دار نشر جامعة قطر
Qatar University Press

كلية القانون
College of Law
QATAR UNIVERSITY جامعة قطر

OPEN ACCESS

Submitted: 22 October 2017
Accepted: 5 March 2018

Research Article

Towards a Qatar Cybersecurity Capability Maturity Model with a Legislative Framework

Rafael Dean Brown, J.D.
Clinical Assistant Professor of Law, Legal Skills Department
Affiliate, Centre for Law and Development, College of Law, Qatar University
rbrown@qu.edu.qa

Abstract

In an age when cybersecurity vulnerabilities can be used as a pretext for a blockade, as in the case of Qatar prompted by a hack of the Qatar News Agency, it becomes incumbent upon states to consider legislating the capability maturity measurement and the development of their cybersecurity programs across the community. This paper proposes a Qatar Cybersecurity Capability Maturity Model (Q-C2M2) with a legislative framework. The paper discusses the origin, purpose and characteristics of a capability maturity model and its adoption in the cybersecurity domain. Driven by a thematic analysis under the document analysis methodology, the paper examines existing globally recognized cybersecurity capability maturity models and Qatar's cybersecurity framework using publicly available documents. This paper also conducts a comparative analysis of existing cybersecurity capability maturity models in light of the Qatari cybersecurity framework, including a comparative analysis of cybersecurity capability maturity model literature. The comparative document analysis helped identify gaps in the existing Qatar National Information Assurance Policy and specifically the Qatar National Information Assurance Manual. The proposed Q-C2M2 aims to enhance Qatar's cybersecurity framework by providing a workable Q-C2M2 with a legislative component that can be used to benchmark, measure and develop Qatar's cybersecurity framework. The Q-C2M2 proposes the USERS domains consisting of Understand, Secure, Expose, Recover and Sustain. Each domain consists of subdomains, under which an organization can create cybersecurity activities at initial benchmarking. The Q-C2M2 uses the following five levels to measure the cybersecurity capability maturity of an organization: Initiating, Implementing, Developing, Adaptive and Agile.

Keywords: Cybersecurity; Qatar; Capability maturity model; C2M2, Blockade; Q-C2M2

Cite this article as: Brown R. D., "Towards a Qatar Cybersecurity Capability Maturity Model with a Legislative Framework", *International Review of Law*, Volume 2018, Blockade Special Issue 4

https://doi.org/10.29117/irl.2018.0036

© 2019 Brown, licensee QU Press. This is an open access article distributed under the terms of the Creative Commons Attribution license CC BY 4.0, which permits unrestricted use, distribution and reproduction in any medium, provided the original work is properly cited.

كلية القانون
College of Law
QATAR UNIVERSITY جامعة قطر

دار نشر جامعة قطر
Qatar University Press

OPEN ACCESS
Submitted: 22 October 2017
Accepted: 5 March 2018

مقالة بحثية

نحو نموذج لتعزيز كفاءة الأمن السيبراني في قطر ضمن الإطار التشريعي

رافاييل دين براون، ج .د.
أستاذ مساعد في القانون الاكلينيكي – قسم المهارات القانونية، منتسب – مركز القانون والتنمية
جامعة قطر، كلية القانون
rbrown@qu.edu.qa

ملخّص

في هذا العصر، يجب على الدول وضع التشريعات التي تقيس قدرات أمنها السيبراني وتطوير برامجها، بالأخص عندما تُستخدم ثغرات الأمن السيبراني كذريعة لفرض الحصار، كما هو الحال في دولة قطر، وذلك بعد أن تم اختراق وكالة الأنباء القطرية. يقترح هذا البحث نموذجًا لتعزيز قدرات الأمن السيبراني (Q-C2M2) في دولة قطر ضمن إطار تشريعي. ويتناول البحث نموذجًا أصيلًا لتعزيز قدرات الأمن السيبراني مع تسليط الضوء على غرضه وخصائصه واعتماده. كما يعرض البحث نماذجًا لتعزيز قدرات الأمن السيبراني الحالية والمعترف بها عالميًا، ودراسة عن الأمن السيبراني في دولة قطر باستخدام الوثائق المتاحة، وذلك بناء على منهجية التحليل الموضوعي للوثائق. كما يقدم هذا البحث تحليلًا مقارنًا لنماذج تعزيز قدرات الأمن السيبراني في ضوء الأمن السيبراني القطري. وفي هذا الإطار، ساعد التحليل المقارن للوثائق في تحديد الثغرات الموجودة في سياسة تأمين المعلومات الوطنية القطرية بشكل عام، ودليل تأمين المعلومات الوطنية القطرية بشكل خاص. يهدف نموذج (Q-C2M2) المقترح إلى تعزيز إطار عمل الأمن السيبراني في قطر من خلال توفير نموذج عملي مع عنصر تشريعي يمكن استخدامه لقياس أداء الأمن السيبراني وتطويره. كما يقترح هذا النموذج مجالات للمستخدمين "USERS" التي تتكون من الفهم (Understand)، والأمن (Secure)، والكشف (Expose)، والاستعادة (Recover)، والاستدامة (Sustain)، حيث يتضمن كل مجال مجالات فرعية، والتي بموجبها يمكن للمؤسسة إنشاء أنشطة للأمن السيبراني عند التقييم الأولي. يستخدم نموذج (Q-C2M2) المستويات الخمسة التالية لقياس تعزيز قدرات الأمن السيبراني للمنظمات: البدء والتطبيق والتطوير والتكيف والمرونة.

الكلمات المفتاحية: الأمن السيبراني، دولة قطر، نموذج تعزيز القدرات، C2M2، حصار، Q-C2M2

Cite this article as: Brown R. D., "Towards a Qatar Cybersecurity Capability Maturity Model with a Legislative Framework", *International Review of Law*, Volume 2018, Blockade Special Issue 4

https://doi.org/10.29117/irl.2018.0036

© 2019 Brown, licensee QU Press. This is an open access article distributed under the terms of the Creative Commons Attribution license CC BY 4.0, which permits unrestricted use, distribution and reproduction in any medium, provided the original work is properly cited.

Introduction

On June 5, 2017, Saudi Arabia, UAE, Bahrain and Egypt cut off diplomatic ties with Qatar. Saudi Arabia closed its land border and the blockading countries closed access to its airspace and ports of entry to Qatar.[1] Later, the blockading countries prohibited their financial institutions from transacting with Qatari banks and from trading in Qatari riyals.[2] One month prior to the blockade, hackers had breached the state-owned Qatari News Agency (QNA) website[3] with little effort, using a kiddie script, due to the site's lax security.[4] Within minutes of the hack,[5] fake remarks that the hackers misattributed to the emir of Qatar were disseminated online through social media and news outlets from the blockading countries.[6] According to *The Washington Post*, U.S. intelligence agencies attributed the hacking to the UAE.[7] The fake remarks on the QNA website were used by the blockading countries as the initial pretext for imposing the blockade on Qatar.[8]

Geopolitics aside, the blockade demonstrated the interconnectedness of cybersecurity and critical infrastructures, a phenomenon that Li and Huang have referred to as "pervasive cyber interdependencies,"[9] which have emerged from the automation and computerization of critical infrastructures. A critical infrastructure has been defined as an element of a system that is necessary to maintain societal function, health and physical security and social and economic welfare.[10] Critical infrastructures include cyber interdependent sectors like food, transportation, information and communication technologies, energy and utilities, financial systems, healthcare and government.[11]

In the case of the Qatar blockade, multiple cybersecurity attacks on a state-owned media's information and communication technologies became the pretext for trade and transportation

1. Tamar Kiblawi et al., Qatar rift: Saudi, UAE, Bahrain, Egypt cut diplomatic ties, *CNN*, July 27, 2017, http://edition.cnn.com/2017/06/05/middleeast/saudi-bahrain-egypt-uae-qatar-terror/index.html (accessed 16 October 2017); BBC, *Qatar crisis: What you need to know*, BBC News, July 19, 2017, http://www.bbc.com/news/world-middle-east-40173757 (accessed October 16, 2017).
2. Tom Arnold, Hadeel Al Sayegh, & Tom Finn, *UPDATE 3-Qatari riyal under pressure as Saudi, UAE banks delay Qatar deals*, CNBC, June 6, 2017, https://www.cnbc.com/2017/06/06/reuters-america-update-3-qatari-riyal-under-pressure-as-saudi-uae-banks-delay-qatar-deals.html (accessed October 16, 2017).
3. Hackers commandeered the Qatar News Agency (QNA) website on May 23–24 and planted misattributed statements, purportedly delivered by Sheikh Tamim during the latest graduation ceremony held for Qatari conscripts. See George Doumar et al., *Crisis in the Gulf Cooperation Council: Challenges and Prospects* (Arab Center Washington DC, 2017) 7.
4. Charlie Osborne, *Script kiddies delight at 'easy' hack which caused Qatar diplomatic crisis*, Zero Day Net, June 8, 2017, http://www.zdnet.com/article/it-was-easy-to-cause-the-qatar-diplomatic-crisis/ (accessed October 15, 2017).
5. *Stupendous hubris…and its damage*, in George Doumar et al., *Crisis in the Gulf Cooperation Council: Challenges and Prospects* (Arab Center Washington DC, 2017), 44 (stating that "within minutes of the publication of the fake statements by Qatar's Emir, Saudi Arabian television stations and individuals were summoned into action against Doha and its leadership").
6. Ben Westcott, Richard Roth, & Ralph Ellis, *Qatar says embargoing nations behind news agency hack*, CNN, July 27, 2017, http://edition.cnn.com/2017/07/20/middleeast/qatar-ambassador-un-demands/index.html. Interestingly, five weeks before the hacking there were thirteen separate opinion pieces attacking Qatar in U.S. media. Doumar et al. (n 3).
7. Karen DeYoung & Ellen Nakashima, *UAE orchestrated hacking of Qatari government sites, sparking regional upheaval, according to U.S. intelligence officials*, The Washington Post, July 16, 2017, https://www.washingtonpost.com/world/national-security/uae-hacked-qatari-government-sites-sparking-regional-upheaval-according-to-us-intelligence-officials/2017/07/16/00c46e54-698f-11e7-8eb5-cbccc2e7bfbf_story.html?utm_term=.af380f2295ce (accessed October 15, 2017).
8. Financial Times, *The blockade against Qatar damages all sides*, July 23, 2017, https://www.ft.com/content/213cfae6-6e28-11e7-bfeb-33fe0c5b7eaa?mhq5j=e7 (accessed October 14, 2017).
9. Li Xiao-Juan & Huang Li-Zhen, Vulnerability and interdependency of critical infrastructure: A review, Third International Conference on Infrastructure Systems and Services: Next Generation Infrastructure Systems for Eco-Cities (INFRA), 1–5 (2010).
10. Jose M. Yusta, Gabriel J. Correa & Roberto Lacal-Arántegui, *Methodologies and applications for critical infrastructure protection: State-of-the-art*, 39(10) Energy Policy 6100–611 (2011); Walter Miron & Kevin Muita, *Cybersecurity capability maturity models for providers of critical infrastructure*, 4(10) Tech Innovation Management Rev 33–39 (2014).
11. Miron and Muita (n 10).

blockades that affected Qatar's financial systems and food supply. According to Miron and Muita,[12] there are three types of attacks on critical infrastructures: (1) a direct infrastructure effect,[13] (2) an indirect infrastructure effect[14] and (3) an exploitation of infrastructure.[15] The Qatar cyberattack had, and continues to have as of the writing of this paper, an indirect infrastructure effect[16] on Qatar. The cyberattack created a cascading disruption on trade and transportation, and accompanying financial consequences for the Qatari government, society and economy through public and private reactions to the attack, such as the initial panic buying caused by the spread of false news.[17]

For Qatar, the blockade was a test of resilience,[18] a wakeup call for enhancing cybersecurity and self-sufficiency. With Qatar's cybersecurity strategy up for reconsideration in 2018 when the action plan will be redrawn,[19] it is timely to reexamine Qatar's cybersecurity capabilities. This paper proposes a cybersecurity capability maturity model (C2M2) for Qatar with a legislative framework. Section II of the paper begins with a discussion of the capability maturity model's origin, purpose, and characteristics and its adoption in the cybersecurity domain. Section III conducts a document analysis of existing C2M2s, with particular focus on the internationally recognized C2M2s: the U.S. Department of Energy's Cybersecurity Capability Maturity Model[20] (U.S. DoE C2M2) and its progeny, the NIST Cybersecurity Framework[21] (NIST Framework), the NICE-CMM[22] and the CERT Resilience Management Model[23] (CERT-RMM).

