a detailed document audit was conducted on existing policies and procedures. The Information Technology (IT) infrastructure (internal, remote locations, and cloud) were reviewed, and a detailed internal vulnerability assessment was also conducted during our investigation.

4 Findings

The responses provided by the Executive, Management, and Technical participants gave insight into the organisation's cyber security posture. Table 1 shows the summary of the compliance of NIST CSF assessment. The compliance scores were determined based on Eq. 1 presented previously.

For Identify core function, the organisation scored 36%. Their ability to track assets centrally, keep management informed, and understand operational risks from a cyber security perspective was limited, while a strategy to manage such risks did not exist. However, the organisation understood its business well and were able set priorities to support risk management decisions.

Access to physical/virtual assets were through authorisation and well-defined processes. The staff were trained and informed adequately of information security related duties and responsibilities. Certain aspects of data security related to confidentiality and availability were done reasonably well, however, assuring integrity of data needed improvement. Similarly, local maintenance and remote maintenance of IT infrastructure were carried out in a manner consistent to policies and procedures. However, relevant policies, processes, and procedures, as well as technology to assist the protection of information systems and relevant assets, were lacking. Therefore, in aggregate, the organisation scored 45% compliance for Protect core function.

The organisation scored weakest in the detection of cyber security incidents with a score of 25%. Although certain monitoring activities were in place to track physical security and malicious code, timely detection of anomalous activities and detection processes were lacking or non-existent.

Despite the lack of a specific response plan to respond to a cyber security events, the organisation had measures in place to report incidents and coordinate activities to respond adequately, which resulted in a 38% compliance score for Respond core function. These practices are updated from time to time; however, mechanism to perform post-incident analysis or to mitigate future cyber security events has not been implemented presently.

Interestingly, the organisation was well prepared to deal with recovery and resumption of core services after a cyber security event. The recovery plans in place are tested, updated, and improved periodically, thus receiving full compliance for Recover core functionality of the framework.

Table 1 NIST CSF compliance matrix

Function	Category	Compliance (%)	Total (%)
Identify (ID)	Asset Management (ID.AM)	33	36
	Business Environment (ID.BE)	75	
	Governance (ID.GV)	25	
	Risk Assessment (ID.RA)	25	
	Risk Management Strategy (ID.RM)	0	
Protect (PR)	Access Control (PR.AC)	60	45
	Awareness and Training (PR.AT)	70	
	Data Security (PR.DS)	50	
	Information Protection Processes and Procedures (PR.IP)	20	
	Maintenance (PR.MA)	75	
	Protective Technology (PR.PT)	38	
Detect (DE)	Anomalies and Events (DE.AE)	0	25
	Security Continuous Monitoring (DE.CM)	43	
	Detection Processes (DE.DP)	25	
Respond (RS)	Response Planning (RS.RP)	0	38
	Communications (RS.CO)	88	
	Analysis (RS.AN)	0	
	Mitigation (RS.MI)	0	
	Improvements (RS.IM)	100	
Recover (RC)	Recovery Planning (RC.RP)	100	100
	Improvements (RC.IM)	100	
	Communications (RC.CO)	100	

5 Recommendations

Based on the findings, the following recommendations were made with respect to each core function of the NIST CSF.

5.1 Identify

(a) Establish a central inventory of assets, including physical devices and systems, software, and external systems with all required information and prioritise based on classification, criticality, and business value.
(b) Identify the organisations role in the supply chain (i.e. producer-consumer model) as it captures and retains public data, collects revenue, and provides services to its stakeholders.
(c) Establish an Information Security policy and reference relevant federal and state policies regarding cyber security to ensure legal and regulatory requirements are understood and managed.

