2019-01-01

Current cybersecurity maturity models: How effective in healthcare cloud?

Akinsanya, OO

CEUR Workshop Proceedings

Current Cybersecurity Maturity Models: How Effective in Healthcare Cloud?

Opeoluwa Ore Akinsanya, Maria Papadaki, Lingfen Sun

School of Computing, Electronics, and Mathematics, University of Plymouth, Plymouth, United Kingdom
info@cscan.org

Abstract. This research investigates the effective assessment of healthcare cyber security maturity models for healthcare organizations actively using cloud computing. Healthcare cyber security maturity models designate a collection of capabilities expected in a healthcare organization and facilitate its ability to identify where their practices are weak or absent and where they are truly embedded. However, these assessment practices are sometimes considered not effective because sole compliance to standards does not produce objective assessment outputs, and the performance measurements of individual IS components does not depict the overall security posture of a healthcare organization. They also do not consider the effect of the characteristics of cloud computing in healthcare. This paper presents a literature review of maturity models for cloud security assessment in healthcare and argues the need for a cloud security maturity model for healthcare organizations. This review is seeking to articulate the present lack of research in this area and present relevant healthcare cloud-specific security concerns.

Keywords: Healthcare, Cyber security, Maturity Model, Cloud Computing

1. Introduction

A maturity model is used as a tool to assess an organization's effectiveness at achieving a particular goal. It can also facilitate an organization's ability to identify where their practices are weak or absent and where their practices are truly embedded. Cyber security maturity model is a tool that can track improvements made over time from embedding security within an organization's daily and strategic workflows, and between similar organizations in an industry.

Security and privacy of patient information are of utmost priority to all healthcare stakeholders. These reasons mostly limit the adoption of cloud computing and the requirement to link isolated electronic healthcare systems [1]. In order to ensure a secure environment for the interconnected systems, it is important to assess the overall security posture of the healthcare organization. The processes and activities are stated at different levels of maturity and compared with the healthcare organization's practices to assess its overall cyber security maturity. The outputs provide better

awareness, visibility and accountability [2], and can reveal the overall security posture of an organization. Healthcare cyber security maturity models provide a collection of capabilities expected in a healthcare organization with an effective approach to cyber security. Therefore, security decisions are supported by capabilities' assessment outputs obtained at different stages, compared against description of processes and activities mapped to cyber security best practices, guidance, and standards [3].

Most recent cyber security maturity models are built on assessing compliance to cyber security standards and guidance or on assessing specific information systems (IS) components like networks, vulnerability risks and intrusion detection [4, 5]. However, these assessment practices are considered not effective because sole compliance to standards does not produce objective assessment outputs, and the performance measurements of individual IS components does not depict the overall security posture of a healthcare organization. These discrepancies affect their adoption as models to derive reliable assessable outputs. In order for interconnected healthcare systems to communicate effectively without worsening the overall security of the system, each healthcare organization's security posture should be well known using reliable and important cyber security indicators that bring visibility and build trust among participating organizations [6].

This paper presents a literature review of cyber security maturity models utilized for cloud security assessment in healthcare and proposes the need for a cloud security maturity model for healthcare. The review includes cyber security maturity models tailored to healthcare assessment in cloud computing, and it is not confined to only academic literature but also includes industry literature. This review is seeking to articulate the present lack of research in this area and present relevant healthcare cloud-specific security concerns. The rest of the paper is organized into the following manner. Section 2 presents methodology, section 3 highlights cloud-specific security standards, best practices and guidance applicable to healthcare, whereas section 4 highlights current cyber security maturity models employed in healthcare cyber security assessment in cloud computing. Section 5 provides the conclusion and further work.

2. Methodology

The research methodology ensued logical and combined reviews based on concept-centric frameworks [7]. The research parameters, and search terms were formulated according to a predefined set of rules, which informed the combination of search terms. Since this research is in the information systems (IS) field, logical literature review guide was also employed since it allows detailed explanation of the process, being comprehensive in scope, and providing an opportunity for repeatability [8, 9].