Part IV conducts a document analysis of Qatar's cybersecurity framework using publicly available documents. In Section V, the paper conducts a comparative analysis of existing C2M2s in light of the Qatari cybersecurity framework, including a comparative analysis of C2M2 literature, a thematic analysis and a summary of the lessons learned from the comparisons. Borrowing from the best features of existing C2M2s and considering Qatar's cybersecurity framework, Section VI of the paper proposes a Qatari Cybersecurity Capability Maturity Model (Q-C2M2) with a legislative framework. While the paper does not aim to propose a fully drawn Q-C2M2,

12. Ibid.
13. Involves a "cascading disruption or arrest of the functions of critical infrastructures or key assets through direct attacks on a critical node, system, or function." Ibid.
14. Involves a "cascading disruption and financial consequences for government, society, and economy through public and private sector reactions to an attack." Ibid.
15. Involves the "exploitation of elements of a particular infrastructure to disrupt or destroy another target." Ibid.
16. Myriam Dunn, *Information risks and countermeasures: Problems, prospects, and challenges of securing the information infrastructure*, in Theodor Winkler, Anja H Ebnöther, Ernst M Felberbauer (eds), *6th International Security Forum: Proceedings of the Conference* (Peter Lang, 2005), 78.
17. Krishnadev Calamur, *What just happened with Qatar?* The Atlantic, June 5, 2017, https://www.theatlantic.com/news/archive/2017/06/what-just-happened-with-qatar/529128/ (accessed October 15, 2017).
18. David Stewart, *Qatar's resilience - a lesson for all on how to respond positively to a crisis*, Gulf Times, October 10, 2017, http://www.gulf-times.com/story/566847/Qatar-s-resilience-a-lesson-for-all-on-how-to-resp (accessed October 17, 2017).
19. Qatar National Cybersecurity Strategy, May 2014, at 13, http://www.motc.gov.qa/en/documents/document/national-cyber-security-strategy (accessed 13 October 2017). ("QNCS").
20. U.S. Department of Energy and U.S. Department of Homeland Security, Cybersecurity capability maturity model (C2M2) v.1.1., February 2014, https://energy.gov/oe/services/cybersecurity/cybersecurity-capability-maturity-model-c2m2-program/cybersecurity (accessed October 16, 2017) ("U.S. DoE").
21. National Institute of Standards and Technology (NIST), Framework for improving critical infrastructure cybersecurity, February 12, 2014, https://www.nist.gov/cyberframework (accessed 17 October 2017).
22. National Initiative for Cybersecurity Education (NICE), Cybersecurity capability maturity model, October 3, 2012, https://www.tdisecurity.com/about-tdi/cybersecurity_education.pdf (accessed October 17, 2017).
23. Richard A. Caralli et al., CERT® Resilience Management Model, Version 1.2, Software Engineering Institute, February 2016, https://www.cert.org/resilience/products-services/cert-rmm/ (accessed October 17, 2017).

which would require further input from relevant cybersecurity stakeholders, the proposed Q-C2M2 provides a workable framework with a legislative component that improves the existing Qatari cybersecurity framework. Section VII discusses the legislative framework in more detail, weighing the need for a legislative mandate, the adoption of Q-C2M2, the role of the forthcoming CIIP law, and the embedded legal framework within the Q-C2M2 design. This paper argues for a legislatively mandated Q-C2M2 under a national security interest viewpoint. In an age when cybersecurity can be used as a pretext for a blockade, it becomes incumbent upon states to consider legislating the capability maturity measurement and development of their cybersecurity programs.

I. Capability Maturity Model and Cybersecurity

This section provides a general overview of the capability maturity model (CMM) with a discussion of its origin, purpose and characteristics. The section then discusses the applicability of the CMM to the cybersecurity field.

A. Origin and Purpose of the Capability Maturity Model

The Software Engineering Institute (SEI) at Carnegie Mellon University originally developed the capability maturity model (CMM) in the 1980s.[24] SEI first applied the CMM to create a simple assessment tool for measuring and thereafter improving the quality and progressive software process capabilities of software engineering.[25] Since then, other fields and industries, ranging from digital forensics to public management, have been inspired and have tailored the CMM to fit the unique needs of their discipline.[26]

The CMM measures the maturity of an organization's process capabilities through sequential levels that aim to improve the capabilities by achieving a targeted state.[27] Typically, a CMM consists of two components: (1) a means of sequentially measuring and describing hierarchical progression and (2) criteria for measuring the capabilities through conditions, processes, or application targets.[28] A CMM guides organizations by providing a set of criteria and a means of measuring progress through the maturity levels.[29] Therefore, an organization must undergo a number of process and quality improvements in several practice areas to achieve higher levels of capability in the evolutionary stages of the CMM.[30] As a process model, a CMM identifies a

24. Angel Marcelo Rea-Guamán et al., *Comparative study of cybersecurity capability maturity models*, in Antonia Mas et al. (eds), *Software Process Improvement and Capability Determination*, SPICE Conference 2017, Communications in Computer and Information Science, vol. 770 (Springer, 2017); Angel Marcelo Rea-Guamán et al., Maturity models in cybersecurity: A systematic review, 2017 12th Iberian Conference on Information Systems and Technologies (CISTI) (2017), 1–6.
25. Oscar González-Rojas, Dario Correal & Manuel Camargo, *ICT capabilities for supporting collaborative work on business processes within the digital content industry*, 80 Computers in Industry 16–29 (2016); Jörg Becker, Ralf Knackstedt & Jens Pöppelbuß, *Developing maturity models for IT Management: A procedure model and its application*, 1(3) Bus & Inf Systems Engineering 213–222 (2009); Gerrit Lahrmann et al., *Inductive design of maturity models: Applying the Rasch algorithm for design science research*, Service-Oriented Perspectives: Design Science Research, 176–191 (Springer, 2011); Roy Wendler, *The maturity of maturity model research: A systematic mapping study*, 54(12) Information and Software Tech 1317–1339 (2012).
26. See generally, Ronald L. Krutz, Methodology for assessing the maturity and capability of an organization's computer forensics processes, U.S. Patent Application 10/952537 (2006) (digital forensics); *The adoption and transformation of capability maturity models in government*, *in Encyclopedia of Information Science and Technology* (4th ed. 2018) (public management); see also Rea-Guamán et al. (n 22).
27. Becker et al. (n 23); Lahrmaan et al. (n 23); Paulk, Mark C. et al., *Capability maturity model version 1.1*, 10(4) IEEE Software 18–27 (1993).
28. Wendler (n 23); Siponen, Mikko, *Towards maturity of information security maturity criteria: Six lessons learned from software maturity criteria*, 10(5) Inf Management & Comp Security 210–224 (2002).
29. Ibid.
30. Buss (n 24).

structured collection of best practices in the field, as proven by experience that describes the characteristics of effective processes.[31] According to Buss, the stages of a CMM "are determined by research evidence, expert opinion, best practices and evaluations."[32]

According to Lahrmaan et al., a CMM's output can provide valuable pragmatic advice and guidance to decision makers on how to improve their capabilities.[33] A CMM, however, must be adaptive to remain relevant and useful,[34] especially because there is no universally agreed upon standard for CMM development and evaluation.[35] The CMM should follow an iterative process in development and evaluation and should include a means for self-assessment by relevant stakeholders and practitioners.[36]

Despite the CMM's significant contributions to improving quality and process, CMMs have been criticized for lacking a theoretical underpinning, for being too costly to implement, and for being subjective and unsuccessful in some organizations.[37] Further, because there is no agreed upon standard for developing and evaluating CMMs, it may be necessary to create an organization to study and vet a CMM's application.[38] Regardless, a number of public and private organizations, from Accenture to the U.S. Navy, have adopted CMMs to enhance their existing processes and raise awareness on the need for process improvement.[39] One field in which CMM is continuing to thrive is cybersecurity.

B. Applicability of the Capability Maturity Model in Cybersecurity

CMMs are germane in determining the capability maturity of cybersecurity organizations.[40] In cybersecurity, a CMM is typically referred to as a Cybersecurity Capability Maturity Model (C2M2). As stated by Chapin and Akridge, an organization's unsystematic implementation of cybersecurity practices increases risks and vulnerabilities.[41] A C2M2 can guide cybersecurity organizations to implement a consistent application, measurement, and improvement of information security controls; and to mitigate against risks and threats to critical infrastructures. A number of governments, such as those of the United States and Italy, have developed C2M2s, some with the aim of creating a national or international standard for cybersecurity capability maturity.[42] In Italy, the *Framework Nazionale per la Cyber Security* adopted a C2M2 approach based on the NIST Framework.[43] In the United States, companies and government agencies, such as Intel and the U.S. Department of Energy, have adopted C2M2s.[44] Sometimes compliance with

31. Rea-Guamán et al. (n 22).
32. Buss (n 24) 1.
33. Lahrmaan et al. (n 23).
34. Ibid.
35. Buss (n 24); Lahrmaan et al. (n 23).
36. Buss (n 24); Lahrmaan et al. (n 23); Becker et al. (n 23).
37. Buss (n 24).
38. Ibid.
39. Uzoka, Faith-Michael E., *A CMM assessment of information systems maturity levels in Botswana*, 16 MIS Rev 53–84 (2010). For a sample list of private and public organizations that have adopted the CMM, see CMMI Institute, Published appraisal results, https://sas.cmmiinstitute.com/pars/pars.aspx (accessed February 22, 2018).
40. Miron and Muita (n 10).
41. D.A. Chapin & S. Akridge, *How can security be measured?* 2 Information Systems Control J 43–47 (2005).
42. Wendler (n 23); Rea-Guamán et al. (n 22).
43. Framework Nazionale per la Cyber Security, Il cybersecurity report 2016, 2016, http://www.cybersecurityframework.it/ (accessed 22 February 2018). Italy adopted a cybersecurity framework based on the U.S. NIST Framework, which is focused on critical infrastructure.
44. Kip Boyle, International use of NIST Cybersecurity Framework, 2016, http://kipboyle.com/2016/05/international-use-of-nist-cybersecurity-framework/ (accessed 22 February 2018).

such financial regulations as the Sarbanes-Oxley Act in the United States may dictate the need for a systematic method for assessing and reporting internal control maturity.[45] By 2020, half of U.S. companies are expected to adopt C2M2s like the NIST Framework.[46]

As is the case with CMMs in general, there is no universally accepted standard for C2M2s. Nevertheless, although a number of C2M2s were initially designed to protect critical infrastructures, C2M2s can be applied to public and private organizations of all sizes and sectors. State entities and private businesses alike need to establish cybersecurity governance, culture and data management processes that adapt to the constantly evolving challenges posed by cybersecurity while maintaining minimal vulnerabilities to threats and ensuring an effective incident response and recovery.[47] C2M2s can help organizations evaluate and improve the capabilities of cybersecurity programs and policies and elevate them to higher levels of maturity.[48] In turn, various organizations have developed C2M2s tailored to their particular needs.[49] The lack of a universal standard for C2M2s further necessitates designing a C2M2 to fit the needs of a particular organization within the context of a particular national policy.

A C2M2 provides an organization with a structure that enables benchmarking of cybersecurity capabilities against a framework of recognized best practices, thus creating a foundation for consistent and systematic evaluation.[50] The C2M2 benchmark can help organizations assess the level of maturity of their cybersecurity practices and processes. Organizations can thereafter make comparisons of cybersecurity capabilities with other similarly situated organizations. Decision makers can also use the C2M2 as a guide to determine allocation of resources, prioritization and goal setting to support progression towards higher levels of capability maturity and the overall improvement in cybersecurity.[51]

C2M2s usually consist of three elements: (1) practice areas or domains, (2) objectives or indicators and (3) measures of maturity. A practice area or domain groups the common cybersecurity practices or processes of an organization. Each practice area or domain contains objectives that the organization must fulfill, and serves to visualize the progress towards the objectives.[52] The measures of maturity determine the maturity level of an organization's cybersecurity capabilities based on the quality of the practices, processes and policies concerning the objectives within a practice area or domain.[53] Most C2M2s have four levels of maturity, ranging from minimal, ad hoc, and early adoption of cybersecurity practices, processes, and policies; to intermediate documented cybersecurity practices, processes, and policies; to dynamic and adaptive cybersecurity practices, processes, and policies that can rapidly detect, respond, and recover from threats, risks, vulnerabilities, and organizational needs.[54]

45. R.S. Debreceny, Re-engineering IT internal controls: Applying capability maturity models to the evaluation of IT controls, *IEEE*, HICSS'06, Proceedings of the 39th Annual Hawaii International Conference on System Sciences 8: 196c–196c (2006).
46. Ibid.
47. Richard Adler, *A dynamic capability maturity model for improving cyber security*, 2013 IEEE International Conference on Technologies for Homeland Security (HST) (2014).
48. U.S. DoE (n 17); Rea-Guamán et al. (n 22).
49. Rea-Guamán et al. (n 22).
50. Adler (n 43).
51. NICE (n 19); Rea-Guamán et al. (n 22).
52. Rea-Guamán et al. (n 22).
53. Ibid.
54. Ibid.

II. Document Analysis of Cybersecurity Capability Maturity Models

A comparative analysis of existing C2M2s is necessary to arrive at a better understanding of the differences among the practice areas, objectives and measures of C2M2s. The comparative analysis will be useful for analyzing the Qatari policy on cybersecurity and for informing the proposal of a C2M2 tailored for Qatar.

A. Document Analysis Methodology

Because of the substantial practical benefits in terms of cost and time, and the lack of ethical constraints due to the public nature of the documents, outweighing the minimal risks of bias in the research, the author adopted a document analysis methodology to determine the content, level and areas of comparative inquiry. Document analysis is an accepted form of qualitative research in which the researcher interprets documents to give voice and meaning to an assessment topic.[55] A document analysis methodology would add validity and reliability to a comparative analysis of existing C2M2s, the primary aim of this research. Additionally, in proposing a C2M2 for Qatar, the secondary aim of this research, a document analysis of publicly available Qatari cybersecurity documents would make the research more relevant and useful.[56] Further, the paper will apply the diffusion of innovation theory to the proposed Qatari C2M2, as Miron and Muita have done.[57] A document analysis of publicly available Qatari cybersecurity documents along with a comparative analysis with existing C2M2s will increase the proposed Qatari C2M2's likelihood of success in attaining the following five factors in the diffusion of innovation theory: relative advantage, compatibility, simplicity, trialability and observability.

