applied sciences

MDPI

Article

Risk-Based Cybersecurity Compliance Assessment System (RC2AS)

Afnan Alfaadhel [1], Iman Almomani [1,2,*] and Mohanned Ahmed [1]

[1] Security Engineering Lab, Computer Science Department, Prince Sultan University, Riyadh 11586, Saudi Arabia; 221421249@psu.edu.sa (A.A.); mqasem@psu.edu.sa (M.A.)
[2] Computer Science Department, King Abdullah II School of Information Technology, The University of Jordan, Amman 11942, Jordan
* Correspondence: i.momani@ju.edu.jo or imomani@psu.edu.sa

Abstract: Cybersecurity attacks are still causing significant threats to individuals and organizations, affecting almost all aspects of life. Therefore, many countries worldwide try to overcome this by introducing and applying cybersecurity regularity frameworks to maintain organizations' information and digital resources. Saudi Arabia has taken practical steps in this direction by developing the essential cybersecurity control (ECC) as a national cybersecurity regulation reference. Generally, the compliance assessment processes of different international cybersecurity standards and controls (ISO2700x, PCI, and NIST) are generic for all organizations with different scopes, business functionality, and criticality level, where the overall compliance score is absent with no consideration of the security control risk. Therefore, to address all of these shortcomings, this research takes the ECC as a baseline to build a comprehensive and customized risk-based cybersecurity compliance assessment system (RC2AS). ECC has been chosen because it is well-defined and inspired by many international standards. Another motive for this choice is the limited related works that have deeply studied ECC. RC2AS is developed to be compatible with the current ECC tool. It offers an offline self-assessment tool that helps the organization expedite the assessment process, identify current weaknesses, and provide better planning to enhance its level based on its priorities. Additionally, RC2AS proposes four methods to calculate the overall compliance score with ECC. Several scenarios are conducted to assess these methods and compare their performance. The goal is to reflect the accurate compliance score of an organization while considering its domain, needs, resources, and risk level of its security controls. Finally, the outputs of the assessment process are displayed through rich dashboards that comprehensively present the organization's cybersecurity maturity and suggest an improvement plan for its level of compliance.

Keywords: compliance assessment; maturity model; cybersecurity; risk; ECC; Saudi Arabia

Citation: Alfaadhel, A.; Almomani, I.; Ahmed, M. Risk-Based Cybersecurity Compliance Assessment System (RC2AS). *Appl. Sci.* **2023**, *13*, 6145. https://doi.org/10.3390/app13106145

Academic Editors: Peter R.J. Trim and Yang-Im Lee

Received: 7 April 2023
Revised: 10 May 2023
Accepted: 12 May 2023
Published: 17 May 2023

1. Introduction

Currently, many organizations have amalgamated cyberspace solutions within their conventional business processes [1]. The more a business integrates digital solutions and increases its online presence, the more it becomes vulnerable to cybersecurity threats. The COVID-19 pandemic was a motivating factor for many companies to embrace technology-based solutions to aid online learning and virtual communication, support vulnerable supply chains, and avail autonomous systems [2]. Cyberattackers also took advantage of the increased online presence of many businesses to intensify their attacks [3]. Reports indicate that 43% of all cyberattacks targeted small and medium enterprises (SMEs) and their employees by initiating attacks such as SQL injections, distributed denial of services, man-in-the-middle, spam, phishing, and email malware [4]. A significant impediment to depending on cyberspace is the emergence of security complexities that could lead to financial losses and, subsequently, adversely affect organizational reputation and goodwill [5] .Based on the numerous benefits associated with the use of cyberspace in work

environments, cybersecurity remains a requirement that businesses must acquire while implementing various types of online technologies to manage their activities.