The methodology consists of four stages: identification, screening, eligibility and the analysis of included publications. Important is that the process should have a clear and repeatable protocol that is followed. Specifically, 93 information sources were identified in the first stage by systematic literature search using a structured approach.

Secondly, the screening of the titles, abstracts and meta-data such as the quality of the source or the type of source, the relevance of the title and abstract led to the exclusion of 56 publications. In the third stage, the literature were fully read. Based on their content, 16 publications were further excluded as out of scope. In the final stage, the remaining 21 publications were critically reviewed as part of this paper. The literature review methodology was based on Liberati [8].

Despite adopting a rigorous approach to reviewing the publications, there still exist the risk of having overlooked important contributions by excluding cyber security maturity frameworks from the search because these could not produce measurable outputs to determine cyber security posture. Since the research topic is still emergent in nature, it makes sense that results are currently being on-going research. However, assessing the quality of the frameworks and models-in-progress is an arduous and error-prone task. By limiting the review there was focus on mature research adhering to the high-quality standards and workflow dynamics of healthcare, which in turn, ensures quality in the reported findings.

3. Cloud security standards, best practices and guidance in healthcare

Standards, guidance, and best practices have been in use for a very long time, and their similarity is that they are reactive in nature. There will always be a gap between deciding whether something is needed and achieving implementation, which may span years. This becomes more of an issue for international standards due to the differing agendas being pursued by different countries, which can further increase the gap to implementation. The problem is yet further worsened in a technological environment, such as security in computing, and especially in a fast-moving technology like cloud computing. However, not only is technology rapidly changing, but the threat environment is also developing at a considerable pace [10].

International Organization for Standardization

ISO 2700-series standards produced by the International Organization for Standardization (ISO) and International Electro technical Commission (IEC) provide best practices recommendation that covers the fundamental requirements of information security management systems, guidelines and principles for the implementation of such systems. The ISO 27001 [11] is valid to all organizations regardless of their size and industries. It specifies the method that organizations should use for information security and the essential components. It also ensures the identification and management of risks are properly verified. Compliance saves organizations the financial penalties and losses associated with data breaches, comply with business, legal, contractual and regulatory requirements, protect and enhance their credibility and reputations.

ISO 17522 [12] and ISO 27799 [13] standards are targeted for health informatics. They provide guidelines for designing health specific information management systems based on ISO 27002, and control patient safety within such systems respectively.

ISO 27001 can be integrated with ISO 27799 standard to address healthcare specific risks. ISO 27017 [14] provide detailed guidance and recommendations for cloud adoption. The ISO 22857 addresses the protection requirements to facilitate cross-border transfer of personal healthcare data [15].

However, these standards do not completely address some of the healthcare-specific concerns, healthcare organizations have not been able to adapt the standards, guidelines and best practices from the frameworks to their specific context and develop practices that meet their own needs. Other concerns include extensive time and expense of complying with different standards, and the need for clarity and simplicity with implementation.

Health Information Trust Alliance

Healthcare industry leaders provide a harmonized, certifiable framework for all organizations that create, access, store, or exchange sensitive and/or regulated health data using HITRUST (Health Information Trust Alliance). The HITRUST Common Security Framework (CSF) version 9 [16], is a comprehensive, risk-oriented framework that normalizes the cyber security requirements of healthcare organizations. It is based on federal legislation such as HIPAA (Health Insurance Portability and Accountability Act) 164.502(ii), and globally recognized standards and guidance including ISO 27799 using ISO 27002, NIST SP 800-53 r4 AC-19 [17]. It provides scalable security requirements tailored to the needs of the healthcare organization, allowing healthcare organizations monitor and maintain compliance with HITRUST data security controls across their cloud infrastructure including multi-cloud deployments.

The HITRUST framework's mapping with the NIST CSF reveals, the HITRUST framework provides healthcare industry-specific model implementation while the NIST framework provides broad guidance to critical infrastructure industries on organizational-level risk programs that are holistic, based on principles and used across industries. A major constraint for HITRUST framework is that it is yet to receive worldwide acceptance.