Document analysis requires coding content into themes and using a rubric to assess the documents.[58] For this paper, the author used types of documents widely recognized in document analysis methodology: public records of C2M2s, training materials, cybersecurity policy manuals, and peer-reviewed journals.[59] The author used multiple sources for triangulation, corroboration and bias reduction.[60] The author began by creating a planned process that consisted of (1) identifying the documents, (2) assessing the documents, (3) acknowledging and addressing bias, (4) ensuring credibility and (5) addressing ethical issues.[61]

Figure 1: Planned Process for Document Analysis

After gathering the documents, the author assessed the documents' authenticity, developed an organizational and management plan, and explored the documents' backgrounds, which included an analysis of tone, style, purpose and potential bias of the document's author. In addressing bias, for example, the author considered the number of authors, the purpose for the document, the document's audience, and the potential subjectivity and bias of the document's author(s). The author used thematic analysis to identify among the documents emerging themes, which

55. Glenn A Bowen, *Document analysis as a qualitative research method*, 9(2) Qual Research J 27–40 (2009).
56. The use of publicly available documents will be sufficient for purposes of this paper. Non-publicly available documents in Qatar will not likely be generalized policies or frameworks about cybersecurity. There is, therefore, a very low risk that non-publicly available documents would have a significant impact on the research, unless Qatar has already adopted a C2M2 and has not made it public. According to Dr. Noora Fetais, director of KINDI, Q-CERT uses CMMI, but there is no other indication that a C2M2 is being used in Qatar. Noora Fetais, director of KINDI Computer Research Center, Qatar University, email correspondence (October 19, 2017) (copy on file with the author); Q-CERT, About Q-CERT, 2017, http://www.qcert.org/about-q-cert (accessed October 18, 2017).
57. Miron and Muita (n 10).
58. Bowen (n 51).
59. Zina O'Leary, *The Essential Guide to Doing Your Research Project* (2nd ed., SAGE Publications, 2014).
60. Bowen (n 51).
61. O'Leary (n 54).

the researcher coded and categorized.[62] To maintain credibility and validity, the author of this paper maintained objectivity and avoided making assumptions about the documents and data.[63]

B. Cybersecurity Capability Maturity Models

While the author conducted a content and thematic analysis of a number of C2M2s, this paper will only cover in depth the most relevant C2M2s and those that the cybersecurity field has recognized nationally and internationally. For example, the author did not give substantial treatment to early examples of C2M2s, such as the International Organization for Standardization's Systems Security Engineering Capability Maturity Model (SSE-CMM);[64] and C2M2s that have not received widespread recognition and adoption, such as the Maqasid al-Shari'ah C2M2.[65] Instead, this paper focuses on comparing only the following four widely recognized[66] C2M2 initiatives: (1) the U.S. DoE's C2M2, (2) the NICE-CMM, (3) the CERT-RMM and (4) the NIST Framework. The author will discuss the main features of these four C2M2s with the aim of later conducting a comparative analysis based on the results of the document analysis.

Table 1: Overview of Cybersecurity Capability Maturity Models

Model Name	U.S. C2M2s	NICE-CMM	CERT-RMM	NIST Framework
Organization	U.S. Department of Energy	U.S. Department of Homeland Security	Software Engineering Institute (SEI)	U.S. National Institute of Standards and Technology
Purpose	any organization	workforce planning	any organization	critical infrastructure
Number of Domains	10	3	26	22
Number of Maturity Levels	4	4	3	4

1. U.S. DoE Approach: C2M2, ES-C2M2, ONG-C2M2

The U.S. Department of Energy collaborated with Carnegie Mellon University to create the Cybersecurity Capability Maturity Model (C2M2),[67] the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2),[68] and the Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model (ONG-C2M2)[69] in 2014.[70] The U.S. DoE designed the three C2M2s to measure the sophistication and sustainability of cybersecurity programs. However, it is important

62. Bowen (n 51).
63. Ibid.
64. Karen Ferraiolo, The Systems Security Engineering Capability Maturity Model (SSE-CMM), International Systems Security Engineering Association (ISSEA), 2000, https://csrc.nist.gov/csrc/media/publications/conference-paper/2000/10/19/proceedings-of-the-23rd-nissc-2000/documents/papers/916slide.pdf (accessed October 12, 2017).
65. Jamaludin Ibrahim et al., A cybersecurity capability maturity model based on Maqasid Shari'ah (MS-C2M2), International Conference on Maqasid Al-Shari'ah in Public Policy and Governance (IAIS Malaysia, 2015).
66. See Rea-Guamán et al. (n 22).
67. U.S. DoE (n 17).
68. U.S. Department of Energy, Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) v.1.1., February 2014, https://energy.gov/oe/cybersecurity-capability-maturity-model-c2m2-program/electricity-subsector-cybersecurity (accessed October 17, 2017) ("U.S. DoE ES-C2M2").
69. U.S. Department of Energy, Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model (ONG-C2M2) v.1.1., February 2014, https://energy.gov/oe/cybersecurity-capability-maturity-model-c2m2-program/oil-and-natural-gas-subsector-cybersecurity (accessed October 17, 2017) ("U.S. DoE ONG-C2M2").
70. The U.S. DoE developed the C2M2 from the precursor Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) by removing sector-specific language. The Electricity Sector Cybersecurity Capability Maturity Model (ES-C2M2) is tailored to the energy subsector, particularly those supplying electric power. The ES-C2M2 includes the core C2M2, additional reference materials, and implementation guidance specifically tailored for the electricity subsector. Likewise, U.S. DoE derived the Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model (ONG-C2M2) from the ES-C2M2. The ONG-C2M2 is tailored to the oil and natural gas subsector. A thematic analysis of the three documents shows that differences exist in the section of the documents providing sector-specific background and in the sector-specific examples used in the domains. As such, the author treated the C2M2, ES-C2M2, and the ONG-C2M2 as a unified group of C2M2 documents. U.S. DoE (n 17); Rea-Guamán et al. (n 22); U.S. DoE ES-C2M2 (n 63); U.S. DoE ONG-C2M2 (n 64); Rahul Gupta, The challenges and recommended steps to improve cybersecurity within industrial control systems, Wood Group Mustang,→

to note that these C2M2s are voluntary public–private partnership programs.[71] Because the original C2M2 was made for the electricity subsector, those who created the model were experts in either public or private energy sector subject matter, and decisions to include or not include certain domains within the C2M2s may have been driven by this background.[72] While the ES-C2M2 and the ONG-C2M2 are sector specific, the C2M2 aims to assess the cybersecurity capabilities of any organization using a maturity model and evaluation tool. The three C2M2s are organized the same way. As shown in Table 1 and Table 2, the C2M2 features ten domains in a logical grouping of cybersecurity practices. The ten domains are measured in four levels of maturity: MIL-O, MIL-1, MIL-2, and MIL-3.[73] According to the C2M2 document, the C2M2 provides a descriptive rather than a prescriptive guidance that is presented at a higher level of abstraction to allow for interpretation and adaptability.[74]

Table 2: Ten Domains in the C2M2[75]

Risk Management (RM)	Asset, Change, and Configuration Management (ACM)	Identity and Access Management (IAM)	Threat and Vulnerability Management (TVM)	Situational Awareness (SA)
Information Sharing and Communications (ISC)	Event and Incident Response, Continuity of Operations (IR)	Supply Chain and External Dependencies Management (EDM)	Workforce Management (WM)	Cybersecurity Program Management (CPM)

2. NICE Approach: NICE-CMM

The U.S. Department of Homeland Security's National Initiative for Cybersecurity Education ("NICE") created the NICE Capability Maturity Model or NICE-CMM and focuses on cybersecurity workforce planning.[76] The NICE-CMM "leveraged the structure and foundational principals of" other workforce planning capability maturity models "to develop its own cybersecurity workforce planning capability maturity model."[77] The NICE-CMM divides key activities into three main areas: (1) process and analytics, (2) integrated governance, and (3) skilled practitioners and enabling technology.[78] The NICE-CMM ranks an organization's cybersecurity with three levels of maturity: limited, progressing, or optimizing.[79] The NICE-CMM focuses only on cybersecurity workforce planning, process maturity and operational resilience. As Miron and Muita aptly observe, the NICE-CMM does not offer specific cybersecurity best practices and will require additional cybersecurity frameworks to do so.[80] The model will be most useful as a supplement to existing C2M2s or when incorporated into a C2M2 that needs a more robust cybersecurity workforce planning. According to Rea-Guamán et al., use of the NICE-CMM will

Petroleum and Power Automation (PPA) Meet, New Delhi, India, 2016, https://www.woodgroup.com/__data/assets/pdf_file/0011/3143/2016-04-ISA-Delhi-power-and-petroleum.pdf (accessed October 1, 2017).
71. U.S. DoE (n 17).
72. Ibid.
73. Rea-Guamán et al. (n 22); U.S. DoE (n 17).
74. Rea-Guamán et al. (n 22).
75. See U.S. DoE (n 17).
76. NICE (n 19).
77. Ibid.
78. Ibid.
79. Ibid.
80. Miron and Muita (n 10).

require an accurate understanding of current staffing capabilities in the three activity areas, and organizations undertaking such C2M2s must be able to provide specific evidence of the activities.[81]

3. CERT Approach: CERT-RMM

Carnegie Mellon's Software Engineering Institute (SEI) developed the Computer Emergency Response Team Resilience Management Model (CERT-RMM) for a broad range of organizations that aim to improve operational resilience, security, and business continuity. CERT-RMM uses a resilience approach to help organizations manage operational risks "to critical assets by optimizing both protection and continuity strategies."[82] As shown in Table 1 and Table 3, CERT-RMM uses 26 domains, called practice areas and has three levels of maturity: Generic Goals 1 (operational resilience management system achieves specific goals), Generic Goals 2 (the process is institutionalized as a managed process) and Generic Goals 3 (the process is institutionalized as a defined process).[83]

Table 3: CERT-RMM Domains

ENGINEERING		**OPERATIONS MANAGMENT**	
ADM	Asset Definition and Management	AM	Access Management
CTRL	Controls Management	EC	Environmental Control
RRD	Resilience Requirements Development	EXD	External Dependencies
RRM	Resilience Requirements Management	ID	Identity Management
RTSE	Resilience Technical Solution Engineering	IMC	Incident Management and Control
SC	Service Continuity	KIM	Knowledge and Information Management
ENTERPRISE MANAGEMENT		PM	People Management
COMM	Communications	TM	Technology Management
COMP	Compliance	VAR	Vulnerability Analysis and Resolution
EF	Enterprise Focus	**PROCESS MANAGEMENT**	
FRM	Financial Resources Management	MA	Measurement and Analysis
HRM	Human Resources Management	MON	Monitoring
OTA	Organizational Training and Awareness	OPD	Organizational Process Definition
RISK	Risk Management	OPF	Organizational Process Focus

4. NIST Approach: NIST Cybersecurity Framework

The U.S. Department of Commerce's National Institute of Standards and Technology (NIST) created the NIST Cybersecurity Framework to improve critical infrastructures.[84] Based on globally recognized effective standards, guidelines, and practices, all of which is referenced in the document, the NIST Cybersecurity Framework provides a set of cybersecurity activities designed to address the need for a common cybergovernance methodology.[85] The NIST Cybersecurity Framework allows organizations of all sizes and sophistications to apply the principles and

81. Rea-Guamán et al. (n 22).
82. CERT, Cyber risk and resilience management: Overview, 2017, https://www.cert.org/resilience/ (accessed October 12, 2017).
83. Caralli (n 20).
84. NIST (n 18).
85. Ibid.

best practices of cybersecurity risk management to improve the cybersecurity and resilience of critical infrastructures.[86] NIST aimed to make the framework suitable for use outside the United States and as a model for international cooperation.[87] However, NIST cautions that the framework is not to be used as a one-size-fits-all approach and encourages organizations to consider unique threats, vulnerabilities and risk tolerances when tailoring the framework to fit a specific organization's critical cybersecurity needs, priorities, and financial resources.[88] Notably, the NIST Framework includes a methodology to protect privacy and civil liberties when cybersecurity operations are conducted, and proposes a set of processes and activities that address privacy and civil liberties implications. The NIST Framework also encourages organizations to add categories and subcategories as needed based on unique organizational risks, and to incorporate emerging risks, threats, and vulnerabilities. The NIST Framework is voluntary and not legislatively required. As shown in Tables 1 and 4, the NIST Cybersecurity Framework consists of five framework core functions subdivided into 22 total categories.[89] The framework has four tiers or levels of maturity: (1) partial, (2) risk informed, (3) repeatable and (4) adaptive.[90]

Table 4: NIST Cybersecurity Framework Core Functions and Categories

IDENTIFY	Asset Management
	Business Environment
	Governance
	Risk Assessment
	Risk Management Strategy
PROTECT	Access Control
	Awareness and Training
	Data Security
	Information Protection Processes and Procedures
	Maintenance
	Protective Technology
DETECT	Anomalies and Events
	Security Continuous Monitoring
	Detection Processes
RESPOND	Response Planning
	Communications
	Analysis
	Mitigation
	Improvements
RECOVER	Recovery Planning
	Improvements
	Communications

5. Other C2M2s and Related CMMs Considered

In addition to the above C2M2s, the author analyzed documents related to other C2M2s and CMMs that concerned cybersecurity. In the end, the author categorized these documents as supplemental sources that could enhance the comparison of the primary C2M2 documents.

86. Ibid.
87. Ibid.
88. Ibid.
89. Each of the categories are further divided into subcategories that are then referenced to globally accepted standards, guidelines, and practices.
90. Ibid.

Notably, the University of San Antonio's Center for Infrastructure Assurance and Security (CIAS) developed the Community Cyber Security Maturity Model (CCSMM) to address the cybersecurity needs of state and local communities as in the cases of the Virginia health agency that was hacked in 2009[91] and a town's water system in Queensland, Australia in 2000.[92] The CCSMM aims to create a viable and sustainable program tailored towards the unique needs of nations, states, communities, and organizations. This model uses aspects such as cybersecurity awareness, security policies and procedures, inter and intra organization information sharing, and cybersecurity development through training and education.[93] As a three-dimensional model, the CCSMM also depicts the various levels of communities to include the nation, state, community, and organization.[94] The CCSMM uses the following five levels to determine the level of capability maturity: (1) initial, (2) established, (3) self-assessed, (4) integrated, and (5) vanguard.[95]

The author also considered the Systems Security Engineering Capability Maturity Model (SSE-CMM);[96] ISO standards[97] like the ISO/IEC 15408, ISO/IEC 27001, and ISO/IEC 21827; the Information Security Management Maturity Model (ISM3);[98] the Control Objectives for Information and Related Technology (COBIT); [99] Adler's Dynamic Capability Maturity Model;[100] Barclay's Cybersecurity Capability Maturity Model (CM^2);[101] and the Holistic Cybersecurity Implementation Framework.[102] However, other C2M2s have not gained the same level of global recognition as the four C2M2s discussed in more detail earlier.