Several cyber security standards have been established for accountability and obligation to ensure that senior leadership in organizations handles risk and security problems thoughtfully and strategically. The enactment of harmonized international cybersecurity regulations has provided a framework for the development of consistent data protection in many organizations, increasing innovation and interoperability and reducing costs, and minimizing the complexity of implementing security and privacy controls as noted by [6]. The implementation of general cybersecurity practices by organizations has enabled businesses to exercise best practices that reduce the risk of access or loss of data, the disruption of business processes, and the loss of assets due to cyberattacks [7]. The implementation of cybersecurity compliance policies improves the protection of an enterprise's information system and related resources from cyberattacks coming from internal or external cyber attackers. Organizations and entities that fail to comply with already set cybersecurity regulations could subject their assets, information systems, and data in cyberspace to massive losses accrued due to penalties, litigation of cyberattack issues, and loss of reliability of their services, which could impact their performances and competitiveness.

Most recent developments in cybersecurity models are in line with the needs of enterprises using cyberspace to manage their operations and databases. Currently, the most used international cybersecurity standard is the National Institute of Standards and Technology (NIST), which provides security guidelines to companies and individuals in the United States to protect their critical infrastructure from cyberattacks. Such standards are also provided by the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001 [8] and the Payment Card Industry Data Security Standard (PCI DSS). Muhammad and Alsaleh [9] noted that organizations are required to comply with cybersecurity because failure to do so increases the risk of undesirable cybersecurity habits that can expose an entity's assets to cyberattacks. Despite the awareness of many organizations about threats to cybersecurity, compliance with cybersecurity standards has been ineffective in most organizations.

Various institutions and government agencies ensure enterprises abide by regulations and compliance policies. In the United States, the major agencies are the NIST and the Cybersecurity and Infrastructure Security Agency (CISA). The United Kingdom has similar agencies that enforce cybersecurity compliance policies. The National Cyber Security Centre (NCSC) provides detailed advice, regulation compliance, and management of cybersecurity incidents [10].

On the other hand, Saudi Arabia (SA) currently aims to change its economic patterns, reduce its reliance on oil, and expand its public service industries throughout its 2030 vision plan. An example of this strategy is the implementation of cybersecurity policies as an advancement toward its Vision 2030 [11]. According to Almudaires et al. [11], cybersecurity has become increasingly significant in Saudi Arabia's economy due to its reliance on technology to sustain its economic activities. The Saudi authorities are potentially threatened by cyber criminals as many incidences of cyberattacks have been reported such as phishing and ransomware. With the contemporary cybersecurity challenges and to maintain the organization's information and digital resources, the Royal Decree established the National Cybersecurity Authority (NCA) on 31 October 2017. The primary responsibility of the NCA is to perform administrative and regulatory roles in the field of cybersecurity in Saudi Arabia. In 2020, based on the collective efforts of NCA and the collaboration of national entities, Saudi Arabia ranked (2) globally in the Global Cybersecurity Index issued by the United Nations specialized agency for Information and Communication Technologies [12]. NCA has developed essential cybersecurity control (ECC), an adequate cybersecurity regulation in Saudi Arabia. ECC aims to ensure the development of services in a coordinated, safe, and secure manner. This includes providing security, meeting demands, managing the scarcity of resources, ensuring market development, protecting users, and supporting innovations.

Compliance with the ECC regulation is mandatory for all of Saudi Arabia's organizations with IT systems [13]. However, (a) there are limitations in the existing research works that highlighted and studied the compliance assessment process of the ECC, (b) the compliance assessment processes of different international cybersecurity standards and controls such as (ISO2700x, PCI and NIST) are usually generic for all organizations with different scopes, business functionalities, and criticality levels. A better understanding of the organization's domain and status should be considered to reflect compliance accurately. Incorporating additional factors to differentiate between the compliance of different organizations prioritizes the compliance level and provides a more reliable cybersecurity landscape at the national level. Therefore, this research proposes a risk-based cybersecurity compliance assessment system (RC2AS) that improves the current assessment process by considering the organization's domain and integrating the corresponding risk in the overall compliance score calculations, consequently continually enhancing the cybersecurity compliance assessment process.