National Institute of Standards and Technology

In addressing cyber security, many entities both within and outside of the healthcare sector have voluntarily relied on detailed cyber security guidance and specific standards issued by NIST. The National Institute of Standards and Technology (NIST) developed a set of guidelines on security and privacy in public computing, SP 800-144 [18]. It provides an overview of the security and privacy challenges for public cloud computing and presents recommendations that organizations should consider when outsourcing data, applications and infrastructure to a public cloud environment. NIST also developed a special publication, SP 800145 [19] for definition of cloud computing which has been globally accepted. SP 500-299 framework [20] was developed to identify core set of security components that can be implemented in cloud to secure the environment, the operations, and the data migrated to the cloud. It also released SP 500-291 Cloud Computing Standards Roadmap [21], SP 800-146 Cloud

Computing Synopsis and Recommendations [22], and SP 500-292 Cloud Computing Reference Architecture [23]. SP 800-66 [24] was developed regarding the guidance for IT security planning, implementation, management, and operation. It includes publications that address many security areas that are impacted by the HIPAA Cyber security Rule. NIST 800-66 provides guidance as to how to map HIPAA controls with NIST 800-53. This is the only guideline that is specifically focused on healthcare although it did not make mention of cloud computing.

In addition, to address the ever-increasing attacks on critical infrastructure, NIST also developed the Cyber Security Framework (CSF) that provides an incident management model that various industries can leverage for improving the management of cyber security risk, and built on ISO 27001, COBIT [25], and NIST 800-53. The framework is clearly structured in terms of the areas of cyber security that need to be implemented. This supports the relevant stakeholders to assess cyber security and identify gaps. Howbeit, the shortfall of the framework's security controls was that they were specifically designed for US Federal agencies, and not accepted worldwide. Initially, it was not sufficiently specific about cloud environments, but now, major cloud service providers, Amazon Web Services [26], Microsoft Azure [27] have taken steps to align their offerings to the framework addressing the ambiguities about the use of the CSF in the cloud.

Health Insurance Portability and Accountability Act

The HIPAA was developed in order to ensure security and privacy of individually identifiable health information. HIPAA deals with security and privacy through its privacy rule [28] and security rule [29]. The privacy rule ensures the flow of health information needed for quality care by addressing proper use and disclosure of health information. The security rule aims at protecting the privacy of individuals' health information by adopting new technologies with a goal of achieving improved quality and efficiency of patient care. It operationalizes the protection mechanisms contained in the privacy rule. HIPAA privacy and security rules are applied to healthcare providers and non-healthcare providers supporting the healthcare providers holding or transmitting health information in electronic form. HIPAA compliance cannot be overlooked when it comes to cloud computing, however, it is no longer enough for a vendor to simply claim "HIPAA readiness." Its controls are indicated as required which makes implementation unclear. HIPAA is not "certifiable" resulting to the need for healthcare organizations to influence internal or external assessors to perform self-assessment for compliance.

The scope of security and privacy protections available in HIPAA are extended through the Health Information Technology for Economic and Clinical Health Act (HITECH). In the healthcare industry, so far HITECH [30] provides legal liability for non-compliance to HIPAA, and ensures the disclosure of breach and unauthorized use of electronic health records to necessary stakeholders.

Cloud Security Alliance Standards

Cloud Security Alliance (CSA) developed security guidance for critical areas of focus in cloud computing including various versions. Version 1.0 [31], Version 2.1 [32], Version 3.0 [33], and Version 4.0 [34]. The latest version focused on meeting the demand of security changes. It also introduced better standards for organizations to manage cyber security for cloud by implementing security domains. The guidance can be applied to cloud service model (IPSaaS) and four deployment models (Public, Private, Community, and Hybrid Cloud) with derivative variations that address specific requirements. The guidance included thirteen (13) different domains, which are divided into two general categories: governance and operations. The governance domains focus on broad and strategic issues as well as policies within a cloud computing environment, while the operations domains focus on more tactical security concerns and implementation within the cloud architecture.

