Creative Research Publishers
https://www.crossref.org/06members/50go-live.html

Journal of Behavioral Informatics
Digital Humanities & Development Research
Vol 7, No 1, 2021 Series

Towards an Effective Information Assurance and Risk Management (IA&RM) Guide: A Case Study.

Ademola, E.O.
Professor, BCS & CMI Subject Matter Expert
Principal Consultant
Power-Age Consulting
E-mails: ojo_ademola@hotmail.co.uk (private); emmanuelojoademola.academia.edu
Mobile: +4479 5813 9157

EXECUTIVE SUMMARY

The implementation of effective information assurance and risk management (IA&RM) guide entails the decision to select, use an appropriate security model, standard, and following the proper risk analysis framework. This White Paper specifies security control processes in a venture's Information Security Management System (ISMS) at a level to fulfil the security objectives of Cerious Cybernetics Corp (CCC). It accomplishes this by illuminating the executive with the appropriate accentuation of security processes and the underlying measurements. It helps to determine the effectiveness of performed controls in decision-making on targeted business. It addresses the board, enterprise and security Architects in the pursuit to enact the ideas and strategies for robust, business-aligned security capabilities within an overall ISMS. It helps practitioners to understand the use of a Ransomware contextual analysis to show how an IA&RM might further the sustainability of CCC objectives within its working context. In CCC, practitioners expectedly, are to create added value by aligning appropriate frameworks to execute strategic approach, comprehensively, cost-effective, and with innovation. It provides expert guidance on mapping processes to implement IA&RM professional guide.

Keywords: Information Assurance, Risk Management (IA&RM), Cybernetics, Business, Innovations.

Journal Reference Format:
Ademola, E.O. (2021): Towards an Effective Information Assurance and Risk Management (IA&RM) Guide: A Case Study. Journal of Behavioural Informatics, Digital Humanities and Development Research. Vol. 7.No. 1, Pp 45-56 Article DOI No - dx.doi.org/10.22624/AIMS/BHI/V7N1P3
Available online at https://www.behaviouralinformaticsjournal.info

1. INTRODUCTION

CCC is a privately-owned firm. A corporation that centres operations on cybernetic research and development (CR&D) and related intelligence innovation. Due to its nature and the environment, it requires a fit-for-purpose, hearty and thorough IA&RM policies, procedures and practices to guarantee effective information assurance (IA) for conducting the business employing front-line and applicable hazard evaluation, treatment and administration; both in the present and future security arrangement. CCC is contending in the well-evolving market space. Srinivasan (2017) indicates the evolutionary activities of hacking as well as billion-dollar industry accentuated with triggering statistics. Santos (2018) suggests that in CR&D, the global weapons trade is a vast and lucrative machine, estimated at generating 70 billion dollars annually. Gould and Bender (2015) state that the market expanded in an incentive from USD 63.5BN in 2015 to USD 71.8BN in 2017 in the US; see also DOD (2016). Similarly, around half of the £410 million Ministry of Defence (MOD) science and innovation (S&T)- CR&D activities outsourced by the Defence Science and Technology Laboratory (DSTL). In such a market domain, Hubbard and Seiersen (2016) argue that decision-makers are to be steady, settling on better decisions through robust analytic models.

Furthermore, CCC has it headquarter (HQ) in London, England, utilising an aggregate of 60 full-time staff; at random could use up-to 20 agency office staff. CCC's HQ is a globally renowned centre of business capacities. Mainly to underscore the counting for clients and the offices providing staff, CCC has various activities, including the MOD and DOD contracts. Subsequently, CCC extends activities to the research of normal operational needs for at least till the next five years. CCC requested a white paper to accentuate the nitty-gritty for executive education about IA from a consolidated, administrative, hierarchical and specialised perceptive. Besides, it consulted for a risk management's (RM) policy, procedure, and practice document from an authoritative setting. The white paper will help in many ways to sharpen the understanding, the capacity to settle on a choice on which approaches, techniques require in creating and actualising them. It guarantees any related asset, in which decision-making could bolster effectively.

An extended request is a Service Improvement Plan (SIP). The firm needs clarification on the handling of ransomware. It will provide an IA&RM guide for an improved, consistent, fit-for-purpose trend in decision-making. It recognises and assesses the standards and ideas of IA&RM. The paper will provide insights into the extension for RM hierarchically. Further, production of SIP to hypothetically and practically identify the IA and RM issues, measure them for continuous improvement strategy to create a robust competitive advantage.