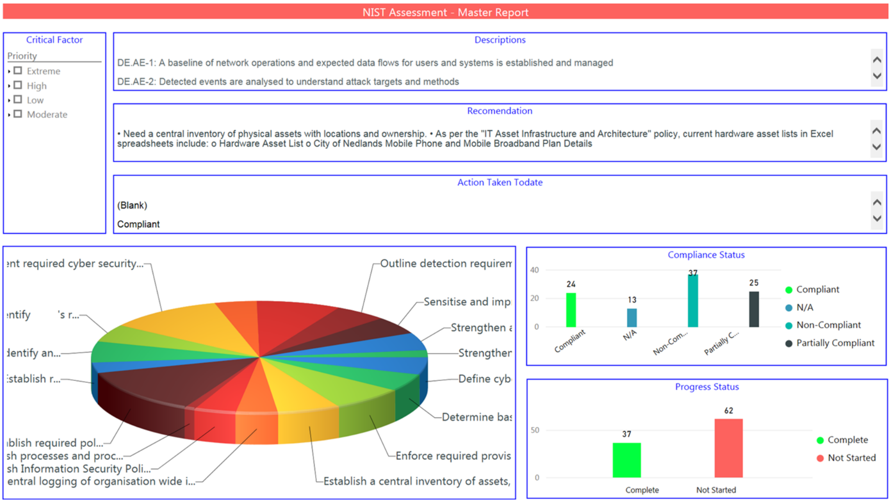
(d) Identify and prioritise threats and vulnerabilities, both internal and external, to determine cyber security risks to the organisations operations, assets, and individuals.
(e) Establish risk management processes that are managed and agreed to by stakeholders to support operational risk decisions.

5.2 Protect

(a) Strengthen the Access Control policy and procedures for organisation-wide assets that require both physical and remote access.
(b) Sensitise and increase awareness about cyber security throughout the workforce more comprehensively and provide adequate cyber security training based on roles and responsibilities. In this regard, clearly describe cyber security roles and responsibilities for relevant staff and external stakeholders.
(c) Enforce required provisions for data security in the policy and implement data-at-rest and data-in-transit security, and integrity-checking mechanisms to ensure confidentiality, integrity, and availability of information and data.
(d) Establish required policies, processes, and procedures to manage protection of information assets. This include establishment of lacking policies and processes, particularly for configuration management, data destruction, and physical operating environment; identification of security baselines; SDLC for system management; formulate vulnerability, response, and recovery plans.
(e) Strengthen processes that control and log remote access to organisational assets by external maintenance contractors.
(f) Establish a central log of organisation-wide information systems and devices, establish Removable Media policy, and strengthen network segregation to protect communications and controls networks.

5.3 Detect

(a) Determine baselines for network operations and data flows, implement appropriate activities to detect and analyse events based on event data aggregated from multiple sources and sensors. Determine incident impact and threshold to prepare and allocate resources appropriately.
(b) Implement tools to monitor cyber and physical environments to detect unauthorised mobile code, external service provider activities, and unauthorised access. Perform organisation-wide vulnerabilities regularly.
(c) Outline detection requirements in Information Security policy and continuously improve these processes to ensure timely and adequate awareness of anomalous events.



NIST Assessment - Master Report

Critical Factor

Priority
- ☐ Extreme
- ☐ High
- ☐ Low
- ☐ Moderate

Descriptions

DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed

DE.AE-2: Detected events are analysed to understand attack targets and methods

Recomendation

• Need a central inventory of physical assets with locations and ownership. • As per the "IT Asset Infrastructure and Architecture" policy, current hardware asset lists in Excel spreadsheets include: o Hardware Asset List o City of Nedlands Mobile Phone and Mobile Broadband Plan Details

Action Taken Todate

(Blank)

Compliant

Fig. 1 Microsoft Power BI Internal Site for tracking, visualising, and reporting NIST CSF assessment findings, courtesy of the participating local government organisation

5.4 Respond

(a) Establish processes and procedures to respond to cyber security events in a timely manner.

(b) Define cyber security roles and responsibilities in Information Security policy to ensure activities are coordinated for internal and external stakeholders including law enforcement in response to cyber security events.

(c) Implement required cyber security events notification and detection systems to ensure adequate information is available to analyse and understand the impact to support recovery activities.

(d) Implement required cyber security controls to detect, report, and contain incidents to prevent escalation of an incident, mitigate its effect, and eradicate the incidents.

Each of the above recommendations also had specific internal stakeholder(s) identified to indicate ownership and responsibility for addressing the issues associated. Consequently, the organisation was then able to develop strategies to address the issues identified, and assign specific tasks to individuals. For this purpose, the organisation established an internal document using Microsoft Power BI [25] (typically referred to as a Power BI site) to track and visualise the status of the NIST CSF assessment (Fig. 1).

The Power BI site facilitated transparency, visibility, and central reporting throughout the organisation. Intuitively, this resulted in a rapid and responsive drive for the organisation to address and prioritise issues based on severity and cost, with the goal of achieving Tier-2 compliance.