III. Document Analysis of Qatari Cybersecurity Framework

In addition to a document analysis of existing C2M2s, a document analysis of publicly available Qatari cybersecurity documents would benefit the paper on two points. First, it would allow for a determination of whether Qatar has adopted a C2M2 framework for cybersecurity benchmarking and process development purposes. Second, it would allow for a cross-comparison of the results of the document analysis of existing globally recognized C2M2 documents and existing Qatari cybersecurity practices, processes, and policies.

---

91. White (n 21); Rea-Guamán et al. (n 22); Jaikumar Vijayan, *Web site offline as police, FBI investigate $10M extortion bid*, Computer World, May 7, 2009, www.computerworld.com/s/article/9132678/Web_site_offline_as_police_FBI_investigate_10M_extortion_bid (accessed February 22, 2018).
92. Todd Datz, *SCADA system security: Out of control*, CSO Online, August 1, 2004, www.csoonline.com/article/219486/scada-system-security-out-of-control (accessed February 22, 2018).
93. Ibid.
94. Ibid. Though not specifically designed for cybersecurity but rather security engineering, the SSE-CMM is worth considering because some organizations have adapted it for use in cybersecurity.
95. Ibid.
96. Ferraiolo (n 59); Rea-Guamán et al. (n 22). Like the CCSMM, the SSE-CMM uses five levels to assess the maturity capability of an organization: (1) performed informally, (2) planned and tracked, (3) well defined, (4) quantitatively controlled, and (5) continuously improving.
97. Miron and Muita (n 10); Rea-Guamán et al. (n 22); NIST (n 18). While not a CMM, ISO standards provide prescriptive guidance for cybersecurity readiness. Unfortunately, ISO standards are complicated and costly to deploy. The NIST Framework referenced many of the ISO standards including ISO/IEC 15408, ISO/IEC 27001, and ISO/IEC 21827. The ISO/IEC 15408 is the criteria for computer security certification. ISO/IEC 27001 provides guidance and specifications for establishing an Information Security Management System (ISMS) in a company. It does not, however, offer a C2M2. ISO/IEC 21827 deals with the evaluation of software engineering processes.
98. Ibid. The Information Security Management Maturity Model (ISM3) focuses on the management of information security metrics and does not deal directly with cybersecurity.
99. Ibid. COBIT focuses on IT governance and does not fully address the issue of cybersecurity.
100. Adler (n 43).
101. Corlane Barclay, Sustainable security advantage in a changing environment: The Cybersecurity Capability Maturity Model (CM2), Proceedings of the 2014 ITU Kaleidoscope Academic Conference: Living in a converged world – Impossible without standards? (July 21, 2014).
102. Issa Atoum, Ahmed Ali Otoom & Amer Abu Ali, *A holistic cyber security implementation framework*, 22 Information Management & Computer Security 3, 251–264(14) (2014).

The Qatar National Information Assurance Framework[103] (NIAF) is the officially recognized national cybersecurity framework for implementing globally recognized cybersecurity standards. The NIAF provides a national governance roadmap for cybersecurity in Qatar. The NIAF consists of policies, standards, and guidelines. At the top of the NIAF is cybersecurity legislation that includes the Electronic Commerce and Electronic Signatures Law,[104] the Cybercrime Law,[105] the Data and Privacy Protection Law,[106] and the Critical Information Infrastructure Protection (CIIP) Law[107] (still in draft form). Supplementing the laws are cybersecurity policies that include, among others, the Qatar National Information Assurance Policy (NIAP),[108] Qatar National Information Assurance Manual (NIAM),[109] the National Information Classification Policy (NICP),[110] and the Information Security for Schools Policy.[111] The NIAF also covers technology standards and best practices.

Qatar also implemented a National Cybersecurity Strategy in 2014 with an action plan from 2014 to 2018.[112] However, Qatar does not currently have an officially recognized national or sector-specific benchmarking model to measure cybersecurity practice, process, and policy development.[113] Qatar's Computer Emergency Response Team (Q-CERT), a government-sponsored organization under the auspices of the Ministry of Transport and Communications, which assesses the current state of cybersecurity efforts in Qatar, is known to have used the System Engineering Institute's Capability Maturity Model Initiative (CMMI).[114] However, the CMMI is not a C2M2, and Q-CERT does not seem to be using the CERT-RMM model. There may be incompatibility with the CMMI and the CERT-RMM in application.[115] Therefore, a Qatari C2M2 would be an appropriate addition to the Qatar cybersecurity strategy and framework.

---

103. Q-CERT, Qatar National Information Assurance Framework 2014, available in English, http://www.itu.int/ITU-D/cyb/events/2008/brisbane/docs/lewis-qatar-national-strategy-brisbane-july-08.pdf (accessed February 22, 2018).
104. Qatar Decree Law No (16) of 2010 on the Promulgation of the Electronic Commerce and Transactions Law, available in English at Al Meezan http://www.almeezan.qa/LawPage.aspx?id=2678&language=en (accessed February 22, 2018).
105. Qatar Cybercrime Law, Decree Law No (14) of 2014, available in pdf (Arabic) at International Labour Organization (ILO) http://www.ilo.org/dyn/natlex/natlex4.detail?p_lang=en&p_isn=100242 (accessed February 22, 2018).
106. Qatar Data and Privacy Protection Law, Decree Law No (13) of 2016, available in pdf (English) at Sultan Al-Abdullah and Partners https://qatarlaw.com/wp-content/uploads/2017/05/Personal-Data-Privacy-Law-No.-13-of-2016.pdf (accessed February 22, 2018).
107. Qatar Critical Information Infrastructure Protection Law (CIIP) (not yet published). The law awaits signature by the emir as of the writing of this paper.
108. Ministry of Information and Communications Technology, National Information Assurance Policy, 2014, http://www.qcert.org/library/36 (accessed October 17, 2017) ("NIAP").
109. Ministry of Information and Communications Technology, National Information Assurance Manual, 2014, http://www.qcert.org/library/36 (accessed October 17, 2017) ("NIAM").
110. Ministry of Information and Communications Technology, National Information Classification Policy, 2014, http://www.qcert.org/library/36 (accessed October 17, 2017) ("NICP").
111. Ministry of Information and Communications Technology, Information Security Framework for School Networks, 2014, http://www.qcert.org/library/36 (accessed October 17, 2017).
112. QNCS (n 16).
113. International Telecommunications Union, Cyberwellness profile: Qatar, in Global Cybersecurity Index & Cyberwellness Profiles: Report, 382, *ABI Research*, 2015, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf (accessed October 17, 2017); ITU, 'Cyberwellness Profile: Qatar' (2014) http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Qatar.pdf (accessed October 17, 2017).
114. Noora Fetais, director of KINDI Computer Research Center, Qatar University, email correspondence (October 19, 2017) (copy on file with the author); Q-CERT, About Q-CERT, 2017, http://www.qcert.org/about-q-cert. (accessed October 18, 2017).
115. Matthew J. Butkovic & Richard A. Caralli, Advancing cybersecurity capability measurement using the CERT®-RMM maturity indicator level scale, Software Engineering Institute, Carnegie Mellon University Research→-Showcase, 2013, http://repository.cmu.edu/cgi/viewcontent.cgi?article=1766&context=sei (accessed October 18, 2017) (stating that "[w]hile the CMMI maturity levels and descriptions are a good fit for CERT-RMM, in practice the spacing between levels often causes CERT-RMM practitioners some difficulty.").

In 2014, Qatar did issue the National Information Assurance Policy (NIAP), which consists of the National Information Classification Policy (NICP)[116] and the National Information Assurance Manual (NIAM).[117] NICP provides a high-level information classification methodology for Qatari state entities that allows for the determination of corresponding values, risks, and protection a state entity must apply to information.[118] NIAM, supplemented by the Guidance for Assurance Manual (GFAM),[119] provides a baseline for controls that an organization should implement at minimum to protect its information system.[120] NIAM is designed to be used in conjunction with the NICP and the applicable laws and regulations within the State of Qatar.[121] NIAM only applies to government agencies and corresponding assets with an NICP classification higher than I0, A0, and C0.[122] Like C2M2s, NIAM categorizes cybersecurity practices and processes into 26 domains.[123]

NIAM, however, does not include a method to measure the maturity of Qatar's cybersecurity process, practices, and policies. In short, NIAM is not a C2M2. However, that NIAM sets outs the policy objectives and baseline controls of 26 domains covering cybersecurity practices, processes, and policies applicable to Qatari state agencies makes it an ideal starting point for a comparison with existing C2M2s and towards a Qatari C2M2.

IV. Comparative Analysis of Existing Cybersecurity Capability Maturity Models in Light of the Qatari Cybersecurity Framework

A. Comparative Analysis of C2M2s in the Literature

A number of researchers, whether to propose a C2M2 as in the case of Miron and Muita[124] or to conduct a comparative study as in the case of Rea-Guamán et al.,[125] have compared existing C2M2 models. According to Miron and Muita, analysis and comparison of existing C2M2s can "provide the stages for an evolutionary path to developing policies and processes" for cybersecurity benchmarking, measurement, and development.[126] While recognizing the robustness of the NIST Framework, Miron and Muita also criticized it for relying on operators "to voluntarily develop individual profiles."[127] Additionally, they criticized existing C2M2s for their lack of specificity in providing only high-level advice, and for being designed by and for specific industries.[128] Furthermore, while they provide specific standards for cybersecurity readiness, the ISO standards, according to Miron and Muita, are complex, expensive, and time consuming to implement.[129] For these reasons, Miron and Muita proposed a C2M2 specifically for municipal critical infrastructure.[130]

116. NIAP (n 143).
117. Ministry of Information and Communications Technology and Q-CERT, National Information Assurance Manual [2014] http://www.qcert.org/sites/default/files/public/documents/nia_policy__manual_english_v2.0_0.pdf (accessed December 12, 2018) ("NIAM").
118. NICP (n 129).
119. Qatar Ministry of Transport and Communications, 'Guidance for Assurance Manual v.2.0' (2014) http://www.motc.gov.qa/sites/default/files/guidance_nia_manual-v2.0_english_1.pdf (accessed 17 October 2017.
120. NIAM (n 135).
121. Ibid.
122. Ibid.
123. Ibid. See Table 5 for a list of NIAM domains.
124. Miron and Muita (n 10).
125. Rea-Guamán et al. (n 22).
126. Miron and Muita (n 10).
127. Ibid.
128. Ibid.
129. Ibid.
130. Ibid.

Rea-Guamán et al. conducted a taxonomical comparative analysis of C2M2s that they considered the most widely mentioned in academic journals: C2M2, SSE-CMM, CCSMM, and NICE.[131] Rea-Guamán et al. largely agree with Miron and Muita's analysis that existing C2M2s require customization, some requiring dual implementation with the NIST Framework. For Rea-Guamán et al., the only C2M2 model designed specifically for cybersecurity is the C2M2.[132] Rea-Guamán et al. also recognized the SSE-CMM as the only one along with the U.S. DoE's C2M2 that specifically focuses on risk management, even though all C2M2s are based on cybersecurity risk management.[133] The SSE-CMM, however, is not designed specifically for cybersecurity but rather for security engineering processes.[134]

Researchers agree that implementation and management of existing C2M2s requires a specialized skill set and is a complicated, expensive, and time-consuming endeavor.[135] Even with the choices among the existing C2M2s, an organization needs to refine and tailor the C2M2 and the organization's processes to implement the chosen C2M2.[136] For this reason, the author proposes that designing a C2M2 for Qatar around already existing processes in the NIAP would minimize these concerns. A proposed Q-C2M2 that already takes into account the existing domains and practices in the NIAP would make it less complicated and less expensive to adopt. Such a Q-C2M2 would also save time, as it would make use of existing personnel with specialized skill sets already available in Qatar.[137]

B. Thematic Analysis of C2M2s and the Qatar Cybersecurity Framework

Having discussed the literature and compared the C2M2s, the paper can now build on previous taxonomical or generalized comparative analysis by analyzing the thematic elements of existing C2M2s and Qatar's cybersecurity framework. Table 5 compares C2M2 domains and adds Qatar's NIAP domains listed under NIAM.

Table 5: Comparison of Domains of Cybersecurity Capability Maturity Models

Model Name	U.S. C2M2s	NICE-CMM	CERT-RMM	NIST Framework	Qatar NIAM/NIAP
Domains	Risk Management	Process and Analytics	Asset Definition and Management	Asset Management	Access Control Security
	Asset, Change, and Configuration Management	Integrated Governance	Controls Management	Business Environment	Audit and Certification
	Identity and Access Management	Skilled Practitioners and Enabling Technology	Resilience Requirements Development	Governance	Business Continuity Management
	Threat and Vulnerability Management		Resilience Requirements Management	Risk Assessment	Change Management
	Situational Awareness		Resilience Technical Solution Engineering	Risk Management Strategy	Communications Security
	Information Sharing and Communications		Service Continuity	Access Control	Cryptographic Security
	Event and Incident Response, Continuity of Operations		Communications	Awareness and Training	Data Labeling
	Supply Chain and External Dependencies Management		Compliance	Data Security	Data Retention and Archival

131. Rea-Guamán et al. (n 22).
132. Ibid.
133. Ibid.
134. Rea-Guamán et al. (n 22).
135. Rea-Guamán et al. (n 22); Miron and Muita (n 10).
136. Ibid.
137. The Q-C2M2 proposed in Section VI addresses these concerns, as discussed in more detail in relation to the diffusion of innovation theory. See infra Section VI(A).