1.1 News Features

News headlines that follow any cyber-attacks are most damaging for business victims. Sutton (2017) regards news headline as a platform to provide a practical context for the activities of a risk assessor; and how the company operates. With or without appropriate IA&RM guidance, success or failure might be a function promoted by new headlines. Nonetheless, attractive news features could add values and help CCC to create a robust competitive advantage. Hubbard and Seiersen (2016) underscore positive news headlines as a catalyst, amplifying board interest to do more. Sutton (2017) suggests that the board could approve the implementation of IA&RM guide to accommodate the integration of SIP to add value in decision-making

1.2 Challenges

In today's digital and GDPR age, there are multiple organisational challenges. The impact of globalisation and technology are apparent considering the global outlook of businesses in security. CCC has security worries that are at the core of its information management frameworks. It has been argued, (Dubois et al. 2010; see also Mayer, Heymans and Matulevicius 2007), that over 200 practitioner-oriented risk management methods and several academic security modelling frameworks are available, a significant challenge in selection arises. The choice becomes a foremost priority. Besides, as security standouts amongst the most risk highlight of IA; Mayer, Heymans and Matulevicius (2007) underscore that data framework in security need agreement and integration. In modelling solutions; displaying dialects and techniques with security-arrangement needs contextual consideration in the development lifecycle. Specialists need RM strategies to measure the relative significance of security risks. Essentially, CCC must comply with legally binding commitments, laws, and directions in the UK and US. There are extra security measures to underline innovation related to military exigency in existing Legislation, Regulation, Contractual (see Appendix A); CCC must abide by it all and ensure to be GDPR compliance.

It has been accentuated, (Smallwood 2014, see also Calder 2011, Sutton 2017, Matic and Sundeqvist 2017), that the critical asset for an organisation is the Intellectual Property (IP). The military nature of the IP imposes other information governance (IG) benchmarks. The GDPR radically accentuates the information asset to handle. The engagement of agency staff could also pose some challenges. Dubois et al. (2010) suggest inappropriate cost hiking as a financial risk associated with the use of agency staff. It underpins deficiency in system reconfiguration. CCC overall objective is to minimise risk in the accomplishment of Confidentiality, Integrity, Availability, Authenticity, and Non-Repudiation. It must fulfil clients' prerequisites with great prudence. Deficient compliance could cause a lethal loss of business.

It has been argued, (Calder 2009; see also Sutton 2014 and Smallwood 2014), that the four key objectives for implementing IA&RM are intersecting. The quadrant destinations are to demonstrate that an ISMS can fulfil interactively: customer confidence, internal effectiveness, compliance and regulation, and external security risks.

2. USE OF STANDARDS

With various standards and frameworks, CCC needs to fortify itself with the implementation of adequate information security (IS) choices. Actualising the right priority must come compelling. It has been suggested, (Andress and Winterfeld 2013; see also Andress 2014 and Smallwood 2014), that security professionals prioritise the concepts of confidentiality, integrity, and availability (CIA) triad with the right choice of standards. The ISO/IEC 27002:2017 accentuates the same conception and capacity. The CIA triad suffices security approach to manage the recognisable proof, appraisal, choice, and usage of standards. Clients and providers could typically agree to quantifiable and assured IA&RM without restrictive expense to approve compliances. According to MacLennan (2014), such priority affords the applicable standards to be independently verifiable and guarantee relative accuracy using the CIA model less expensively.

With IA, (MacLennan 2014; see also NIST 2014 and Andress 2013), maintain that an organisation should also put in place measurable actions to assess the effectiveness of standards and frameworks. Goedeken (2015) argues a security descriptor of regulatory compliance helps in the improvement of critical infrastructure of CIA and appropriateness of IA&RM guidance. Models and structures are a component by which adherence can be estimated (McCarthy 2009; see also Leon 2018; Hubbard and Seiersen 2016). CCC would profit from the correct implementation of models as well as engaging effectively with the quality of service (QoS). It includes expansion of customer-base, honing business forms, and cutting expenses for IA&RM. Such preference could drive productivity and add values. Cost-benefit analysis (CBA) helps to improve administrative consistency; create a robust competitive advantage and accentuate a paradigm shift in actualising ISMS. Dubois et al. (2010) state that measurement provides a definitive domain for IA&RM implementation.

Mayer, Heymans and Matulevicius (2007) underscore that standards help IS practitioners to convey solutions appropriately, permitting intertwin between organisations. Clients confidence boosted as it evacuates restrictive observation. For instance, benchmarking could give speed in a less costly approach to implementations. It empowers an expanded shift in marketing through enabled certification.