Accordingly, the benefits of proposing a risk-based cybersecurity compliance system in terms of a well-developed system can be summarized in the following points:

(a) Measuring the organizations' cybersecurity compliance level using a self-assessment questionnaire (SAQ) approach.
(b) Choosing one of the proposed overall compliance-calculation methods based on the organizations' domains, needs, and resources.
(c) Using color-coding techniques to better reflect the compliance status based on the risk level.
(d) Determining the critical risk controls based on the domain risk level and the impact that is based on the organizations' criticality, scope, and business functionality.
(e) Producing rich dashboards to present the organization's cybersecurity maturity and compliance status.
(f) Setting a clear improvement and action plan to reach the organization's target compliance.
(g) Offering a cybersecurity tool to help the assessor to perform the audit assessment.

Therefore, this paper presents a customized and comprehensive cybersecurity compliance system based on ECC, the national cybersecurity reference regulation in Saudi Arabia. The ECC has well-defined regulations built based on different international standards. Thus, using the ECC for this research will support adopting the RC2AS system for other international standards. The system services are offered through an offline standalone assessment tool for organizations to measure their cybersecurity compliance level efficiently. The assessment results are presented through rich dashboards to reflect the organization's current status. Additionally, the proposed system guides the organization to an action plan to reach its target compliance level. Figure 1 shows our overall methodology to create the proposed RC2AS.

The rest of the paper is organized as follows. Section 2 presents the overall methodology followed to build the proposed RC2AS. Section 3 introduces the current cybersecurity standards and recent related works. Section 4 presents the details of the proposed risk-based cybersecurity compliance assessment system (RC2AS). Section 5 shows the evaluation of RC2AS and discusses its results. Finally, section 6 draws conclusions and suggests possible future works.

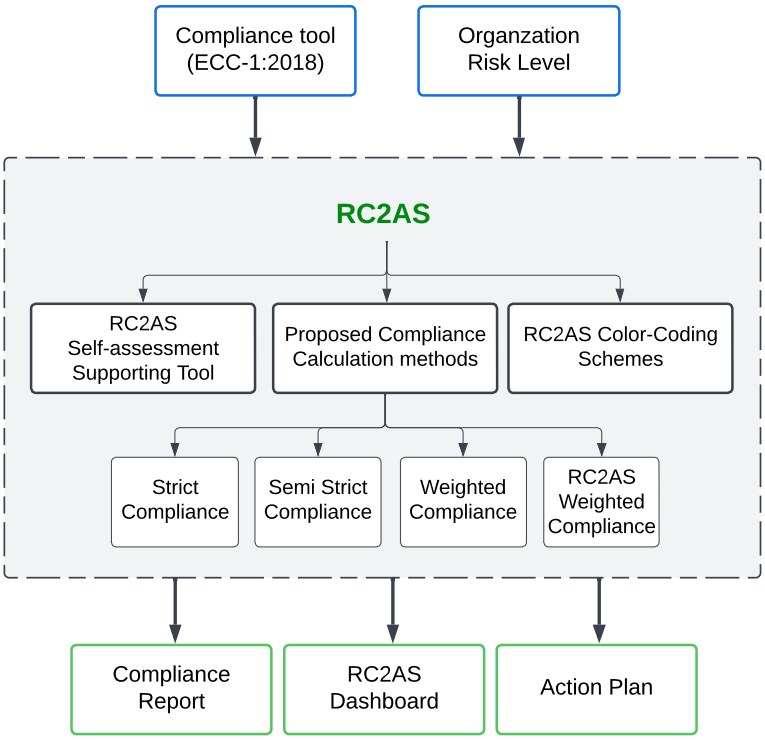

Figure 1. Overall RC2AS building methodology.

2. Methodology

The methodology we followed to solve the research problem addressed in this study is summarized as follows. The main inputs to our proposed solution are the current ECC tool beside the organization risk level of each subdomains. The risk level is identified based on the domain and the nature of the organization, which can be decided by the cybersecurity authority in any country. The proposed solution (RC2AS) includes but is not limited to (a) the RC2AS self-assessment supporting tool, (b) suggested well-studied compliance-calculation methods (four methods), and (c) RC2AS color-coding schemes. Finally, the outcome of our proposed solution and the assessment process are presented in terms of a compliance report, RC2AS's rich dashboards, and future action plans. Figure 1 presents the overall methodology followed to build the proposed RC2AS.