Furthermore, a desire to achieve a higher compliance level such as Tier-3 was expressed. Such aspiration is encouraged, however, with caution. Even though a higher level of compliance will improve the cyber security posture of the organisation, it will also affect other aspects such as resources and cost. For example, when contrasting the Risk Management Process between Tier-2 and Tier-3 as defined in the NIST CSF [28]:

(a) Implementation of risk management practices are not mandatory in Tier-2, whereas these have to be implemented as organisation-wide policies in Tier-3. Thus, Tier-3 organisations should have procedures, processes, technology, and human resources to implement relevant policies.
(b) The cyber security activities' priorities are updated in a passive nature in Tier-2 as opposed to regular active updates and constant re-evaluation of priorities for Tier-3 compliance. To acquire such capability, an organisation requires adequate technology, skilled human resources, and relevant policies that would enable keeping pace with the changes in the technology and threat landscape.

In addition to the two points highlighted above, considering both Integrated Risk Management Program and External Participation [28], significant investment in resources and human skills development or acquisition is needed to make the transition from Tier-2 to Tier-3. Moreover, this should only be considered carefully based on the organisation's business requirements, strategic objectives, budget, risk appetite, and current and future threats.

6 Related frameworks

The diversity and complexity of Information Technology (IT) system components have increased significantly in recent years. Consequently, in order for businesses to adequately secure these systems, several standards and frameworks have been developed [2]. Such frameworks need to be applicable to all manner of business sectors, be they government or private, enterprise or small-business. Tables 2 and 3 provide a summary of useful examples of how both NIST SP 800-53 and ISO/IEC 27001:2013 frameworks have been applied in practice.

Since NIST CSF can be considered as a high-level abstraction of related frameworks, it provides references to other related frameworks for specific implementation guidelines. These referenced frameworks include:

- NIST SP 800-53 Rev. 4.
- Control Objectives for Information and Related Technologies (COBIT5).
- ISO/IEC 27001:2013.
- ISA 62443-2-1:2009.
- ISA 62443-3-3:2013.

These are further described below.

6.1 NIST SP 800-53 Rev. 4

NIST SP 800-53 [27] revisions are made according to changes in responsibilities under the Federal Information Security Management Act (FISMA), Public Law (P.L.) 107-347. The latest version of this framework consists of five functions (Identify,

Table 2 Summary of case studies for NIST SP 800-53

Case study	Description
Maroochy water services cyber attack against critical infrastructure in 2000 [1]	Disgruntled former employee used insider knowledge, stolen configuration and equipments to release more than one million litres of untreated sewerage water resulting in considerable environmental damage and prosecution by the Environmental Protection Agency. The case study revealed that the application of CSF controls would have mitigated the cyber attack
Intel's high-risk IT business units' pilot project [11]	Intel IT's Office and Enterprise business units, considered to be high-level risk environments, were the testbed for a pilot project to test the effectiveness of the NIST SP 800-53. The benefits of using this framework were realised within a short timeframe, with coherent use of risk management technologies across the business model, improved identification of strengths and weaknesses, and more efficient assessments of security priorities. As a result of the pilot project, Intel IT planned to expand the framework's implementation throughout their business infrastructure
Cyber security framework implementation at the University of Chicago [32]	The University of Chicago used the framework to establish cyber security protection for Biological Services Division (BSD). The four-part implementation consisted of identifying the initial state of cyber security processes, assessment of the initial threat landscape, determination of the desired target status, and a roadmap to establish and monitor progress. This resulted in better identification of security requirements and target objectives, develop and maintain departmental processes to achieve these objectives, provide long-term security solutions in a cost-effective manner, and improve information-sharing and good work practices across departments with different cyber security requirements
How the University of Pittsburgh is using the NIST cyber security framework [31]	The University of Pittsburgh used the NIST SP 800-53 to implement an IT security package that would cater for diversified needs while enabling collaboration between different departments, accommodate a wide variety of information types and sensitivities, and encompass third-party contractors on an ad hoc basis. NIST SP 800-53 enabled these goals to be met through the streamlining of existing practices and improving documentation. The scalable nature of NIST CSF was applicable to the differing scope and IT requirements of each department within the University
SIEM-based framework for security controls automation [26]	The potential of using SIEM technology is investigated with the aim of maximising security-control automation. For the security controls identified in NIST SP 800-53, approximately 30% of these controls were considered as having the capability of automation control. The cost of implementing a SIEM-based framework for security-control automation would be quickly recouped within a short time compared to the reduced employee-hours required to monitor an infrastructure the size of a local government organisation