2.1 Selection and Implementation Of Standards

With the transactional style of CCC, cyber Essentials (CE) Plus, NIST 800-53 and ISO 27001 are applicable standards. The various BSI ISO/IEC standards designed to interoperate, increasing in demand and implementation. Subscription to certification recorded an increase of about 20% over the last decade. Calder (2013) attributes this to the ease of interoperability, its amenable integrations with ISO's RM 31000 and 31010. It's usability with ISO's Business Continuity 22301, Service Management 20000, and Quality Management 9001. Further, the Records Management ISO 30301, BS 7858:2012 ensure the security of the human resource (HR) IS. The ease of integration with ISO/IEC Incident Management 18044:2004, BS ISO 28000 Supply Chain Management provides a bedrock for the implementation of the appropriate governance policy considering the ISO's BS 13500. Considering the Defense Cyber Protection Partnership (DCPP) Guidance Update (2016), CE and certifications are essentials for CCC to win new contracts from the MOD. Cyber Security Model (CSM) guarantee new MOD contracts will be liable to a risk assessment because of IP. CCC's CEs Plus must come with independently verifiable necessities. With the DCPP's CSM, auditable self-evaluation is essential and measured against the level of risk evaluation. It could be crucial that CCC apply the same level of meticulousness to subcontracts as to providers. CE barely engaged system constraint to limit firewalls and web entryways. Its actualisation fortifies against malware notwithstanding the provision of the ISO 27001.

DOD (2014) underscores the need for Risk Management Framework (RMF) in the Instruction Number 8510.01. CCC would embrace the RMF steady with the standards of NIST Special Publication (SP) 800-37. The frameworks categorisation must be done in the understanding of the Committee on National Security Systems Instruction (CNSSI) 1253. The security controls from NIST SP 800-53 executed and measured as itemised in NIST SP 800-53A. It is an approach that supersedes the DOD's IA Certification and Accreditation Process. Further, risk centres strategy using NIST for evaluation and authorisation, risks and associated determinations effectively observing and implementing best practices.

Preference for NIST over ISO, yes, as it is uninhibitedly accessible through similar guidelines as CE; likewise, unreservedly available. All requirements fulfilled, the cost for certification and accreditation exercises becomes essentially unavoidable. Given that ISO 27000K benchmarks is a standout amongst the most broadly implemented, supplements and adjustments to the NIST available to enhance the CE components. CCC norms could fill the business originates from the MOD. In the implementation, this approach boosts robust monitoring of risks in a nearly real-time fashion. IA&RM motivates board security objectives to settle on financially savvy frameworks.

3. RISK ASSESSMENT AND MANAGEMENT

In the management of risk, NIST builds on existing and emerging standards, guidelines, and practices. Gives standard classifications for CCC to portray cybersecurity act. It conveys developmental opportunities in a ceaseless context and repeatable process for meeting targets. It helps in the articulation of related cybersecurity risks. NIST complements CCC's RM in cybersecurity projects. It entails the use of current procedures and leverage to identify capacities, strengthen and communicate RM issues while aligning with industry practices. Alternatively, CCC without an existing cybersecurity programme can use the NIST as a reference to establish one. Stages suffice in the implementation of the ISO 27000 framework. Initially, the senior management would provide strategic direction, resources and support to define the scope.

Followed by the creation of a catalogue of assets. For CCC, assets to protect includes information systems, data, and IP. Identifying the assets helps in risk assessment (RA) as the decision to address risks explored. Statement of Applicability (SOA) record decisions. The risk treatment plan (RTP) regularly updated to delineate risks identified and how to reduce or mitigate them. Upon this, is the launch of the ISMS following the ISO/IEC 27003 implementation guide. Following the ISMS programme, is the upkeeping through regular RA and decisions, enhancing controls to explicate continuous improvement base on the Service Improvement Plan (SIP).

A hybrid approach to deal with the implementation gives a pathway for useful measurements (Calder 2009; see also Hubbard and Seiersen 2016). It highlights the contrast between ISMS frameworks. ISMS specialists prefer quantitative proof to subjectively uncover forms for security controls within an under-accomplishing security target. With this, an ISMS administrator applies the know-how to retire or adopt an ISMS. Significantly, with measurements, security architect could report to the Board on ISMS performance against security targets and underpin successful RA to meet objectives.

3.1 Risk Treatment, Evaluation and Monitoring

The board engages experts in testing to deal with administering cyber-risks. CCC required to guarantee clients access to cyber-risks expertise. The ISO/IEC 27005:2011 provides the RA implementation ethos. It embeds the ISO 31000 and BS EN 31010:2010 to centre on the RA techniques and its management. It has been argued, (Dubois et al. 2010; see also Beckers 2015; Calder 2009 and Sutton 2014), that getting the cyber-risks on the agenda follows a design methodology. It entails setting the right context, identifying the risks, underscore risk treatment options, risk acceptance, getting the priority highlighted in an audit report, evaluation including each asset and maintaining controls to determine any current gap to update the risk register.