This guidance is relevant to cloud computing, its service models and its deployment models. As regards cloud security management, the guidance focuses on cloud-specific concerns: interoperability and portability, data security, and virtualization. Dividing the implementation domains into two groups with strategic and tactical categories is another salient point of the guidance. This approach allows cloud consumers, providers to bring financial, and human resources into security consideration. Furthermore, the guidance can be mapped to existing security models including the Cloud Control Matrix [35]. Despite these benefits, the guidance lacks assessment guide for each domain. In addition, it does not consider security metrics for security practices. Therefore, organizations find it difficult to determine the security level of a domain.

There are several standards, guidelines and directives that are strongly complied with in all industries but, as commonly observed, they are not specifically focused on the healthcare industry nor do they meet the entire requirement for healthcare cloud. To address the healthcare cloud-specific needs, various selection of standards is expected to be based on parameters, such as scope, level of integration, industry applicability, prescriptiveness, scaling, tailoring, compliance, certification, shared assurance, assessment guidance, and tool support.

4. Review of current cloud security maturity models in healthcare

Many healthcare security leaders are recognizing that compliance activities are important, but not enough to adequately mitigate the risks of data breaches and attacks.

Information Security Focus Area Maturity Model

The Information Security Focus Area Maturity (ISFAM) model is a focus area-oriented maturity model, originally proposed as a method for incremental progression [36]. It consists of a fixed number of maturity levels, each process identified by a focus area/domain, is assigned its own number of progressively more mature capabilities. The model is able to determine the current information security maturity level.

ISFAM model has 12 maturity levels and 13 focus areas. In these focus areas, 64 capabilities are assigned at the various maturity levels. The assessment of the maturity level is executed through a survey or a directed interview with an expert. The ISFAM covers the complete domain of information security, combining the application of ISO 2700-series, chapters from CISSP (Certified Information Systems Security Professional), Standard of Good Practice of the Information Security Forum (ISF), and the IBM Security Framework [37]. Its subsequent practices in information security divides the capabilities within the maturity model into four (4) groups such as, design, implementation, operational effectiveness, and monitoring.

As with all focus area maturity matrices, the lowest implemented capability defines the maturity level reached. ISFAM has successfully been evaluated using a medium-sized telecommunications organization. Despite its extensive and relatively fine-grained, and its practical approach are based on IBM's experiences, the ISFAM model remains designed as a sector-specific maturity model - small and medium-based organizations as its focus. In addition, it was developed for application with software development, and was specifically made for information security problems obtained from IBM's experience. Lastly, it made no mention of been applicable to future technologies such as cloud computing.

Cloud Security Capability Maturity Model

The Cloud Security Capability Maturity Model (CSCMM) includes domains and maturity levels. There are twelve cloud security domains and four maturity levels. Each domain consists of a set of cyber security practices, and the practices are achievement objectives specific for each cloud security domain. The maturity levels apply to each domain and specify progression of maturity. The model can be tailored for suitable objectives of different cloud service model (IPSaaS) and deployments (Public, Private, and Hybrid Cloud). Lastly, it provides the guidance to support the organizations implement and enhance their cyber security capabilities on cloud system [38].

There is not a complete cloud security standard because cloud technology is evolving much faster than standards [39]. Therefore, creating a set of cyber security domains just based on the current security standards does not fully consider emerging issues and attack surfaces. CSCMM was built from a systematic review approach on existing cloud security models and standards, traditional security maturity models, as well as trends in emerging technologies. As a result, these twelve security domains, eight security domains are from traditional maturity models, and four cloud specific security domains were chosen as they cover comprehensive aspects of cyber security and accommodate emerging security issues.

To assess the maturity level of the model in general and a security domain in particular, a security metrics framework was proposed. This framework includes relevant quantitative metrics for measurable assessment. It presents a balance assessment of the overall security of an organization qualitatively and quantitatively. For senior managers, it offers assessment of the security status for making decision concerning

business plan and direction. For security practitioners, it offers proactive measures and responsive actions. In addition, CCSMM model has 3 dimensions such as domain, levels and community (such as organization, community, state), this makes the model more suitable for organizations of different sizes, however, this model is considered technically complex to implement in healthcare [40–42].