3. Background and Related Work

This section presents the background to national and international cybersecurity frameworks and standards. Additionally, it discusses and compares recent related works.

3.1. International Cybersecurity Framework and Standards

Developing a cybersecurity maturity model aims to help organizations systematically improve their cybersecurity status over time and align it with their overall business objectives. Most cybersecurity maturity models are currently developed according to international standards such as NIST, ISO/IEC 27001, and PCI DSS. Various studies have been proposed focusing on improving enterprises' cybersecurity practices. For instance, Gerl et al. [14] examined the utilization of control objectives for information technologies (COBIT-19) in establishing an IT governance framework for collaboration in higher education settings in Bavaria. The authors hypothesized that the chief information officer (CIO) role is critical to improving collaboration among universities. Based on the findings, implementing COBIT enhanced the trust among collaborating partners. COBIT also creates

a consistent model of the role of the CIO in defining the baseline of mutual understanding of competencies and responsibilities. Since the article presented a case study, the generalization of the findings to other problems or settings can be challenging. Cybersecurity is an essential subject in the industrial internet of things because the information equips individuals that use various practices and tools to protect individuals and organizations from occurrences such as data breaches and ensures they comply with cybersecurity policies [15]. Implementing security controls could also involve incorporating blockchain technologies to strengthen cybersecurity. For example, a study exploring a security framework based on blockchain is presented in this study [16]. Thus, adjustments to the security regulations arise because of the constantly shifting information technology environment.

Almuhammadi and Alsaleh [9] defined a five-level maturity model that includes the twenty-two categories of the NIST cyber security framework for critical infrastructure (CSF) to measure the implementation regularly and maintain the security posture. The model presented a comparison between NIST CSF and additional frameworks and standards related to security such as ISO/IEC 27001 and COBIT. According to the authors of [17], Canada can achieve better outcomes in managing health emergencies and maintaining privacy rights by designing laws to comply with European Union (EU) in a way that freedoms relating to privacy can only be limited for shorter periods. Additionally, Aliyu et al. [18] noted that the challenge encountered was a lack of capability maturity models that integrate regulations within the United Kingdom. As a result, they developed a novel framework that includes all of the privacy and security regulations and best practices, such as the general data protection regulation (GDPR), the data security and protection toolkit (DSPT), and PCI DSS. These security standards can be leveraged to enhance the cybersecurity compliance levels of higher education institutions. From a theoretical viewpoint, capability maturity models offer a framework for improving process development operations. The proposed model, which comprises fifteen categories related to security and six maturity levels, can be developed into an online system to support self-assessment and automated compliance reporting. A major weakness of the article is that it is largely theoretical. Indeed, an empirical analysis of the model can provide insight into the effectiveness of its utilization in practical environments.

Although the current maturity models are used to measure the security maturity level of enterprises or specific systems, they cannot be used to create and establish cybersecurity maturity models for protecting cyberspace. The existing maturity models have created static security models and are not flexible to react to new security trends. Zarour et al. [19] explains that the emergence of DevOps is informed by the need to produce fast and high-quality releases by bringing the development and operations teams to work together. DevOps still lack a clear definition in most studies, thereby creating challenges in some quarters. DevOps maturity models are instrumental in providing critical insights regarding what can be done in assessing DevOps-adopted practices. Therefore, there is a need to incorporate perspectives from various levels, such as security experts, practitioners, and management. This can help measure the enterprise's overall security level or the critical system from emerging security threats.

Many cybersecurity compliance and maturity models have been presented. Firstly, Proença and Borbinha [20] introduced a maturity model as an assessment tool for enterprises to provide the current state maturity model of the information security management system (ISMS) based on ISO/IEC 27001. Another approach was proposed by Bolanio et al. [21] to improve the security network of higher education institutions based on ISO27033. [22] Makupi and Masese [23] also created a model to compute the university's information security model based on ISO27001 using related clauses of higher education institutions. Yaokumah and Dawson [24] applied ISO/IEC 21827 [25] to measure the controls related to the security of higher education institutions (HEIs) in Ghana. Another model proposed by [26] examined the maturity level of information systems from a security perspective based on ISO 27001:2013. The idea was to help institutions identify vulnerable areas and implement appropriate interventions to enhance cybersecurity compliance.