Table 2 continued

Case study	Description
Recommendations for information security awareness training for college students [24]	A survey largely based on NIST SP 800-50 was designed to assess information security awareness amongst students at the business college of a mid-sized University in New England. The survey found that less than one-quarter of the participants had undertaken any form of Information Security Awareness Training (ISAT), and only two of the 68 had enrolled in University-provided training. ISAT of employees in local government is an integral part of a well-implemented cyber security infrastructure. Any cyber security review needs to ascertain current levels of information security awareness to gauge whether existing training is effective or deficient. The training needs to be regularly updated as new vulnerabilities and threats continually develop in this field

Protect, Detect, Respond, and Recover), 22 categories, and 98 subcategories. This framework utilises a four-tier security model (Partial, Risk Informed, Repeatable, and Adaptive) and a seven-step process (Prioritise and Scope, Orient, Create a Current Profile, Conduct a Risk Assessment, Create a Target Profile, Determine, Analyse and Prioritise Gaps, and Implement Action Plan). It focuses on assessing the current situation by determining how to assess security, how to consider risk, and how to resolve the security threats.

6.2 Control Objectives for Information and Related Technologies (COBIT5)

COBIT5 [17] is a business CSF designed for the governance and maintenance of enterprise IT systems. It consists of five domains and 37 processes in line with the responsibility areas of plan, build, run, and monitor. COBIT5 is aligned and coordinated with other recognised IT standards and good practices, such as NIST, ISO 27000, COSO, ITIL, BiSL, CMMI, TOGAF and PMBOK. It is built around the following considerations:

– The need to meet stakeholder expectations.
– The end-to-end process control of the enterprise.
– To work as a single integrated framework.
– Recognising that “Management” and “Governance” are two different things.

6.3 ISO/IEC 27001:2013

ISO/IEC 27001:2013 [23] is an international information security standard published by the International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC), which originated from the British Standard, BS 7799. This framework consists of 114 controls in 14 groups describing the requirements needed to design and implement an Information Security Management Systems (ISMS). Version 2 released in 2013 replaces the 2005 version 1 edition. It is a standard

Table 3 Summary of case studies for ISO 27001:2013

Case study	Description
Thames Security Shredding (TSS) Ltd. [3]	TSS specialises in the collection and destruction of confidential documentation on a commercial scale. Maintaining information security is, therefore, a critical process to protect their clients' identity and to ensure compliance with the UK Data Protection Act 1998. Certification to the ISO/IEC 27001 standard was seen as an integral part of the implementation and maintenance of world-class customer-centric security controls that would satisfy existing and prospective customers' needs and allow for rapid growth in the business. ISO/IEC 27001 certification resulted in an improved attitude and awareness of their staff towards information-security-related issues. A risk-based business continuity plan was used to minimise the impact of any potential security breaches. The certification allowed documentation to be continually updated and improved as corrective actions were taken
Fredrickson International [4]	Debt collection is a sector which, like banking, finance, telecommunications, and local government, is coming under increasing scrutiny and regulation. Fredrickson International is a debt collection agency who lists a central government department, and several UK financial institutions and FTSE 100 companies amongst their clients. Since attaining ISO/IEC 27001 certification, Fredrickson has achieved higher levels of security awareness throughout its departments, staff, and employees. Security audits have become more streamlined, and customers were given the confidence that Fredrickson was conducting international best practice when it came to information security
Legal Ombudsman [5]	The office of the Legal Ombudsman for England and Wales was established to simplify the process by which members of the public, small businesses, charities, clubs, trusts, etc., could resolve complaints about legal practitioners. To improve its customer service, information security practices conducted by the office needed to show that greater information security awareness had been established, diligence and compliance in handling sensitive information were in place, and that an assurance framework was aligned with global best practice. ISO/IEC 27001 certification helped the Legal Ombudsman for England and Wales to provide clients with the confidence and reassurance that it was conducting its work by the highest work standards. A better understanding of the information security among its staff led to a reduction in risk and an increase in productivity
SVM Cards Europe [7]	SVM is a leading provider of gift card, voucher, e-code, reward code, and similar promotional and benefit schemes throughout Europe. SVM required secure business processes, improved internal organisation, increased information protection, and sought greater tender and competitive advantage. With ISO/IEC 27001 certification, SVM observed that processes became more of a lifestyle than strictly about security only, which resulted in less downtime, instigated a stronger organisational structure, improved on its ability to win new contracts, and have greater confidence that their information security processes were working properly