Further twelve (12) cyber security maturity models were reviewed to investigate their strengths and weaknesses. These similarities identified amongst these maturity models are; all the models are hybrid-type maturity models with their multi dimensions including security domains and maturity levels, most security domains vary from infrastructures, data, networks, human, application, communications, compliance, to legal and contractual. To implement best security practices, security standards such as NIST, ISO 27000 series, COBIT are the baseline to implement and measure security levels in all models. Most of the models have implementation process through four steps from evaluation, gap identification, priority and planning, and plan implementation. Lastly, most of the models implement a 5-level framework to assess security state of each domain. These 5 levels involve a 3-stage process, the first stage is with no security management implementation, following stage focuses on the implementation of security standards to control security concerns. The third stage is an automatically security management with full security implementation. This stage is considered the innovative stage with highest security.
The differences also identified includes, each model has domains with different security requirements based on the goals of the model, making each model to have different advantages. None of these models mentioned extend their application to cloud computing environments and were industry-generic not streamlined to healthcare environment.

NHS National Infrastructure Maturity Model

The National Infrastructure Maturity Model (NIMM) Programme designed by Connecting for Health (CfH), has provided useful guidance, national standards, best practices and capability maturity tool for National Health Services (NHS) IT organizations to benchmark their local IT infrastructure services/capability in order to create a road map for improvements. It supports healthcare organizations to assess the maturity of different components of their business and IT capabilities. The assessment will provide an indication of how mature the organization is in a particular area and what steps should be taken to improve maturity. Healthcare organizations are to exercise the 12 NIMM core capability assessments in the first instance. Afterwards, a roadmap should be formulated to improve maturity, then assessments that are more specific to the healthcare organization should be selected and completed, and the outputs from these are then incorporated into the formulated roadmap [43].
Most healthcare trusts are required to work towards Level 3, Standardized – Consistent and predictable services, increasing the maturity of their infrastructure and service provision, moving from manual configurations to managed systems with automation and proactive monitoring of services. The Healthcare organizations recognize the fundamental part played by infrastructure in underpinning all information management and technology (IM&T) strategy and so has adopted the NIMM [44].

This model is still presently relevant in the cyber security maturity assessment of healthcare organization and stated to be platform-independent, however, it does not take into consideration the rapidly changing landscape of technology, such as characteristics of cloud and its resulting threats.

Health Information Network Capability Maturity Model

Health Information Network (HIN) Capability Maturity Model is a tool that will support the objective assessment and formulate plans for improve operational capabilities, level of service and value delivered by HIN organizations. This fully vetted and accepted pan Canadian model can serve as a strategic and operational planning tool. It was established based on other maturity models in healthcare and other industries, Canada Health Infoway's strategic opportunities for action and key enablers [45], HIN Planning and Operations Leading Practices Discovery Framework [46], and observations and input from the leading practice organization interviews. It is intended to be a tool for guiding stepwise assessment which can be used to determine a jurisdiction's current capability maturity level, categorize an objective maturity level appropriate to the jurisdiction's needs, and develop a roadmap for progression toward that desired maturity level.
HIN Capability Maturity Model comprises of 10 capability domains and 5 maturity levels for each. It also includes an aggregate maturity across all domains, which can be used to broadly compare and communicate the overall maturity of the HIN. In order to apply this model, it is required to be refined with input from current jurisdictional HIE organization operators, system planners, and policy makers, and tools for self-assessment, action planning, and progress monitoring will also be required to make it consistently and uniformly applicable [47]. Its shortcomings are in tune with the NHS NIMM.

In summary, it can be inferred that mostly cyber security models require revision because of its fragmented and local approach. This review has established that cyber security maturity models support effective and efficient management of the security of their organizations. More importantly, stakeholders operate along secure mature path as mapped out by the maturity model to ensure overall security of the organization, rather than applying all the security controls available. Despite all these benefits, maturity models only provide a baseline-compliance model rather than the desired cyber security model that can deal with emerging cyber environment, its demanding cyber security usage, as well as its sophisticated attacks.