Risk communication strategies enable information sharing between decision-makers and stakeholders. With effective monitoring: new assets, changes in threats or vulnerabilities, changes to the impact and consequences, and security incidents remain identifiable. When the control meets maturity, the risk mitigation controls becomes measurable against a maturity model like BS ISO/IEC 15504, CMMi, COBIT, O-IMS3, SSE-CMM. With an IG maturity model, both ARMA (2013) and TOG (2011) provide a useful maturity model to implement a maturity assessment score as a guide improvement using the Plan-Do-Check-Act in SIP. Crossler et al. (2013) suggest rigorous approaches, ensuring and moderating risks to underscore the data resources and specialised assets within digitised frameworks.

Notably, the working of the FAIR risk analysis relates to ISO/IEC 27005 as the risk elements underscored accordingly. FAIR's place within ISO/IEC 27005 meets security expertise expectations while ISO/IEC 27001 provides process outlining for managing risks at a very high level with clear definitions of ISMS. ISO/IEC 27005 meets an exemplary specification- assessing and managing risk at a deterministic level. Subsequently, FAIR though a strong complement to the ISO/IEC 27005 provides support to ISMS as a methodology to determine and impact actual risks. Such an integrative approach works effectively.

4. BUSINESS CASE AND REGULATORY COMPLIANCE

Dependably, security policy framework should fathom several business indices. The Cabinet Office (2014) necessitates that a board level arrangement in charge of security and related controller must discharge security duties daily. The US, UK and comparative global GDPR regimes make the case to provide an adaptive security response to strategic business questions. With CCC's size and style, it is essential to fully understand strategic security response to business growth and return on investment challenges. Could security elements be qualitatively or quantitatively measured to prepare a level of proactive and innovative response-in-depth aftermath of a cyber incident? Has the situation contextually changed?

Undoubtedly, it is a nature of administration to revealing security occurrences of MOD and DOD with the due implementation of appropriate clearance procedures. At times, CCC depends on agency staff and the communication management of who has access to information from guests to the team. The networks, IA officer must guarantee security compliance. Crypto Custodian is not an issue as of now. As accentuated in Appendix A: risks, vulnerabilities, threats are security issues. CCC needs IA&RM directions and controls to security challenges of the military segment.

It includes authoritative stipulations, IP handling, undercover work, APT, data sharing, internet-based life, nation and client varieties, access and utilisation of information outside of the workplace, use of personal gadgets, foundation checking of staff, etc. It has been argued, (Hill and Varone 2014; see also Smallwood 2014 and Smith 2018), that jurisdiction and related legislation, regulation and contractual considerations are significant elements of an effective policy. With CCC, systems in Appendix B, C, D suffice considering assets, policies/procedures, risks, threats, and vulnerabilities.

With the proper IA&RM- direction set up, implementation of its gateway, CCC must cover the critical zones of the guide with adequate spending plan; finding savvy security insurance to customers from the interruption of noteworthy ransomware or any digital assaults responsibly. Essentially, there is no point spending the whole budget on one zone, regardless of how great it is, leaving other territories unfilled. Ensure everything is set up; otherwise, the digital lawbreakers will destructively exploit.

4.1 Assurance and Certification

Characterising measurements with direction from ISO/IEC 27004 and Business Continuity Planning (BCP) utilising ISO 22301 should follow. CCC ought to have the capacity to fulfil an internal review and a consistency audit. It is a QoS for independent and free appraisal. The British Assessment Bureau (2014) states that ISO 27001 certification achieves within twelve weeks and the authentication keeps going three years subject to annual reassessment.

The two stages for assurance and certification must be strictly followed to allow for effective assessment, review, independent appraisal, certification and verification audit. It extends similar requisites for CE assurance to fulfilling the essential two stages of initial self-evaluation and independent verification. Marching organisational capacity to the delivery satisfaction of clients. The external accredited auditor must decide the outcome. It underscores the second stage of CE Plus with an extended assurance of independent vulnerabilities input. Annual recertification is essential to fulfilling commercial and BCP requirement.

CCC adaptive model to Certification and Accreditation (C&A) NIST SP 800-37 embeds the RM's six stages. Information frameworks, select security controls, execute security controls, survey security controls, approve data frameworks, and screen security controls sorted with the RM. System owner entirely in charge, independent assessment serves a significant input. According to MOD (2016), an outline in the Defense Assurance Risk Tool (DART) underscores the functionality of industrial security accomplices. It interfaces with data frameworks as the information are highly secured and sentinel. The RM Accreditation Document Sets (RMADS) catches the risks, vulnerabilities, resources, dangers and alleviations. It permits an accreditor to evaluate the risks and related issues, allowing contingency upon the technique in use. Outdated information filtered appropriately.