Table 3 continued

Case study	Description
InfoView Technologies [6]	InfoView Technologies, a Queensland-based data analytics company, required a business model that met state government requirements, improved data security understanding, became more professional, improved its business culture, and be able to sustain and continuously improve its information security management, systems, and policies. These goals were achieved through ISO/IEC 27001 accreditation, after which InfoView Technologies were able to gain increased market access, meet compliance requirements of the Queensland state government, reduce risk, become more competitive, and streamline its practices and business culture
Capgemini [8]	Capgemini is the largest IT services company in Europe; and a global leader in its multiple domains of services. Operating in more than 40 countries, and over 100 languages, Capgemini's business model needed to transcend national and cultural boundaries. Systems were required to be robust to avoid losing business and maintain competitiveness. Protection of client assets and resources was deemed a priority to assure confidentiality, integrity, and availability. Through ISO/IEC 27001 certification, Capgemini was able to ensure improved security within its departments and for its clients, enhance security awareness in its staff and employees, and provide more efficient and streamlined documentation and reporting procedures. Standards certification needed to be applicable within the global marketplace, and remain pertinent regardless of cultural differences
Costain [9]	Costain, a UK-based engineering and construction group, has contributed to the construction of significant projects worldwide. Obtaining standards certifications was seen as the correct path to achieve improvements in several internal processes. Such goals required the implementation of several standards, such as quality management standard (ISO 9001), environmental management (ISO 14001), health and safety (BS OHSAS 18001), collaborative business relationships (BS 11000), information security management (ISO/IEC 27001) and business continuity management (ISO 22301). Through the enactment of multiple standards, Costain was able to improve several areas of their business to the benefit of their internal and external customers

that should be instigated by all businesses where information security is a critical factor, but in particular, applies to software development, managed service providers/hosting services providers, IT, banking and insurance, information management, government agencies and their service providers, and E-commerce merchants [23].

6.4 ISA 62443-2-1:2009

ISA 62443-2-1:2009 [21] is an International Standards on Auditing (ISA) standard covering the elements required to develop an Industrial Automation Control System Security Management System (IACS-SMS). It consists of three categories, three element groups, and 22 elements. The framework is the first of four ISA policy and procedure products that identifies the essentials necessary to establish an effective cyber security management system (CSMS). However, the step-by-step approach as to how this is achieved is company-specific and according to their own business culture. These essentials are:

- Risk analysis.
- Addressing risk with the CSMS.
- Monitoring and improving the CSMS.

6.5 ISA 62443-3-3:2013

ISA 62443-3-3:2013 [22] is an International Standards on Auditing (ISA) standard covering the elements required for cyber security controls of industrial control systems (ICS). It consists of seven Foundation Requirements and 51 System Requirements.

ISA 62443-3-3:2013 is the third of three ISA systems products, that outlines system security requirements and security levels [22].

6.6 Other frameworks

In addition to the above, other frameworks used in the industry include:

- *Committee of Sponsoring Organizations of the Treadway Commission (COSO)* is an enterprise risk management standard, designed jointly by five leading associations, with the aim of integrating strategy and performance [13].
- *Council on CyberSecurity Top 20 Critical Security Controls (CCS CSC)* consists of a prioritised set of actions, originally developed by the SANS Institute, to protect assets from cyber attack [12].
- *ISF Standard of Good Practice (SoGP)* is a standard aimed at providing controls and guidance on all aspects of information security [20].
- *ETSI Cyber Security Technical Committee (TC Cyber)* was developed to improve standards within the European telecommunications sector [15].
- *Sherwood Applied Business Security Architecture (SABSA) Enhanced NIST Cybersecurity (SENC)* project enhances the five core levels of the NIST CSF into a SABSA model consisting of a six-level security architecture [30].
- *IASME Consortium (IASME)* is an information assurance standard based on ISO 27000, but aimed at small businesses [18].
- *RFC 2196 - Site Security Handbook (SSH)* represents a guide on how to develop computer security policies and procedures [19].
- *Health Information Trust Alliance (HITRUST)* is the first IT security CSF designed specifically for the healthcare sector. It is based on existing NIST standards and is aimed at healthcare and information security professionals [16].
- *North American Electric Reliability Corporation Critical Infrastructure Protection (NERC-CIP) version 5* is a set of requirements needed to secure the assets of the North American bulk electric system [14].