5. Conclusion and Future work

This paper reviewed cyber security standards, best practices, and guidance, and models including cloud security models, cyber security capability maturity models, mostly applicable within the healthcare environment. The main insight to be considered about the review is the present inadequacy of cyber security maturity models to effectively assess security in healthcare organizations actively using cloud computing.

Three specific issues were identified: First, the influencing factors of cyber security of a security maturity model should be more than standards-compliance. Second, integrate identified relevant factors into the maturity levels, and determine appropriate metrics for security assessment. Third, the model should be malleable for ensuring current cyber security and extensible for dealing with security for emerging cyber threats. These are the research problems this research intends to mitigate or resolve by the proposal of a maturity model - Maturity Model for Healthcare Cloud Security (M^2HCS). By identifying interactions between the several domains of healthcare information security and signifying them cogently in the M^2HCS, the model aims to be able to mitigate reactive assessment of security in healthcare cloud environment, and support incrementally operations to improve information security maturity within the healthcare organization.

References

1. Jafari S, Mtenzi F, Fitzpatrick R, O'shea B (2010) Security Metrics for e-Healthcare Information Systems: A Domain Specific Metrics Approach. Int J Digit Soc 1:
2. Herrmann DS (2007) Complete Guide to Security and Privacy Metrics: Measuring Regulatry Compliance, Operational Resilience, and ROI, 1st ed. Auerbach Publications, London
3. Payne SC (2007) A Guide to Security Metrics
4. Pamula J, Ammann P, Jajodia S, Ritchey R (2006) A framework for establishing, assessing, and managing trust in inter-organizational relationships. In: Proceedings of the 3rd ACM workshop on Secure web services - SWS '06. ACM Press, New York, New York, USA, p 23
5. Chew E, Swanson M, Stine K, et al (2008) Performance Measurement Guide for Information Security: NIST Special Publication 800-55 Revision 1. Gaithersburg, MD
6. Schneier B (2004) Secrets and lies : digital security in a networked world. John Wiley & Sons
7. Webster J, Watson RT (2002) Analyzing the past to prepare for the future:writing a literature review. MIS Q 26:xiii–xxiii
8. Liberati A, Altman DG, Tetzlaff J, et al (2009) The PRISMA Statement for Reporting Systematic Reviews and Meta-Analyses of Studies That Evaluate Health Care Interventions: Explanation and Elaboration. PLoS Med 6:e1000100. https://doi.org/10.1371/journal.pmed.1000100
9. Okoli C, Schabram K (2010) A Guide to Conducting a Systematic Literature Review of Information Systems Research. Sprouts Work Pap Inf Syst 10:
10. (2013) Cisco Annual Security Report
11. (2013) ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements. In: Organ. Int. Norm. https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en
12. (2015) ISO/TR 17522:2015, Health informatics — Provisions for health applications on mobile/smart devices. In: Organ. Int. Norm. https://www.iso.org/obp/ui/#iso:std:iso:tr:17522:ed-1:v1:en
13. (2016) ISO 27799:2016 - Health informatics -- Information security management in health using ISO/IEC 27002. In: Organ. Int. Norm. https://www.iso.org/standard/62777.html
14. (2015) ISO/IEC 27017:2015 - Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services. In: Organ. Int. Norm. https://www.iso.org/standard/43757.html