4.2 Ransomware and Service Improvement Plan (SIP)

CCC's options regarding detection of ransomware and SIP are fundamental to reduce the risk of extortion and decreasing risk from ransomware. Reuvid (2018) demonstrates that in the ongoing ransomware review: 80% of respondents saw ransomware as an extraordinary or moderate danger; 75% experienced up to five attacks in a year with associated indices. Taken the news headline definition of ransomware, no surprise as for why its market currently valued at over a US$ billion. It grows exponentially as risk actors either as an organised digital crime or malicious attacks.

Nonetheless, the trend in threat detection and modelling entails monitoring tools of the critical layer-of-defence against ransomware attacks. Figure 1 underscores how ransomware works, its real-time dynamism of detection and rapid response; crucial to a solution package. Cybersecurity Insiders (2017) accentuate the anatomy of a ransomware attack in a massive global WannaCry. It misuses the server weakness of the Server Message Block (SMB) administration via unpatched Microsoft Windows frameworks. Unprecedentedly, the malware self-propagated to other vulnerable systems.

Substantially, the three essential factors for fighting ransomware assaults against frameworks converge. Petya ransomware quick reaction guide, AlienVault USM, Kaspersky, and the preferences to prioritise solution could be impressive as cyber-criminals are powerfully adjusting their techniques to advancing risks. Victims must act speedily deploying every implementable response without panic. Hadlington (2017) and Reuvid (2018) suggest that response systems must be robust with a well-defined checklist to isolate infected systems and recover functional systems. With cyber-attack globally increasing, CCC must be on continuous alert. Fortunately, Microsoft weekly patched information, regular updates from NCSC on Ransomware prevention via Cyber Incident Response initiative, all entail significant support.

Creative Research Publishers
https://www.crossref.org/06members/50go-live.html
Journal of Behavioral Informatics Digital Humanities & Development Research
Vol 7, No 1, 2021 Series