Domains	Workforce Management	Skilled Practitioners and Enabling Technology	Enterprise Focus	Information Protection Processes and Procedures	Documentation
	Cybersecurity Program Management		Financial Resources Management	Maintenance	Gateway Security
			Human Resources Management	Protective Technology	Governance Structure
			Organizational Training and Awareness	Anomalies and Events	Incident Management
			Risk Management	Security Continuous Monitoring	Information Exchange
			Access Management	Detection Processes	Logging, Auditing, and Security Monitoring
			Environmental Control	Response Planning	Media Security
			External Dependencies	Communications	Network Security
			Identity Management	Analysis	Personnel Security
			Incident Management and Control	Mitigation	Physical Security
			Knowledge and Information Management	Improvements	Portable Device and Working Off-Site Security
			People Management	Recovery Planning	Product Security
			Technology Management	Improvements	Risk Management
			Vulnerability Analysis and Resolution	Communications	Security Awareness
			Measurement and Analysis		Software Security
			Monitoring		System Usage Security
			Organizational Process Definition		Third Party Security Management

The most striking thematic organization of existing C2M2s is the NIST Framework, which organizes the framework into the five core functions of cybersecurity: identify, detect, protect, respond, and recover.[138] After the coding and analysis of the core functions of the NIST Framework, the thematic analysis revealed that the five words repeat thematically in the NIST Framework, the U.S. DoE's C2M2, and the CERT-RMM. These words do not exist thematically in the NICE-CMM. In Qatar's NIAP and National Cybersecurity Strategy, the five words appear thematically.[139] However, there is one glaring observation: the word "respond" only appears once in the NIAP and is not a thematic element. Additionally, the theme "critical infrastructure" is prevalent in the NIST Framework and the U.S. DoE's C2M2, but the term does not appear in the CERT-RMM and the NICE-CMM. In the Qatari cybersecurity framework, critical infrastructure is an important element and falls under the Qatar NIAF, for which Qatar is in the draft stages of the CIIP Law. The Qatar cybersecurity framework refers to critical infrastructure as "critical information infrastructure." Critical infrastructure or critical information infrastructure appear in the Qatar National Cybersecurity Strategy, the NIAF, and the NIAP. Interestingly, in the NIAP neither critical infrastructure nor critical information infrastructure appears as a thematic element, but only as a reference to the CIIP Law.

"Risk management" appears as a thematic element in the NIST Framework, the U.S. DoE's C2M2, and the CERT-RMM, but does not appear in the NICE-CMM. Risk management also appears in the Qatar National Cybersecurity Strategy and the NIAP. "Data security" is a thematic element

138. NIST (n 18).
139. See generally NIAP (n 143); QNCS (n 16).

in the NIST Framework and the CERT-RMM, but is not in the U.S. DoE's C2M2 nor in the NICE-CMM. The NIST Framework defines data security as "information and records (data) managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information."[140] In the Qatar cybersecurity framework, data security is not a thematic element and does not appear in the documents. This is interesting because "security" is a thematic element in the NIAP, which covers 12 of the 26 domains on different types of security practices but does not cover data security specifically.[141] Instead, the NIAP deals with data security implicitly in separated and ad-hoc practices such as logging and classification.

"Asset" is a thematic element in the NIST Framework, the U.S. DoE's C2M2, and the CERT-RMM, but does not appear in the NICE-CMM. Asset is also a thematic element in the Qatar cybersecurity framework, including in the NIAP and in the Qatar National Cybersecurity Strategy. However, while the NIAP recognizes asset as a thematic element and thus includes a classification policy for information assets, the NIAP lacks an asset management plan similar to those in the NIST Framework, the U.S. DoE's C2M2, and the CERT-RMM. Additionally, "governance" and "training" are thematic elements that appear in all the C2M2s and the Qatar cybersecurity framework, including the NIAP and the Qatar National Cybersecurity Strategy.

Table 6: Sample Thematic Analysis of C2M2 Documents and Qatar's Cybersecurity Framework Documents

Themes Analyzed	U.S. C2M2s	NICE-CMM	CERT-RMM	NIST Framework	Qatar National Cyber-security Strategy	NIAP
identify	YES	NO	YES	YES	YES	YES
detect	YES	NO	YES	YES	YES	YES
protect	YES	NO	YES	YES	YES	YES
respond	YES	NO	YES	YES	YES	YES
recover	YES	NO	YES	YES	NO	NO
critical infrastructure	YES	NO	NO	YES	YES	NO
risk management	YES	NO	YES	YES	YES	YES
data security	NO	NO	YES	YES	NO	NO
asset	YES	NO	YES	YES	YES	YES
governance	YES	YES	YES	YES	YES	YES
training	YES	YES	YES	YES	YES	YES

C. Lessons Learned from the Comparative Analysis

The thematic and comparative analysis of the documents reveals important lessons about both the existing C2M2s and Qatar's cybersecurity framework.

That "respond" is not a thematic element in the NIAP signals that the respond core function of the NIAP may need improvement. A Q-C2M2 that uses the NIST Framework's core functions would benefit the benchmarking and development of Qatar's cybersecurity framework.

Concerning critical infrastructure, that Qatar uses the terminology "critical information infrastructure" may signal Qatar's potential for a limited definition of "critical infrastructure" in the CIIP Law or a similar approach as the CCSMM's "critical cyber infrastructure." As

140. NIST (n 18).
141. NIAP uses the word "security" for the following domains: Access Control Security, Cryptographic Security, Gateway Security, Media Security, Network Security, Personnel Security, Physical Security, Portable Device and Work Off-Site Security, Product Security, Software Security, System Usage Security, and Third Party Security.

mentioned in the introduction, however, it is important to recognize the interdependent nature of cybersecurity, and that critical infrastructures could include cyber interdependent sectors like food, transportation, information and communication technologies, energy and utilities, financial systems, health, and government.[142] Notably, that the NIAP only gives passing reference to the theme "critical infrastructure" or "critical information infrastructure" means that the NIAP will need improvements to cover critical information infrastructure, especially to meet the requirement of the CIIP Law once it is enacted.

When comparing NIAP with existing C2M2s, it becomes clear that NIAP lacks certain domains and activities deemed essential according to globally recognized standards and practices. One reason may be that NIAP is not a C2M2 but rather a policy for enhancing the security of information.[143] Nevertheless, the comparative analysis identified areas for improving NIAP. The comparative analysis revealed, among other discoveries, the importance of adding compliance, protective technology, awareness and training, mitigation, improvement, and communication in a C2M2 designed for Qatar, as shown in Table 8.

One of the most important aims is to add more explicit domains and activities relating to organizational response to a cybersecurity incident. The NIST Framework's mitigation and communication domains would bolster NIAP and make it more resilient. NIAP's governance domain also lacks focus on legal and regulatory compliance, and financial planning. NIAP also lacks domains relating to maintenance and improvement, which are present in the NIST Framework and the CERT-RMM.

Table 7: Sample Comparison of C2M2 with Qatar's NIAP

NIST Core Functions	U.S. C2M2s	NICE-CMM	CERT-RMM	NIST Framework	NIAP
Identify	NONE	NONE	Compliance	NONE	NONE
Identify	NONE	NONE	Financial Resource Management	NONE	NONE
Identify	NONE	NONE	Measurement and Analysis	NONE	NONE
Protect	Threat and Vulnerability Management	NONE	Vulnerability Analysis and Resolution	NONE	NONE
Protect	Threat and Vulnerability Management	NONE	Controls Management	Maintenance	NONE
Protect	Threat and Vulnerability Management	NONE	Resilience Requirements Development	Protective Technology	NONE
Protect	Workforce Management	Process and Analytics	Human Resource Management	Awareness and Training	NONE
Protect	Workforce Management	Trained professionals and enabling technology	People Management	Awareness and Training	NONE
Respond	Event and Incident Response, Continuity of Operations	NONE	Incident Management and Control	Analysis	NONE
Respond	Event and Incident Response, Continuity of Operations	NONE	NONE	Mitigation	NONE
Recover	Information Sharing and Communications	NONE	Communications	Communications	NONE

142. Miron and Muita (n 10).
143. NIAP (n 143); NIAM (n 135). NIAM states that it "provides, baseline controls which an organization should implement at minimum to protect their information system."

V. Qatar Cybersecurity Capability Maturity Model (Q-C2M2)

As stated above, this paper conducted a document analysis of the most prominent and proven C2M2s, and compared the domains of those C2M2s to Qatar's cybersecurity framework, by taking into account Qatar's NIAM. One of the paper's main aims is to propose a Qatar C2M2 or Q-C2M2 with a legislative framework. This section examines the potential contribution of the Q-C2M2 to the Qatari cybersecurity framework, and discusses the likelihood of adoption by applying the diffusion of innovation theory. The section concludes with a discussion of the domains and measures of the Q-C2M2.

It should be noted that this paper does not propose a predetermined set of activities for each of the domains. Rather, the paper provides a workable framework of domains and subdomains based on existing C2M2s with the hope that potential adopters of the Q-C2M2, when establishing an initial benchmark, would look through the activities in existing C2M2s and reconcile those activities with the adopting organization's existing cybersecurity activities, profile, and risk tolerance. As in capacity building, the implementation method will differ for each organization, and as such, "the participation of senior decision makers across all areas of the company is critical."[144] Likewise, the building of the Q-C2M2 should take a comprehensive approach that includes the participation of decision makers, and is tailored to the organization's existing cybersecurity program.

Borrowing from a feature of the CCSMM, the Q-C2M2 is designed for applicability across dimensions within the Qatari context, and this section discusses Q-C2M2's applicability in public, private, and personal dimensions. The section then proposes a legislative framework for the implementation of Q-C2M2.

A. Contribution of Q-C2M2 and the Diffusion of Innovation Theory

Utility and validity will largely determine whether an organization will accept a proposed CMM.[145] It is important that a proposed CMM will be useful and valid for an organization. In the context of a Q-C2M2, usefulness will depend on the proposed model's compatibility with existing frameworks and policy, such as Qatar's National Information Assurance Policy (NIA Policy). Validity will depend on the proposed C2M2's basis for determining the domains and measures of capability, mainly whether it is based on existing and proven C2M2s and whether the creation of the C2M2 took into account Qatar's existing frameworks and policies.

In determining what will prompt organizations, especially state entities, to adopt a C2M2, Miron and Muita referred to the diffusion of innovation theory.[146] The theory identifies five factors that affect the decision to adopt a C2M2: (1) relative advantage, (2) compatibility, (3) simplicity, (4) trialability and (5) observability.[147] Relative advantage refers to the value that the proposed technology or innovation will contribute to the current existing processes or practices.[148] The proposed Q-C2M2, therefore, should add value to the Qatar NIAP and the NIAF. In this regard, the Q-C2M2 adds value by having identified domains or practice areas where the Qatar NIAP does not cover, and which the Q-C2M2 would enhance, including to improve cybersecurity protection

144. Adam Palmer, *A model framework for successful cybersecurity capacity building*, J of Internet L 15 (2016).
145. Lahrmaan et al. (n 23).
146. Miron and Muita (n 10); Everett M. Rogers, *Diffusion of Innovations* (Free Press, 1983).
147. See generally Rogers (n 162).
148. Ibid.

with protection technology and resilience management, and to improve cybersecurity response with mitigation and improvement management.

Compatibility refers to the ease with which Qatari state entities and non-state organizations can incorporate the proposed Q-C2M2 into their current processes, practices, and policies.[149] As this paper's comparative and document analysis included Qatari cybersecurity documents, the proposed Q-C2M2 takes into account existing Qatar cybersecurity processes, practices, and policies. Therefore, the proposed Q-C2M2 will likely have a high level of compatibility.

Simplicity refers to the user friendliness of the innovation, whether users find it difficult to use. Indeed, as noted by a number of researchers, complexity has been a hallmark of C2M2s.[150] The proposed Q-C2M2 aims to simplify by grouping practices and processes into themes the way the NIST Framework's core functions does, and by measuring the capability maturity of the core functions. By working at the thematic level, the Q-C2M2 will help simplify and streamline the Qatar NIAM. Trialability refers to the user's ability to try the innovation without commitment.[151] As the Q-C2M2 is not a commercial venture, Qatari state entities and non-state organizations could assess and try the Q-C2M2 without commitment. If the Q-C2M2 becomes incorporated into Qatar's NIAF as a legislative requirement or policy, the author suggests that a trial and training period be implemented.

Finally, observability refers to the visibility of the innovation in a community of the adopter's peers.[152] When applied to cybersecurity, the question could be translated into whether other state and non-state organizations have used a C2M2. While other organizations may not have used the Q-C2M2, as they would have tailored a C2M2 for their unique organization needs, the use of C2M2s in the cybersecurity field has been widespread.[153] Leading state agencies in the United States and the United Kingdom do use a C2M2. The use of C2M2s would be readily observable among peers in the cybersecurity community.

B. Q-C2M2 Domains and Subdomains

The proposed Q-C2M2 adopts the NIST Framework's approach of using five core functions as the main domains of the model.[154] The five core functions are applicable in the Qatari context because they are common across critical infrastructure sectors, an important element in the Qatari cybersecurity framework, and they remain important thematic elements in existing C2M2s. Additionally, the five core functions can be a means to simplify the organization and process of the Q-C2M2. Even if the five core functions are not common in non-critical infrastructures, they remain important thematic concepts even in non-critical infrastructure C2M2s like the CERT-RMM and the CCSMM, both of which do not focus on critical infrastructure but maintain the five core functions as key thematic elements.