- *Open Security Architecture (OSA)* is a free community-owned resource of advice on the selection, design, and integration of devices required to provide security and control of an IT network [29].
- *Good Practice Guide 13 (GPG13)* is a UK government CSF related to Code of Connection (CoCo) compliance for businesses to secure IT systems [10].

7 Conclusion

In this paper we have used the NIST CSF to evaluate the cyber security risks of a local government organisation in Western Australia. Our approach can be used to derive measurable metrics for each Framework Core function and respective categories, thus enabling the organisation to ascertain the cyber security preparedness to actual risk.

Our findings suggest that evaluating the Desired Tier compliance to the NIST CSF helps identify the specific people, process, and technology areas that require improvement (i.e. gaps), which directly influence threat mitigation. The application of CSF helped us understand the current security context of the organisation while identifying the risks and future growth areas to improve. While higher tier compliance maybe desired, we have also recommended that the organisation's business requirements, strategic goals, budget, risk appetite, and current and future threats to be considered carefully.

Furthermore, as we have presented several related frameworks, navigating such frameworks for self assessment can be challenging, often not intended by design even, but not impossible. We have observed that the NIST CSF offers an advantage over other frameworks in this regard. However, there is still room for developing additional tools that would simplify the implementation process and speed up adoption.

Therefore, our future work will aim to improve the current Assessment Tool we have used, with a focus of making it adaptable and accessible to a wider audience and measurable for accurate quantification of cyber preparedness.

Acknowledgements We would like to thank the Western Australia local government organisation for sharing their case study for this research. We would also like to thank their staff for their support and cooperation during the assessment.

References

1. Abrams M, Weiss J (2008) Malicious control system cyber security attack case study: Maroochy water services, Australia. https://www.mitre.org/sites/default/files/pdf/08_1145.pdf. Accessed 29 Jan 2018
2. Angelini M, Lenti S, Santucci G (2017) Crumbs: a cyber security framework browser. In: 2017 IEEE Symposium on Visualization for Cyber Security (VizSec). IEEE, pp 1–8