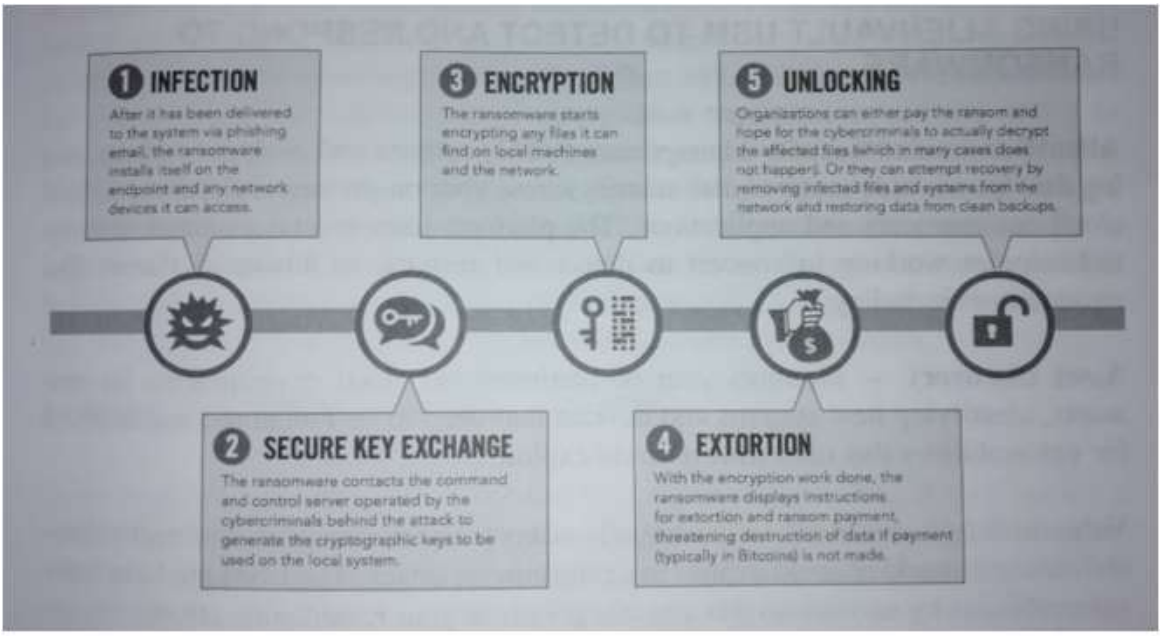

Figure 1: Anatomy of a Ransomware attack

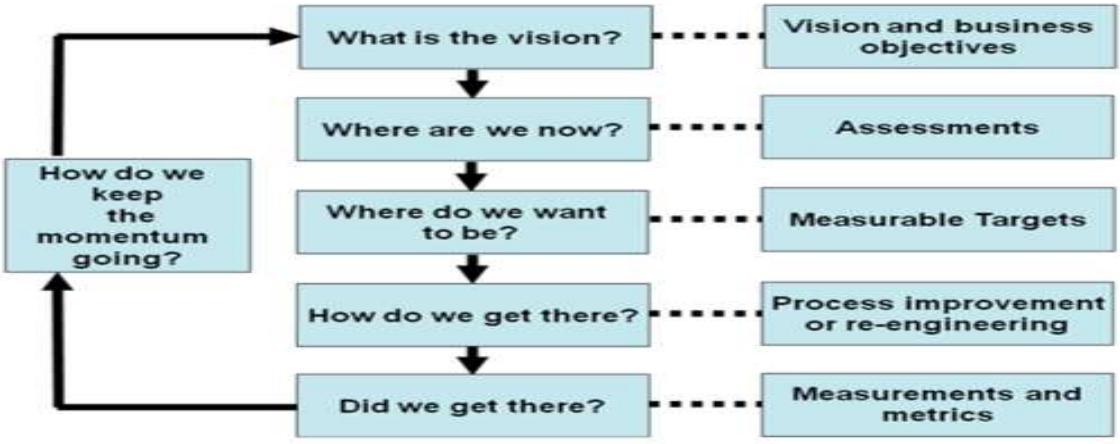

Figure 2: CSI Opportunities Model

4.3 SIP in ITIL

The CCC request for a SIP is a strategic envision of a significant gap in the expected delivery of QoS and the actual delivery. The cost of recovery could be no less than the value of being proactive through efficient preparation (Reid 2016; see also Kenyon 2016 and Reuvid 2018). Street et al. (2015) argue that interruption and counteractive action through fixing, arrangement, web URL sifting, DNS and firewalls are straightforward yet powerful controls. Figure 2 shows the opportunities underlined in a Continual Service Improvement (CSI) model detailed in the ITILv3 service management process.

Creative Research Publishers
https://www.crossref.org/06members/50go-live.html
Journal of Behavioral Informatics
Digital Humanities & Development Research
Vol 7, No 1, 2021 Series

CSI implementation uses the Plan-Do-Check-Act (PDCA) or the Deming cycle adapted in Figure 3 based on the ISO/IEC 27001:2007/2013. Such an effective SIP based on the specific service strategy, outlined in Figure 4, underscored the ITIL seven-step improvement plan. SIP in ITIL convey the opportunities for improvement suggestions, regularly measure the impacting effort, and provide a solution in refining manner. It helps CCC to enhance the revolving security elements, recognise issues and present restorative activities that should be taken to improve the administration. Figure 5 underscores the quadrant-reason, providing a critical path to an evaluation of the SIP in ITIL to ever-improving suggestions arising from all parts of service delivery. Consequently, for CCC, a SIP in ITIL setup would be collaboratively a coordinated improvement shown in Figure 6. Nonetheless, achieving an active RM in IA, with a SIP in ITIL accentuated could be a challenge. CCC perhaps may struggle to have enough resources to implement the plan. After all, CCC uses agency staff to carry out some daily activities. Therefore, outsourcing of the SIP to meet best practice could be a viable option.

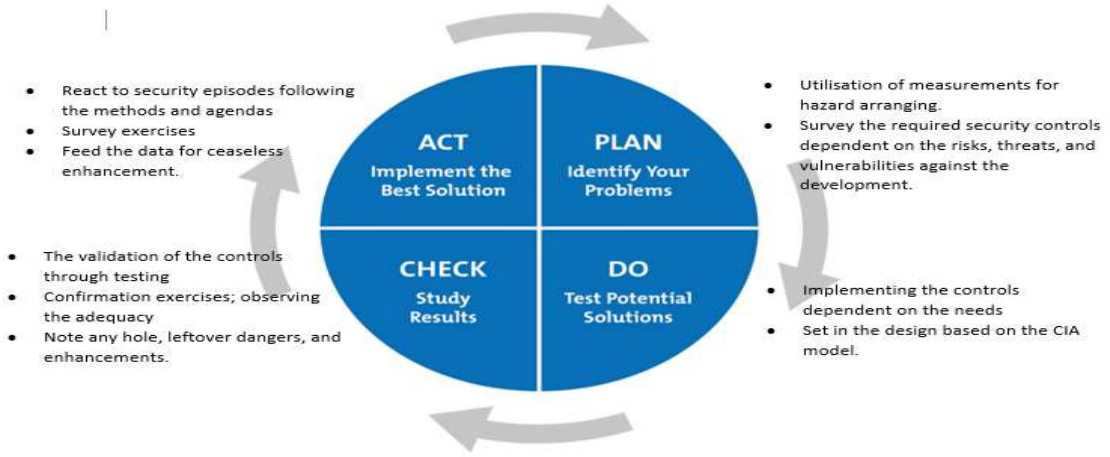

Figure 3: PDCA Cycle

Figure 4: ITIL Seven step improvement process

Creative Research Publishers
https://www.crossref.org/06members/50go-live.html
Journal of Behavioral Informatics
Digital Humanities & Development Research
Vol 7, No 1, 2021 Series