The Q-C2M2, however, renames the core functions into the following domains: Understand Secure, Expose, Respond, and Sustain. Renaming the core functions into the domains achieves

149. Ibid.
150. Ibid.
151. Ibid.
152. Ibid.
153. Miron and Muita (n 10).
154. For an explanation of the NIST Framework's five core functions, see NIST (n 18) 8 and App A.

preciseness and clarity, and can now be easier to remember as USERS. These five domains are compatible with the control types classification of the NIAP, which are deter, avoid, prevent, detect, react, and recover.[155] In comparison to the NIST Framework's core functions, Understand is more precise than NIST's Identify because the organization must understand what and how to control cybersecurity risks to assets, data, personnel, systems, and processes. Secure is more appropriate than Protect in the Qatari context because of the NIAP's focus on security, security being a persistent and observable thematic element in the NIAP. Expose is more appropriate than Detect because it implies the need to uncover the perpetrators or the source of an event, and covers a cybersecurity program's exposure to risks. Detecting an event without a policy towards discovering the source is reactive rather than proactive and may result in repeated future events. Respond seems the most appropriate term concerning an organization's action after an event or incident is exposed. Sustain is more precise than NIST's Recover because it embraces the concept of resilience and continuity at a certain level. Table 9 below illustrates the domains and subdomains under the Q-C2M2.

Table 8: Q-C2M2 Domains and Subdomains

DOMAINS	SUBDOMAINS
Understand	Cybergovernance
	Assets
	Risks
	Training
Secure	Data Security
	Technology Security
	Access Control Security
	Communications Security
	Personnel Security
Expose	Monitoring
	Incident Management
	Detection
Respond	Analysis
	Exposure
Sustain	Recovery Planning
	Continuity Management
	Improvement
	External Dependencies

1. Understand Domain

The Understand domain includes four subdomains: Cybergovernance, Assets, Risks, and Training. These four subdomains are consistent with the existing C2M2, primarily the NIST Framework, the U.S. DoE's C2M2, and the CERT-RMM, all of which include governance, asset management, risk management, and training as categories. The NICE-CMM only includes governance. The Q-C2M2's Cybergovernance domain includes the Governance and Business Environment categories under the NIST Framework and the Compliance and Financial Resource Management of the CERT-RMM, and combines these activities with the Governance, Documentation, and Change Management domains under the NIAP. Essentially, the Cybergovernance domain enhances the NIAP's approach

155. Q-CERT, National Information Assurance Policy Ver 2.0 Control Types, http://www.qcert.org/sites/default/files/public/documents/cs-csps_controls_classification_v1.1.pdf (accessed Dcember 17, 2018).

by adding management of regulatory, legal, financial, and strategic organizational needs.[156] Under the Q-C2M2, NIAP's Data Labelling, as required under the NICP, and Data Retention and Archival would fall under the Assets subdomain, which includes the management of data, personnel, technology, systems, and facilities. The Q-C2M2 would improve on the NIAP's focus on information asset classification by managing other types of assets. The Risk domain includes risk assessment, risk management, and risk strategy, combined with the NIAP's approach of best practices among the C2M2s. One significant difference in the Q-C2M2 as compared to the NIST Framework is that Training now falls under the Understand domain as training enhances an organization's understanding of cybersecurity risks. The NIST Framework's inclusion of Awareness and Training is confusing when reconciled with the definition of Identify, which aims to develop organizational understanding and awareness of cybersecurity risks.

2. Secure Domain

The Secure domain follows the NIAP approach and adopts a similar approach to the Security Controls and Security Processes under NIAP. Subdomains under the Secure domain include Data Security, Technology Security, Access Control Security, Communications Security, and Personnel Security. The proposed Q-C2M2, however, adds Data Security as a subdomain, consistent with Qatar's Data and Privacy Protection Law. The proposed Q-C2M2 also adds Technology Security, which consolidates a number of technology-related security controls under NIAP including Cryptographic Security, Software Security, Network Security, Gateway Security, Product Security, Media Security, Portable Device and Off-Site Security, and Virtualization. Another subdomain under the Secure domain is Access Control Security, which encompasses System Usage Security, Identity and Logging Security, and Physical Access Security. Another subdomain is Communications Security, which has Information Exchange Security among its activities. The proposed Q-C2M2 adopts from the NIAP as a subdomain Personnel Security, which deals with the human element.

3. Expose Domain

The Expose domain includes the subdomains of Monitoring, Incident Management, Detection, Analysis, and Exposure. The Expose domain combines the Incident Management domain of NIAP with the Monitoring domain of the NIST Framework and the CERT-RMM, and the Detection Processes domain of the NIST Framework. The Expose domain also includes an Analysis subdomain, borrowed from the U.S. DoE's C2M2, and an Expose subdomain, which aims to track and uncover sources of incidents. Identifying perpetrators, however, has been identified as one of the key challenges to cybersecurity. As stated by Palmer, "[m]oving from monitoring and investigating advanced electronic evidence to the identification, disruption, and apprehension of the perpetrator(s) can represent a significant challenge."[157] The Expose subdomain, for example, requires an organization to seek assistance from private sector service providers, and may also require the investigation and monitoring of criminal networks.[158]

4. Respond Domain

The Respond domain borrows heavily from the NIST Framework and includes Response Planning, Mitigation, and Response Communication. The proposed Q-C2M2 improves Qatar's NIAP by

156. According to Palmer, "Cybersecurity is not just a technical solution. The foundation for all technical solutions should be based on a clear understanding of policy requirements and strategy goals." Palmer (n 160) 15.
157. Palmer (n 160) 16.
158. Ibid.

borrowing from the NIST Framework, especially in terms of Mitigation and Improvement. Qatar's NIAP currently groups response activities under the Incident Management domain and, in so doing, bypasses important activities such as mitigation and improvement of incident response. The Response Communication subdomain borrows from both the NIST Framework and the U.S. DoE's C2M2 in that it aims to ensure proper response communication with internal and external stakeholders.

5. Sustain Domain

The Sustain domain reorients the NIST Framework's core concept of Recover to emphasize that recovery must embrace maintaining and managing a certain level of sustainability long term. The Sustain domain includes Recovery Planning, Continuity Management, Improvement, and External Dependencies. The Continuity Management subdomain adopts the NIAP's Business Continuity Management domain. However, Recovery Planning, which addresses the immediate recovery from an incident, is separated under the Q-C2M2. The Improvement subdomain, borrowed from the NIST Framework, is another important addition to ensure that sustainability includes the process of learning from past incidents. Finally, the External Dependencies subdomain, borrowed from the U.S. DoE's C2M2 and the CERT-RMM, is combined with the NIAP's Third Party Security Management domain.[159]

D. Q-C2M2 Measures

One main difference versus the NIST Framework is that the Q-C2M2 will measure the capability maturity of a state entity or non-state organization at the core function level. The NIST Framework measures capability maturity in a rather general sense and does not rely on the tier measurement but rather on a review of the overall profile to determine maturity. In this regard, NIST has been criticized for not providing a specific measure of capability maturity. The Q-C2M2 adopts the concept behind the core functions of the NIST Framework but improves it by measuring capability maturity at the core function stage.

The Q-C2M2 will measure a state entity or a non-state organization's level of Understanding, Security, Exposure, Responsiveness, and Sustainability. These measures are easier to comprehend as measurements than the NIST Framework's core functions. The measures will identify an organization's maturity in terms of the following levels: Initiating, Implementing, Developing, Adaptive, and Agile. These levels are a combination and an improvement from existing C2M2s because of the document and comparative analysis conducted in this paper.

In the Initiating stage, an organization is only employing ad-hoc cybersecurity practices and process under some of the domains. In the Implementing stage, an organization has adopted policies to implement all of the cybersecurity activities under the domains with the aim of completing implementation at a certain time. In the Developing stage, an organization has implemented policies and practices to develop and improve cybersecurity activities under the domains with the aim of suggesting new activities to implement. In the Adaptive stage, adopted from the NIST Framework, an organization revisits and reviews cybersecurity activities and adopts practices based on a predictive indicators derived from previous experiences and measures. In the Agile stage, an organization continues to practice the Adaptive stage but with

159. Palmer also identifies internal/external cooperation as necessary for cybersecurity capacity building and development. Palmer (n 160) 17.

an added emphasis on agility and speed in implementing activities in the domains.

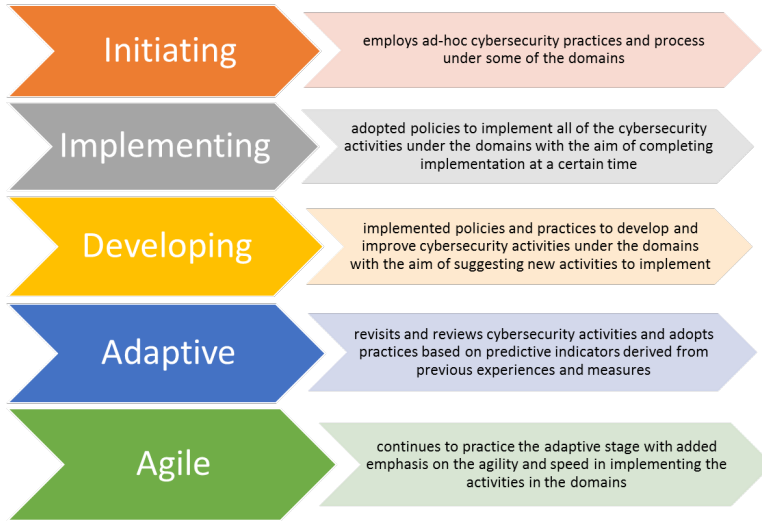

Figure 2: Q-C2M2 Maturity Levels

E. Q-C2M2 Dimensions

The proposed Q-C2M2 borrows from the CCSMM's focus on the third dimension posed by cybersecurity risks to communities at the national, state, community and organization levels. When adopted by Qatar, the dimensions will include national, municipal, community, and organization levels. Adopting these community dimensions is a recognition that cybersecurity is interdependent and that cybersecurity protection of government entities alone could lead to vulnerabilities. For example, false news hacked into community or organization levels could impact national cybersecurity. The Q-C2M2, therefore, also measures the capability maturity of cybersecurity programs at the municipal, community, and organization levels. Businesses, ranging from small and medium enterprises to large enterprises, would fall under the organization level.

VI. Legislative Framework

This section discusses the legislative and regulatory aspects of the Q-C2M2. First, the section discusses and argues for a legislatively mandated Q-C2M2 to make it a more effective improvement to Qatar's NIAF. Second, the section discusses the issue of adopting the Q-C2M2 and incorporating it within Qatar's existing cybersecurity framework's legislations, policies, and standards. Third, the section discusses the important role of the Critical Information Infrastructure Protection Law, which is expected to be signed into law soon. Finally, the section elaborates on the legal framework embedded within the Q-C2M2 design itself, with particular emphasis on legal and regulatory compliance, an obviously lacking domain under the existing NIAM.

A. Legislatively Mandated Q-C2M2

One of the prevailing criticisms of existing C2M2s is its voluntary nature. According to Miron and Muita, C2M2s cannot be "fostered effectively in an unlegislated environment."[160] The C2M2s analyzed in this paper, for example, are all voluntary. Even for providers of critical infrastructures in the United States, C2M2s are not mandatory.[161] To make the proposed Q-C2M2

160. Miron and Muita (n 10).
161. See U.S. DoE (n 17); U.S. DoE ONG-C2M2 (n 66); U.S. DoE ES-C2M2 (n 64). See also Miron and Muita (n 10).

more effective, the author advocates for a legislatively mandated Q-C2M2 with tiered levels of mandatory capability and voluntary capability.

For example, Qatar should mandate all public entities and private entities, in sectors considered part of critical infrastructure (food, finance, transportation, media, energy, and communications), to attain the highest level of maturity across all domains within specified deadlines. The Q-C2M2 proposes that the level of legislatively mandated capability maturity for critical infrastructures should be Agile maturity. Other private organizations in non-critical infrastructures should meet a lower level of mandated maturity, but may voluntarily achieve the highest level of maturity across all domains. The level of capability maturity for non-critical infrastructures entities under the Q-C2M2 should be, at minimum, a Developing maturity. UAE's NESA is an example of a similar approach with mandatory and voluntary aspects in the maturity capability assessment. [162] NESA's reporting procedures require a maturity-based self-assessment by stakeholders to be consistent with NESA's mandatory versus voluntary requirements.[163] Only a mandatory system would achieve the aims of the C2M2 and ensure a stronger cybersecurity environment. As the adage goes, a chain is only as strong as its weakest link.