3. BSI Group (2011) Case study Thames Security Shredding (TSS) Ltd. https://www.bsigroup.com/Documents/iso-27001/case-studies/BSI-ISO-IEC-27001-case-study-Thames-Security-UK-EN.pdf?epslanguage=en-MY. Accessed 15 Feb 2018
4. BSI Group (2012) How Fredrickson has reduced third party scrutiny and protected its reputation with ISO 27001 certification. https://www.bsigroup.com/Documents/iso-27001/case-studies/BSI-ISO-IEC-27001-case-study-Fredrickson-International-EN-UK.pdf?epslanguage=en-MY. Accessed 15 Feb 2018
5. BSI Group (2013) Implementing best practice and improving client confidence with ISO/IEC 27001. https://www.bsigroup.com/Documents/iso-27001/case-studies/BSI-ISO-IEC-27001-case-study-Legal-Ombudsman-UK-EN.pdf. Accessed 15 Feb 2018
6. BSI Group (2013) Infoview case study. https://www.bsigroup.com/LocalFiles/EN-AU/_Case%20Studies/BSI%20Infoview%20Case%20Study.pdf. Accessed 15 Feb 2018
7. BSI Group (2013) Supporting business growth with ISO/IEC 27001. https://www.bsigroup.com/Documents/iso-27001/case-studies/BSI-ISO-IEC-27001-case-study-SVM-UK-EN.pdf. Accessed 15 Feb 2018
8. BSI Group (2014) Using ISO/IEC 27001 certification to increase resilience, reassure clients and gain a competitive edge. https://www.bsigroup.com/Documents/iso-27001/case-studies/BSI-ISO-IEC-27001-case-study-Capgemini-UK-EN.pdf. Accessed 15 Feb 2018
9. BSI Group (2015) Integrating management systems to improve business performance and achieve sustained competitive advantage. https://www.bsigroup.com/Documents/iso-22301/case-studies/Costain-case-study-UK-EN.pdf. Accessed 15 Feb 2018
10. Cabinet Office (2010) Gpg13: Protective monitoring controls. http://gpg13.com/executive-summary/. Accessed 13 Mar 2018
11. Casey T, Fiftal K, Landfield K, Miller J, Morgan D, Willis B (2015) The cybersecurity framework in action: an Intel use case. Intel Corporation, pp 1–10. https://supplier.intel.com/static/governance/documents/The-cybersecurity-framework-in-action-an-intel-use-case-brief.pdf. Accessed 30 Jan 2018
12. Center for Internet Security (2018) CIS controls. https://www.cisecurity.org/controls/. Accessed 6 Mar 2018
13. COSO (2017) Guidance on enterprise risk management. https://www.coso.org/Pages/erm.aspx. Accessed 6 Mar 2018
14. Elkins V (2014) Summary of CIP version 5 standards. http://www.velaw.com/uploadedfiles/vesite/resources/summarycipversion5standards2014.pdf. Accessed 12 Feb 2018
15. ETSI (2017) Overview of cybersecurity. https://www.enisa.europa.eu/events/enisa-cscg-2017/presentations/brookson. Accessed 7 Mar 2018
16. HITRUST (2017) Introduction to the HITRUST CSF. https://hitrustalliance.net/documents/csf_rmf_related/v9/CSFv9Introduction.pdf. Accessed 21 Mar 2018
17. IASCA (2012) Cobit 5. https://cobitonline.isaca.org/. Accessed 01 Feb 2018
18. IASME Consortium (2014) About cyber essentials. https://www.iasme.co.uk/cyberessentials/about-cyber-essentials/. Accessed 07 Mar 2018
19. IETF (1997) Rfc 2196: site security handbook. https://www.ietf.org/rfc/rfc2196.txt. Accessed 8 Mar 2018
20. Information Security Forum (2016) The ISF standard of good practice for information security. https://www.securityforum.org/tool/the-isf-standardrmation-security/. Accessed 8 Mar 2018
21. ISA (2009) ANSI/ISA-99.02.01-2009. http://www.icsdefender.ir/files/scadadefender-ir/paygahdanesh/standards/ISA-62443-2-1-Public.pdf. Accessed 13 Mar 2018
22. ISA (2012) ANSI/ISA-62443-3-3 (99.03.03)-2013. http://www.icsdefender.ir/files/scadadefender-ir/paygahdanesh/standards/ISA-62443-3-3-Public.pdf. Accessed 13 Mar 2018
23. ISO (2013) ISO/IEC 27001:2013. https://www.iso.org/standard/54534.html. Accessed 1 Feb 2018
24. Kim EB (2014) Recommendations for information security awareness training for college students. Inf Manag Comput Secur 22(1):115–126. https://doi.org/10.1108/IMCS-01-2013-0005
25. Microsoft (2018) Power BI. https://powerbi.microsoft.com/en-us/. Accessed 12 Apr 2018
26. Montesino R, Fenz S, Baluja W (2012) Siem-based framework for security controls automation. Inf Manag Comput Secur 20(4):248–263. https://doi.org/10.1108/09685221211267639
27. NIST (2014) Assessing security and privacy controls in federal information systems and organizations. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf. Accessed 1 Feb 2018

28. NIST (2014) Framework for improving critical infrastructure cybersecurity: Version 1.0. https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf. Accessed 30 Jan 2018
29. OSA (2007) Osa landscape. http://www.opensecurityarchitecture.org/cms/foundations/osa-landscape. Accessed 15 Mar 2018
30. SABSA (2015) Project charter for the development of a SABSA enhanced nist cybersecurity framework. https://sabsa.org/sabsa-nist-framework-project/. Accessed 21 Mar 2018
31. Sweeney S (2015) How the University of Pittsburgh is using the NIST cybersecurity framework. https://www.sei.cmu.edu/podcasts/podcast_episode.cfm?episodeid=445056&autostarter=1&wtpodcast=howtheuniversityofpittsburghisusingthenistcybersecurityframework. Accessed 1 Feb 2018
32. University of Chicago (2016) Applying the cybersecurity framework at the university of Chicago: an education case study. http://security.bsd.uchicago.edu/wp-content/uploads/sites/2/2016/04/BSD-Framework-Implementation-Case-Study_final_edition.pdf. Accessed 31 Jan 2018