Figure 5: Quadrant reasons for measurement

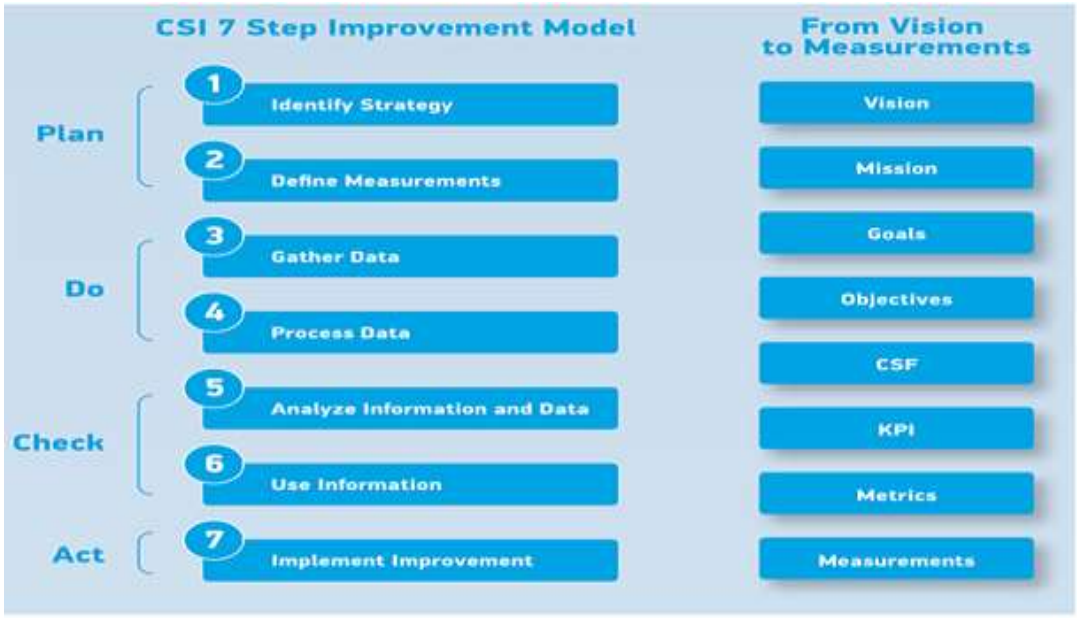

Figure 6: Collaborative SIP in ITIL

5. WAY FORWARD AND AREAS FOR FURTHER RESEARCH

In the age of ever-growing cybersecurity invasion and mobile resources, the protection of CCC's information and information assets is critical as a daily on-going concern. It is an all-inclusive responsibility of executive and staff. CCC should collaborate with clients to deliver R&D services. Adequate funding must be available to researchers in the design of RM in an IA, cyber skill management, intrusion detection system evaluation and related issues. Design and Implementation must be affordable; and cost-effectively accessible.

Research remains an innovation to managing new risks, threats, vulnerabilities. It endeavours new openings in defence of the CIA of CCC information assets. Such engagement extends to CCC's financial specialists, providers and clients could open further opportunity for various staff developmental agenda. There must be a regular update of anticipated risks, centre on frequently updating the list of future threats underscoring an integrated solution. Cumulation on medical and health concerns from human applied sciences becomes essential.

The financial uncertainty may impact on security controls as risks exposure for niche solutions may narrow application; therefore, higher risk suffices for not selling the solution to recoup costs. CCC must attend to changing agenda underscored in GDPR and Data Protection Act 2018. Collaboration and information sharing with other companies to reduce the chances of increased cyber-attacks. New ways of working might generate new risks and create robust RM. Increased competition could create opportunities for competitive advantages. Political changes like Brexit in the UK's trades exclusion; GDPR regime in the US, Russia; could strengthen needs for global collaborations.

Effective IA&RM best practices could open opportunities to create a robust competitive advantage. It could facilitate a robust agenda for business continuity. It helps in escalating the culture of proactive security, continuous improvement, adaption and response to emerging threats. Implementation of associated security and related frameworks would assist CCC in achieving contextual regulatory compliance, be in a stronger position to resist security threats, lowers the risk and costs associated with security incidents. Necessarily, the drive for social change agenda to protect against unsafe dangers becomes an organisational achievement. An ISMS integrates all components into unified multiple-stakeholder systems to convey the advantages. It is an outcome to exhibit CCC administrative consistency, upgrade notoriety to win and hold business, enhance proficiency, and fulfil review.