One predictable criticism of a mandated approach is the cost that such a system would pose on businesses. A cost–benefit analysis supports a mandated system. However, as the cost of implementing a mandated cybersecurity capability maturity would be lower in a small country such as Qatar, the benefits of lower cyberattacks and cybercrimes outweigh the costs. In Qatar's case, the hacking of QNA, which led to the economic blockade, makes for an even stronger argument in favor of national security, as a weak cybersecurity environment lacking such a mandate would lead to higher risks and costs for businesses. Mandating the Q-C2M2 for national and public security interests would be consistent with Qatar's cybersecurity strategy.[164]

B. Adopting the Q-C2M2

Adopting a C2M2 would not necessarily be a novel approach in the region, but it would bring Qatar in line with leading practices. Oman, the only country in the Gulf Region to achieve a "leading" status in the ITU Global Cybersecurity Index of 2017,[165] adopted, through its Information Technology Authority, a Cybersecurity Capability Maturity Assessment back in 2015.[166] Countries adopting a capability maturity assessment approach in their cybersecurity framework have not faced difficulty in making the adoption, but the execution of such approaches has certainly

162. Downton (supra n 161).
163. Ibid.
164. QNCS (n 16). It states that "Qatar's vision is to establish and maintain a secure cyberspace to safeguard national interests…"
165. International Telecommunications Union, Global Cybersecurity Index 2017, 2017, → https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf (accessed February 23, 2018). Oman ranked fourth, while Qatar, classified as "maturing," ranked twenty-fifth globally.
166. Sultanate of Oman, Information Technology Authority, Annual report 2015, available in (English) pdf at https://www.ita.gov.om/ITAPortal/MediaCenter/Document_detail.aspx?NID=115 (accessed December 17, 2018). In 2015, the UAE's National Electronic Security Authority (NESA), charged with protecting the UAE's critical information infrastructure and cyber security, also adopted a maturity-based assessment like a C2M2 and was inspired by the NIST Framework. Ben Downton, *NESA - the new standard of information security in the UAE*, MWR Security, April 6, 2015, https://www.mwrinfosecurity.com/our-thinking/nesa-the-new-standard-of-information-security-in-the-uae/ (accessed February 23, 2018). The Saudi Arabian Monetary Agency (SAMA), also uses a cybersecurity framework with maturity levels like the C2M2, adopting an approach similar to the NIST Framework. Saudi Arabia Monetary Authority (SAMA), Cyber security framework v. 1 (May 2017), available in (English) pdf at http://www.sama.gov.sa/en-US/Laws/BankingRules/SAMA%20Cyber%20Security%20Framework.pdf (accessed February 23, 2018). Kuwait and Bahrain have not adopted a C2M2-like approach in their cybersecurity framework.

increased these countries' ability to improve cybersecurity, as seen in the case of Oman.[167]

Additionally, adoption and implementation of a C2M2 in Qatar could be achieved without further need for new legislation. Adopting the Q-C2M2 would certainly fall under the mandate of the Qatar Cybersecurity Strategy and the National Information Assurance Framework. The Q-C2M2 would be incorporated into the NIAF and would fall within the scope of existing policies, standards, and legislation. The NIAF's tiered approach to cybersecurity, as discussed in Section IV above, could accommodate the incorporation of the Q-C2M2. First, the Q-C2M2 could be an addition to existing policies or standards under the NIAF. Second, the Q-C2M2 could also be added as an amendment to existing legislation to ensure compliance with both the Q-C2M2 and the existing cybersecurity legislations such as the Data and Privacy Protection Law. Interestingly, the Data and Privacy Protection Law already includes an audit compliance mechanism.[168] A Q-C2M2 compliance could perhaps be added to such an audit compliance as well, and it could also be added through a committee process in one of the pending legislations, most appropriately the forthcoming CIIP Law. Alternatively, the Q-C2M2 could be incorporated into existing policies and standards such as the NIAM under the NIAP, or as a third extension in the NIAP, which would then include the NICP, NIAM, and Q-C2M2. Again, the NIAP already includes an audit compliance mechanism for state agencies, relating the NICP for auditing asset identification and classification.[169] The Q-C2M2 could also be incorporated into that mechanism. Unfortunately, the audit requirement under the NIAP only applied to state agencies.[170]

C. Critical Information Infrastructure Protection Law

For critical infrastructures, it remains to be seen whether the forthcoming CIIP Law will include a benchmarking and process improvement framework like the proposed Q-C2M2. The need for such a process for benchmarking and measuring the development of cybersecurity for critical infrastructures is even more striking for the financial, food, and media sectors. These three sectors were greatly affected by the cybersecurity vulnerabilities exposed by the blockade on Qatar. It remains to be seen whether the CIIP Law will define critical infrastructure sectors broadly or with a limited scope. According to Q-CERT, "sectors are deemed critical when their incapacitation or destruction would have a debilitating impact on the national security and social well-being of a nation."[171] Q-CERT also aims to identify critical infrastructure interdependencies by creating a critical information infrastructure protection interdependency database.[172] The economic blockade should be a lesson for a broader approach in defining critical infrastructure because of the interdependence of cybersecurity with the different infrastructure types.

It also remains to be seen whether the Qatari CIIP Law will adopt a regulatory framework similar to that of the European Union. So far, only the European Union has adopted a regulatory model for critical infrastructure protection under the European Programme for Critical Infrastructure

167. Ibid.
168. Qatar Data and Privacy Protection Law, Decree Law No (13) of 2016, available in pdf (English) at Sultan Al-Abdullah and Partners https://qatarlaw.com/wp-content/uploads/2017/05/Personal-Data-Privacy-Law-No.-13-of-2016.pdf (accessed February 22, 2018).
169. NIAP (n 143).
170. NIAP (n 143).
171. Q-CERT, National Information Assurance Framework, 2014, https://www.scribd.com/document/273021971/Qatar-National-Information-Assurance-Framework-Ismael (accessed October 18, 2017).
172. Q-CERT, Critical Information Infrastructure Protection Interdependency Database, http://www.qcert.org/services/critical-information-infrastructure-protection-interdependency-database (accessed October 18, 2017).

Protection (EPCIP).[173] The EPCIP legislative approach mandates EU nations to create an Operator Security Plan (OSP) for designated European critical infrastructures.[174] The OSP must cover the identification of important assets, a risk analysis based on major threat scenarios and the vulnerability of each asset, and the identification, selection, and prioritization of countermeasures and procedures.[175] The United States,[176] the United Kingdom,[177] and Canada[178] have adopted a cooperative framework[179] among government and critical infrastructure operators. A cooperative framework relies on the adoption by operators, rather than a legislatively mandated compliance program, through fostering communication of best practices.[180]

A critical infrastructure protection framework designed as a regulatory model similar to the EPCIP will certainly make it easier to incorporate a capability maturity model like the proposed Q-C2M2 with a legal framework. At the very least, Qatar should legislatively mandate the benchmarking of critical infrastructure protection and cybersecurity protection. A benchmarking program like the proposed Q-C2M2 will help identify both asset and threat-based risks. A Q-C2M2 can help the government better allocate time and resources for developing critical infrastructure and cybersecurity protection.

D. Legal Framework Embedded within the Q-C2M2's Design

Even without a legislative mandate for adoption, the Q-C2M2 incorporates a legal framework in the model's design under the Understand domain, which includes the Cybergovernance subdomain. Under Cybergovernance, an organization should have a set of activities related to legal and regulatory compliance, a domain glaringly missing under the existing NIAM. The Q-C2M2's Cybergovernance subdomain includes the Governance and Business Environment categories under the NIST Framework and the Compliance and Financial Resource Management of the CERT-RMM, and combines these domains with the Governance, Documentation, and Change Management domains under the NIAP. Essentially, the Cybergovernance domain enhances the NIAF's approach by adding compliance and management of regulatory, legal, financial, and strategic organizational needs.

In cybersecurity capacity building, Palmer suggests capacity-building training to support development of internal legislative, procedural, and technical operational capabilities.[181] In

173. Miron and Muita (n 10). See Council Directive (EC) 2008/114 on European Critical Infrastructures, 2008, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF (accessed October 17, 2017); Commission of the European Communities, Communication from the Commission on a European Programme for Critical Infrastructure Protection COM, 2006, 786 final, December 12, 2006, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF (accessed October 17, 2017); European Commission, Critical Infrastructure, Migration and Home Affairs, July 20, 2014, https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure_en (accessed October 17, 2017).
174. Council Directive (EC) 2008/114 (n 209).
175. Ibid.; Madelene Lindström & Stefan Olsson, *The European programme for critical infrastructure protection*, in Stefan Olsson (ed), *Crisis Management in the European Union* (Springer, 2009).
176. U.S. Department of Homeland Security, NIPP 2013: Partnering for critical infrastructure security and resilience, 2013, https://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf (accessed October 17, 2017).
177. See Centre for Protection of National Infrastructure, Critical National Infrastructure, 2017, https://www.cpni.gov.uk/critical-national-infrastructure-0 (accessed October 17, 2017).
178. National Strategy for Critical Infrastructure, Canada, 2009, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crt-cl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf (accessed October 17, 2017).
179. Miron and Muita (n 10).
180. Ibid.
181. Palmer (n 160) 16.

other words, cybergovernance and development of cybersecurity capability maturity must include a legislative framework. Cybergovernance should include managers complying with procedural frameworks in the Q-C2M2.[182] Likewise, higher-level managers should incorporate a process for legal compliance similar to the CERT-RMM, including identifying and documenting legal and regulatory compliance processes and practices. Legal and regulatory compliance should be included as a process under all the domains. The organization should task a legal team to oversee compliance under each domain through periodic policy, practice, and process reviews. Such a legal audit would be compatible with the Qatari cybersecurity framework's audit and certification process incorporated in the NIAP.

The proposed Q-C2M2 takes into account compliance with existing Qatari cybersecurity laws, with specific focus on the Data and Privacy Protection Law.[183] The Data and Privacy Protection Law, among others, requires controllers of data to review data privacy procedures; to identify the person responsible for personal data privacy protection; to conduct awareness training; to develop a sound internal system for dealing with data breach complaints and personal data management; and to conduct audits to determine compliance levels.[184] The law provides exemptions, among others, for the protection of national and public security and in the investigation of crimes, which means that public entities already working to prevent cyberattacks or cybercrimes will likely fall under the exemption.[185] The Q-C2M2, under the Cybergovernance subdomain, would include compliance activities on how exempted individuals and organizations may fall within the exemption. Furthermore, for individuals and organizations that are not covered by any exemption, the Q-C2M2's cybergovernance subdomain would provide guidance on how to follow data privacy procedures and ensure cybersecurity readiness. In other words, the involved operations in the Q-C2M2 should adopt activities that include the management of legal and regulatory compliance with attention to protecting civil liberties when conducting cybersecurity operations and activities.

The Q-C2M2 should also adopt activities that ensure compliance with international law principles, such as the applicability of the UN Charter to cyberspace, as recognized by the UN's Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE).[186] In its consensus report in June 2015, the GGE stated that when using information communication technologies (ICTs), states must observe international law principles including the peaceful resolution of disputes, state sovereignty, and non-intervention.[187] The GGE also found that international law obligations, such as the obligation to respect and protect human rights and free speech, are applicable whenever states use ICTs.[188]

182. Ibid. (stating that "[i]nitiatives to combat advanced cyber threat activity must be placed within a solid procedural framework.").
183. Qatar Data and Privacy Protection Law, Decree Law No (13) of 2016, available in pdf (English) at Sultan Al-Abdullah and Partners https://qatarlaw.com/wp-content/uploads/2017/05/Personal-Data-Privacy-Law-No.-13-of-2016.pdf (accessed February 22, 2018).
184. Ibid.
185. Ibid.
186. United Nations Officer of Disarmament Affairs (UNODA), Developments in the field of information and telecommunications in the context of international security, https://www.un.org/disarmament/topics/informationsecurity/ (accessed February 22, 2018); United Nations Secretary General, Report of the group of governmental experts on developments in the field of information and telecommunications in the context of international security, 2015, available in (English) pdf http://undocs.org/A/70/174 (accessed February 22, 2018). The GGE was established pursuant to paragraph 4 of General Assembly Resolution 68/243.
187. Ibid.
188. Ibid.

Interestingly, the UAE and Saudi Arabia's ban of social media speech in countries that show support for Qatar following the economic blockade violates the international law obligations to free speech. Additionally, the GGE stated that states must not engage in the use of proxies "to commit internationally wrongful acts using ICTs, and should seek to ensure that their territory is not used by non-State actors to commit such acts."[189] Under the Understand domain and Cybergovernance subdomain of the proposed Q-C2M2, in the instance of a cyberattack a legal team must advise Qatar on international law compliance and the legally appropriate response.

Conclusion

After a document and comparative analysis of pertinent C2M2 models and the Qatar cybersecurity strategy and the NIAP, the author recommends that, at minimum, Qatar should update the NIAP to include compliance, financial resources management, protective technology, awareness and training, mitigation, analysis, improvement, and communication. Qatar should also mandate a minimum level of cybersecurity capability with a means for measuring the cybersecurity maturity level for public and private entities, with utmost priority given to critical infrastructures including organizations in the food, transportation, finance, communication, media, and energy sectors. The author recommends the adoption of the proposed Q-C2M2 as a means of measuring and enforcing compliance. Qatar could adopt the Q-C2M2 without further need for new legislation, as it falls within the scope of existing policies, standards, and legislation or it can be introduced as an amendment to existing legislation.

The proposed Q-C2M2 does not aim to be a full proposal with ironed ironed-out detailed activities. Rather, the proposed Q-C2M2 provides a workable framework that Qatari cybersecurity stakeholders can use in working together to identify fully researched and negotiated activities that fall under the Q-C2M2's domains and subdomains. Most importantly, the Q-C2M2 stems from a methodologically derived comparison of existing C2M2s and the Qatari cybersecurity framework with an emphasis on the NIAM domains. This paper proposes a legislative framework that will enhance the development, sustainability, and agility of the Qatari cybersecurity framework. The blockade of Qatar has been a lesson of self-sufficiency, resilience, and the importance of building measures for security, of which cybersecurity plays a pivotal role.

Bibliography

Adler, Richard, *A dynamic capability maturity model for improving cyber security*, 2013 IEEE International Conference on Technologies for Homeland Security (HST) (2014).

Arnold, Tom, Hadeel Al Sayegh, and Tom Finn, *UPDATE 3-Qatari riyal under pressure as Saudi, UAE banks delay Qatar deals*, CNBC, June 6, 2017, https://www.cnbc.com/2017/06/06/reuters-america-update-3-qatari-riyal-under-pressure-as-saudi-uae-banks-delay-qatar-deals.html.

Atoum, Issa, Ahmed Ali Otoom, and Amer Abu Ali, *A holistic cyber security implementation framework*, 22 Information Management & Computer Security 3, 251–264(14) (2014).

Barclay, Corlane, Sustainable security advantage in a changing environment: The Cybersecurity Capability Maturity Model (CM2), Proceedings of the 2014 ITU Kaleidoscope Academic Conference: Living in a converged world – Impossible without standards? (July 21, 2014).

189. Ibid.

BBC, *Qatar crisis: What you need to know*, BBC News, July 19, 2017, http://www.bbc.com/news/world-middle-east-40173757.