15. (2013) ISO 22857:2013 - Health informatics -- Guidelines on data protection to facilitate trans-border flows of personal health data. In: Organ. Int. Norm. https://www.iso.org/standard/52955.html
16. (2018) HITRUST CSF version 9.1
17. (2013) NIST Special Publication 800-53 Revision 4 - Security and Privacy Controls for Federal Information Systems and Organizations. Gaithersburg
18. Jansen W, Grance T (2011) Guidelines on security and privacy in public cloud computing. Gaithersburg, MD
19. Mell PM, Grance T (2011) The NIST definition of cloud computing. Gaithersburg, MD
20. NIST Cloud Computing Security Working Group (2013) SP 500-299 (DRAFT), NIST Cloud Computing Security Reference Architecture
21. Hogan MD, Liu F, Sokol AW, Jin T (2011) NIST-SP 500-291, NIST Cloud Computing Standards Roadmap | NIST
22. Badger L, Grance T, Patt-Corner R, Voas J (2012) Cloud Computing Synopsis and Recommendations Recommendations of the National Institute of Standards and Technology
23. Liu F, Tong J, Mao J, et al (2011) NIST cloud computing reference architecture. Gaithersburg, MD
24. Scholl MA, Stine KM, Hash J, et al (2008) An introductory resource guide for implementing the Health Insurance Portability and Accountability Act (HIPAA) security rule. Gaithersburg, MD
25. (2012) A Business Framework for the Governance and Management of Enterprise IT
26. Cotton M, Cruley D, Gray J, et al (2017) NIST Cybersecurity Framework (CSF) Aligning to the NIST CSF in the AWS Cloud
27. (2018) Mapping Microsoft Cyber Offerings to NIST Cybersecurity Framework Subcategories
28. (2015) The Privacy Rule - HIPAA. In: HHS.gov. https://www.hhs.gov/hipaa/for-professionals/privacy/index.html
29. (2017) The Security Rule - HIPAA. In: HHS.gov. https://www.hhs.gov/hipaa/for-professionals/security/index.html
30. (2017) HITECH Act Enforcement Interim Final Rule. In: HHS.gov. https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html
31. (2009) Security Guidance for Critical Areas of Focus in Cloud Computing
32. (2009) Security Guidance for Critical Areas of Focus in Cloud Computing V2.1
33. (2011) SECURITY GUIDANCE FOR CRITICAL AREAS OF FOCUS IN CLOUD COMPUTING V3.0
34. Mogull R, Arlen J, Gilbert F, et al (2017) Security Guidance for Critical Areas of Focus in Cloud Computing v4.0
35. (2013) Auditing the Cloud Controls Matrix
36. Steenbergen VM, Bos R, Brinkkemper S, et al (2010) The Design of Focus Area Maturity Models. In: Winter WR, Zhao JL, Aier S (eds) LNCS. Springer-Verlag Berlin Heidelberg, pp 317–332
37. Spruit M, Röling M (2014) ISFAM: THE INFORMATION SECURITY FOCUS AREA MATURITY MODEL. In: European Conference on Information Systems (ECIS). AIS Electronic Library (AISeL), Tel Aviv, p 16
38. Le NT, Hoang DB (2017) Capability Maturity Model and Metrics Framework for Cyber Cloud Security. In: Special Issue on Communication, Computing, and Networking in Cyber-Physical Systems. Universitatea de Vest din Timisoara, pp 277–290
39. Duncan B, Whittington M (2014) Compliance with standards, assurance and audit:

does this equal security? In: Proceedings of the 7th International Conference on Security of Information and Networks - SIN '14. ACM Press, New York, pp 77–84
40. Siponen M, Willison R (2009) Information security management standards: Problems and solutions. Inf Manag 46:267–270. https://doi.org/10.1016/J.IM.2008.12.007
41. Stevanović B (2011) Maturity Models in Information Security. J Inf Technol 1:44–47
42. Le NT, Hoang DB (2016) Can maturity models support cyber security? In: IEEE 35th International Performance Computing and Communications Conference (IPCCC). IEEE Computer Society, Las Vega, NV, USA, pp 1–7
43. Savvides A (2009) NHS Infrastructure Maturity Model BCS/ASSIST Presentation
44. NHS England SS and T (2014) General Practice IT Infrastructure Specification
45. (2013) Opportunities for Action A Pan-Canadian Digital Health Strategic Plan
46. Giokas D, Sekhon H, Mestre A, et al (2015) A White Paper - Health Information Network (HIN) Leading Practices
47. Giokas D, Sekhon H, Mestre A, et al (2015) A Discussion Paper for Health Information Network (HIN) Capability Maturity Model