6. CONCLUSION

Having considered the options available to CCC, the protection of an organisation's information and information assets is critical. As technology expands in sophistication, so do tactics for unauthorised access and compromise to information assets. Underscoring this, much effort engaged in designing and developing RM in an IA platform to help defend the CIA organisational information assets. While the focus of different frameworks may vary, the fundamentals are the same. Key components include implementation of policies and procedures designed to protect CCC's information and information assets; preparing a list of all information assets and assessing the risks associated with each asset; assigning and implementing controls to mitigate the risks identified; continuous monitoring and assessment of the powers and processes to ensure its ongoing effectiveness. For CCC's IA, organisational culture, regional and industry-specific regulations should be in consideration, business objectives tailored to meet specific needs, and components from multiple frameworks. All integrated to create the best practice for CCC.

REFERENCES

1. Andress, J. and Winterfeld, S., 2013. *Cyber warfare: techniques, tactics and tools for security practitioners*. Elsevier.
2. Andress, J., 2014. *The basics of information security: understanding the fundamentals of InfoSec in theory and practice*. Syngress.
3. Beckers, K., 2015. Supporting ISO 27001 Compliant ISMS Establishment with Si. In *Pattern and Security Requirements* (pp. 109-137). Springer, Cham.
4. British Assessment Bureau. (2014). CERTIFICATION CYCLE EXPLAINED Available at: http://www.british-assessment.co.uk/guides/the-3-year-certification-cycle-explained/ (Accessed: 31 October 2018)
5. Cabinet Office. (2014). Security Requirements for List X Contractors. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/367514/Security_ Requirements_for_List_X_Contractors.pdf (Accessed: 31 October 2018)
6. Calder, A., 2009. Implementing information Security Based on ISO 27001/ISO 270002. *Ontario-Canada*.
7. Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M. and Baskerville, R., 2013. Future directions for behavioural information security research. *computers & security*, *32*, pp.90-101.
8. Dubois, É., Heymans, P., Mayer, N. and Matulevičius, R., 2010. A systematic approach to define the domain of information system security risk management. In *Intentional Perspectives on Information Systems Engineering* (pp. 289-306). Springer, Berlin, Heidelberg.
9. Goedeken, E.A., 2015. Information Governance and Assurance: Reducing Risk, Promoting Policy: London: Facet Publishing.
10. Gould, S. and Bender, J., 2015. Here's how the US military spends its billions. *Business Insider*, *29*.
11. Hill, M. and Varone, F., 2014. *The public policy process*. Routledge.
12. Hubbard, D.W. and Seiersen, R., 2016. *How to measure anything in cybersecurity risk*. John Wiley & Sons.
13. Leon, R.J., 2018. *An Event Management Framework to Aid Solution Providers in Cybersecurity* (Doctoral dissertation, The George Washington University).
14. MacLennan, A., 2014. *Information governance and assurance: reducing risk, promoting policy*. Facet Publishing.
15. Matic, S. and Sundeqvist, E., 2017. Information security at Swedish startups.
16. Mayer, N., Heymans, P. and Matulevicius, R., 2007. Design of a Modelling Language for Information System Security Risk Management. In *RCIS* (pp. 121-132).
17. McCarthy, J., 2009. *An Examination of the Impact of E-Business Evolution within Small and Micro Businesses* (Doctoral thesis, Brunel University).
18. MOD. (2016) Defence Assurance and Information Security: defence industry/list X. Ministry of Defence. Available at: https://www.gov.uk/guidance/defence-security-and-assurance-servicesdefence-industry-list-x (Accessed: 31 October 2018)
19. Reuvid, J. ed., 2018. *Managing Cybersecurity Risk: Cases Studies and Solutions*. Legend Press Ltd
20. Santos, R. ed., 2018. *Arms Sales, Treaties, and Violations*. Greenhaven Publishing LLC.
21. Shabou, B.M., 2018. An Information Governance Policy Is Required for My Institution, What to Do? *Diverse Applications and Transferability of Maturity Models*, p.61.
22. Smallwood, R.F., 2014. *Information governance: Concepts, strategies, and best practices* (Vol. 574). John Wiley & Sons.
23. Smith, K.B., 2018. *The public policy theory primer*. Routledge.
24. Srinivasan, C.R., 2017. Hobby hackers to billion-dollar industry: the evolution of ransomware. *Computer Fraud & Security*, *2017*(11), pp.7-9.
25. Sutton, D., 2014, November. Information Risk Management: A practitioner's guide. BCS.
26. Sutton, D. 2017. *Cyber Security: A practitioner's guide.* BCS.