Becker, Jörg, Ralf Knackstedt, and Jens Pöppelbuß, *Developing maturity models for IT Management: A procedure model and its application*, 1(3) Bus & Inf Systems Engineering 213–222 (2009).

Bowen, Glenn A., *Document analysis as a qualitative research method*, 9(2) Qual Research J 27–40 (2009).

Boyle, Kip, International use of NIST Cybersecurity Framework, 2016, http://kipboyle.com/2016/05/international-use-of-nist-cybersecurity-framework/.

Buss, Terry F., *The adoption and transformation of capability maturity models in government*, in *Encyclopedia of Information Science and Technology* (4th ed. 2018).

Butkovic, Matthew J., and Richard A. Caralli, Advancing cybersecurity capability measurement using the CERT®-RMM maturity indicator level scale, Software Engineering Institute, Carnegie Mellon University Research Showcase, 2013, http://repository.cmu.edu/cgi/viewcontent.cgi?article=1766&context=sei.

Calamur, Krishnadev, *What just happened with Qatar?* The Atlantic, June 5, 2017, https://www.theatlantic.com/news/archive/2017/06/what-just-happened-with-qatar/529128/.

Caralli, Richard A., et al., CERT® Resilience Management Model, Version 1.2, Software Engineering Institute, February 2016, https://www.cert.org/resilience/products-services/cert-rmm/.

Centre for Protection of National Infrastructure, Critical National Infrastructure, 2017, https://www.cpni.gov.uk/critical-national-infrastructure-0.

CERT, Cyber risk and resilience management: Overview, 2017, https://www.cert.org/resilience/.
Chapin, D.A., and S. Akridge, *How can security be measured?* 2 Information Systems Control J 43–47 (2005).

CMMI Institute, Published appraisal results, https://sas.cmmiinstitute.com/pars/pars.aspx.

Commission of the European Communities, Communication from the Commission on a European Programme for Critical Infrastructure Protection COM, 2006, 786 final, December 12, 2006, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF.

Council Directive (EC) 2008/114 on European Critical Infrastructures, 2008, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF.

Datz, Todd, *SCADA system security: Out of control*, CSO Online, August 1, 2004, www.csoonline.com/article/219486/scada-system-security-out-of-control.

Debreceny, R.S., Re-engineering IT internal controls: Applying capability maturity models to the evaluation of IT controls, *IEEE*, HICSS'06, Proceedings of the 39th Annual Hawaii International Conference on System Sciences 8: 196c–196c (2006).

DeYoung, Karen and Ellen Nakashima, *UAE orchestrated hacking of Qatari government sites, sparking regional upheaval, according to U.S. intelligence officials*, The Washington Post, July 16, 2017, https://www.washingtonpost.com/world/national-security/uae-hacked-qatari-government-sites-sparking-regional-upheaval-according-to-us-intelligence-officials/2017/07/16/00c46e54-698f-11e7-8eb5-cbccc2e7bfbf_story.html?utm_term=.af380f2295ce.

Doumar, George et al., *Crisis in the Gulf Cooperation Council: Challenges and Prospects* (Arab Center Washington DC 2017).

Downton, Ben, *NESA - the new standard of information security in the UAE*, MWR Security, April 6, 2015, https://www.mwrinfosecurity.com/our-thinking/nesa-the-new-standard-of-information-security-in-the-uae/.

Dunn, Myriam, *Information risks and countermeasures: Problems, prospects, and challenges of securing the information infrastructure*, in Theodor Winkler, Anja H Ebnöther, Ernst M Felberbauer (eds), *6th International Security Forum: Proceedings of the Conference* (Peter Lang, 2005).

European Commission, Critical Infrastructure, Migration and Home Affairs, July 20, 2014, https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure_en.

Ferraiolo, Karen, The Systems Security Engineering Capability Maturity Model (SSE-CMM), International Systems Security Engineering Association (ISSEA), 2000, https://csrc.nist.gov/csrc/media/publications/conference-paper/2000/10/19/proceedings-of-the-23rd-nissc-2000/documents/papers/916slide.pdf.

Fetais, Noora, director of KINDI Computer Research Center, Qatar University, email correspondence (October 19, 2017) (copy on file with the author).

Financial Times, *The blockade against Qatar damages all sides*, July 23, 2017, https://www.ft.com/content/213cfae6-6e28-11e7-bfeb-33fe0c5b7eaa?mhq5j=e7.

Framework Nazionale per la Cyber Security, Il cybersecurity report 2016, 2016, http://www.cybersecurityframework.it/.

González-Rojas, Oscar, Dario Correal, and Manuel Camargo, *ICT capabilities for supporting collaborative work on business processes within the digital content industry*, 80 Computers in Industry 16–29 (2016).

Gupta, Rahul, The challenges and recommended steps to improve cybersecurity within industrial control systems, Wood Group Mustang, Petroleum and Power Automation (PPA) Meet, New Delhi, India, 2016, https://www.woodgroup.com/__data/assets/pdf_file/0011/3143/2016-04-ISA-Delhi-power-and-petroleum.pdf.

Harb, Imad K., *Stupendous hubris…and its damage*, in George Doumar et al., *Crisis in the Gulf Cooperation Council: Challenges and Prospects* (Arab Center Washington DC, 2017).

Ibrahim, Jamaludin et al., A cybersecurity capability maturity model based on Maqasid Shari'ah (MS-C2M2), International Conference on Maqasid Al-Shari'ah in Public Policy and Governance (IAIS Malaysia, 2015).

International Telecommunications Union, Cyberwellness profile: Qatar, 2014, http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Qatar.pdf.

International Telecommunications Union, Cyberwellness profile: Qatar, in Global Cybersecurity Index & Cyberwellness Profiles: Report, 382, *ABI Research*, 2015, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf.

International Telecommunications Union, Global Cybersecurity Index 2017, 2017, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf. Kiblawi, Tamar et al., Qatar rift: Saudi, UAE, Bahrain, Egypt cut diplomatic ties, *CNN*, July 27, 2017, http://edition.cnn.com/2017/06/05/middleeast/saudi-bahrain-egypt-uae-qatar-terror/index.html.

Krutz, Ronald L., Methodology for assessing the maturity and capability of an organization's computer forensics processes, U.S. Patent Application 10/952537 (2006).

Lahrmann, Gerrit et al., *Inductive design of maturity models: Applying the Rasch algorithm for design science research*, Service-Oriented Perspectives: Design Science Research, 176–191 (Springer, 2011).

Li, Xiao-Juan, and Huang Li-Zhen, Vulnerability and interdependency of critical infrastructure: A review, Third International Conference on Infrastructure Systems and Services: Next Generation Infrastructure Systems for Eco-Cities (INFRA) (2010).

Lindström, Madelene, and Stefan Olsson, *The European programme for critical infrastructure protection*, in Stefan Olsson (ed.), Crisis Management in the European Union (Springer, 2009).

Ministry of Information and Communications Technology, Information Security Framework for School Networks, 2014, http://www.qcert.org/library/36.

Ministry of Information and Communications Technology, National Information Assurance Manual, 2014, http://www.qcert.org/library/36.

Ministry of Information and Communications Technology, National Information Assurance Policy, 2014, http://www.qcert.org/library/36.

Ministry of Information and Communications Technology, National Information Classification Policy, 2014, http://www.qcert.org/library/36.

Ministry of Transport and Communications, Guidance for Assurance Manual v. 2.0, 2014, http://www.motc.gov.qa/sites/default/files/guidance_nia_manual-v2.0_english_1.pdf.

Ministry of Information and Communications Technology and Q-CERT, National Information Assurance Manual, 2014, http://www.qcert.org/sites/default/files/public/documents/nia_policy__manual_english_v2.0_0.pdf.

Miron, Walter, and Kevin Muita, *Cybersecurity capability maturity models for providers of critical infrastructure*, 4(10) Tech Innovation Management Rev 33–39 (2014).

National Initiative for Cybersecurity Education (NICE), Cybersecurity capability maturity model, October 3, 2012, https://www.tdisecurity.com/about-tdi/cybersecurity_education.pdf.

National Institute of Standards and Technology (NIST), Framework for improving critical infrastructure cybersecurity, February 12, 2014, https://www.nist.gov/cyberframework.

National Strategy for Critical Infrastructure, Canada, 2009, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf.

O'Leary, Zina, *The Essential Guide to Doing Your Research Project* (2nd ed., SAGE Publications, 2014).

Osborne, Charlie, *Script kiddies delight at 'easy' hack which caused Qatar diplomatic crisis*, Zero Day Net, June 8, 2017, http://www.zdnet.com/article/it-was-easy-to-cause-the-qatar-diplomatic-crisis/.

Palmer, Adam, *A model framework for successful cybersecurity capacity building*, J of Internet L 15 (2016).

Paulk, Mark C. et al., *Capability maturity model version 1.1*, 10(4) IEEE Software 18–27 (1993).

Qatar Critical Information Infrastructure Protection Law (CIIP) (not yet published).

Qatar Cybercrime Law, Decree Law No (14) of 2014, available in pdf (Arabic) at International Labour Organization (ILO) http://www.ilo.org/dyn/natlex/natlex4.detail?p_lang=en&p_isn=100242.

Qatar Data and Privacy Protection Law, Decree Law No (13) of 2016, available in pdf (English) at Sultan Al-Abdullah and Partners https://qatarlaw.com/wp-content/uploads/2017/05/Personal-Data-Privacy-Law-No.-13-of-2016.pdf.

Qatar Decree Law No (16) of 2010 on the Promulgation of the Electronic Commerce and Transactions Law, available in English at Al Meezan, http://www.almeezan.qa/LawPage.aspx?id=2678&language=en.

Qatar National Cybersecurity Strategy, May 2014, http://www.motc.gov.qa/en/documents/document/national-cyber-security-strategy.

Q-CERT, About Q-CERT, 2017, http://www.qcert.org/about-q-cert.

Q-CERT, Critical Information Infrastructure Protection Interdependency Database, http://www.qcert.org/services/critical-information-infrastructure-protection-interdependency-database.

Q-CERT, National Information Assurance Policy Ver 2.0 Control Types, http://www.qcert.org/sites/default/files/public/documents/cs-niap_controls_classification_eng_v1.0.pdf.

Q-CERT, Qatar National Information Assurance Framework 2014, available in English, https://www.scribd.com/document/273021971/Qatar-National-Information-Assurance-Framework-Ismael.

Rea-Guamán, Angel Marcelo et al., *Comparative study of cybersecurity capability maturity models*, in Antonia Mas et al. (eds), *Software Process Improvement and Capability Determination*, SPICE Conference 2017, Communications in Computer and Information Science, vol. 770 (Springer, 2017).

Rea-Guamán, Angel Marcelo et al., Maturity models in cybersecurity: A systematic review, 2017 12th Iberian Conference on Information Systems and Technologies (CISTI) (2017).

Rogers, Everett M., *Diffusion of Innovations* (Free Press, 1983).

Saudi Arabia Monetary Authority (SAMA), Cyber security framework v. 1 (May 2017), available in (English) pdf at http://www.sama.gov.sa/en-US/Laws/BankingRules/SAMA%20Cyber%20Security%20Framework.pdf.

Siponen, Mikko, *Towards maturity of information security maturity criteria: Six lessons learned from software maturity criteria*, 10(5) Inf Management & Comp Security 210–224 (2002).

Stewart, David, *Qatar's resilience - a lesson for all on how to respond positively to a crisis*, Gulf Times, October 10, 2017, http://www.gulf-times.com/story/566847/Qatar-s-resilience-a-lesson-for-all-on-how-to-resp.

Sultanate of Oman, Information Technology Authority, Annual report 2015, available in (English) pdf at https://www.ita.gov.om/ITAPortal/MediaCenter/Document_detail.aspx?NID=115.

United Nations Officer of Disarmament Affairs (UNODA), Developments in the field of information and telecommunications in the context of international security, https://www.un.org/disarmament/topics/informationsecurity/.

United Nations Secretary General, Report of the group of governmental experts on developments in the field of information and telecommunications in the context of international security, 2015, available in (English) pdf http://undocs.org/A/70/174.

U.S. Department of Energy, Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) v.1.1., February 2014, https://energy.gov/oe/cybersecurity-capability-maturity-model-c2m2-program/electricity-subsector-cybersecurity ("U.S. DoE ES-C2M2").

U.S. Department of Energy, Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model (ONG-C2M2) v.1.1., February 2014, https://energy.gov/oe/cybersecurity-capability-maturity-model-c2m2-program/oil-and-natural-gas-subsector-cybersecurity ("U.S. DoE ONG-C2M2").

U.S. Department of Energy and U.S. Department of Homeland Security, Cybersecurity Capability Maturity Model (C2M2) v.1.1., February 2014, https://energy.gov/oe/services/cybersecurity/cybersecurity-capability-maturity-model-c2m2-program/cybersecurity.

U.S. Department of Homeland Security, NIPP 2013: Partnering for critical infrastructure security

and resilience, 2013, https://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf.
Uzoka, Faith-Michael E., *A CMM assessment of information systems maturity levels in Botswana*, 16 MIS Rev 53–84 (2010).

Vijayan, Jaikumar, *Web site offline as police, FBI investigate $10M extortion bid*, Computer World, May 7, 2009, www.computerworld.com/s/article/9132678/Web_site_offline_as_police_FBI_investigate_10M_extortion_bid.

Wendler, Roy, *The maturity of maturity model research: A systematic mapping study*, 54(12) Information and Software Tech 1317–1339 (2012).

Westcott, Ben, Richard Roth, and Ralph Ellis, *Qatar says embargoing nations behind news agency hack*, CNN, July 27, 2017, http://edition.cnn.com/2017/07/20/middleeast/qatar-ambassador-un-demands/index.html.

Yusta, Jose M., Gabriel J.Correa, and Roberto Lacal-Arántegui, *Methodologies and applications for critical infrastructure protection: State-of-the-art*, 39(10) Energy Policy 6100–611 (2011).