Based on the results, most institutions of higher learning in Indonesia have not complied with the requirements of ISO 27001:2013 for cybersecurity; the biggest domain gap has been observed between the current and the expected maturity levels observed in compliance and system acquisition, development, and maintenance. While using a questionnaire as the study methodology helped answer the research questions, the subjectivity associated with this research approach was not addressed. One study proposes a dynamic approach to compliance assessment where organizations consider the return on investment relevant to the savings an organization can realize pertinent to the losses that could arise when security features are not implemented [27]. One of the significant guidelines for implementing cybersecurity governance is ISO/IEC 27001, directing institutions and companies to create specific protocols to mitigate, control, and supervise potential risks. Through the protocols, implementing digital environment rules becomes easier [28]. Suwito et al. [29] applied the assessment security maturity model by combining various models and standards such as ISO/IEC 27001, COBIT 4.1, and ITIL v3 (information technology infrastructure library) for higher education institutions in Indonesia. Hung et al. [30] examined the methods of enhancing the information security governance (ISG) of Taiwanese universities through a questionnaire by building the ISG maturity model by looking at appropriate features. A similar model was designed by Bass [31] as derived from a documentary and the result from selected Ethiopian universities. Ismail et al. [32] proposed a specialized information security framework for Malaysia's higher education institutions.

3.2. Importance of Security in Saudi Arabia

Cybersecurity threats are one of the primary concerns of the Saudi leadership in this digitalized world. Since August 2017, the cyberattack on Saudi Aramco was inflicted with the virus named Shamoon. It considers one of the renowned cyberattacks cases in Saudi Arabia [33]. Due to the contemporary cybersecurity challenges and to maintain the organization's information and digital resources, the government of Saudi Arabia has classified the strategics' priority as cybersecurity and businesses are making it a priority to avoid breaches reputationally and financially. In 2017, a Royal Decree was issued to establish the National Cybersecurity Authority (NCA), which is the national and specialized reference for matters related to cybersecurity in the Kingdom. The primary responsibility of this organization is to realize the idea of a safe and reliable Saudi cyberspace that enables growth and prosperity [34].

Based on the NCA's objectives and in continuation of its part in regulating and protecting Saudi Arabia's cyberspace, NCA has established and developed several cybersecurity frameworks, controls, and guidelines at the national level within its scope to protect its national security vital interests, government services, and critical infrastructure in line with vision 2030 of Saudi [13]. The NCA has set out to establish the cybersecurity minimum standards for national and government agencies at risk of cyberattacks to ensure the safety of their data, for instance, essential cybersecurity controls (ECC), critical systems cybersecurity controls (CSCC), and data cybersecurity controls (DCC).

3.3. Saudi Arabia Security, Frameworks Maturity, and Standards

Enterprise security is very important in Saudi Arabia because many incidences of cyberattacks have been reported compared to other countries. Saudi Arabia's government is committed to developing a powerful and operational cybersecurity framework to overcome these issues. They have designed multiple frameworks, such as NCA creating essential cybersecurity controls (ECC) to help the enterprise follow cybersecurity best practices [13]. The Communications and Information Technology Commission developed a cybersecurity regulatory framework (CRF) for the Information and Communications Technology sector [35]. Moreso, a SAMA cybersecurity framework, was formerly developed by the Saudi Central Bank (SAMA) to secure financial sectors such as banks, financing companies, and financial market infrastructure from cyberattacks [36]. In academic literature, Al Hamed and Alenezi [37] presented a maturity model to mature the ability of business continuity

management (BCM) and disaster recovery (DR) for Saudi Arabia's information technology companies. Additionally, Nurunnabi [38] explains that the investigation of the differences between International Financial Reporting Standards (IFRS) and Saudi accounting standards provides an opportunity for the areas that may need to improve further to ensure better standards are realized in the financial sector. Moreover, it ensures that investors have a clear understanding of the financial reporting strategies that they need to embrace in different transactions.

The rationale behind this study was to address cybersecurity issues facing SMEs by presenting an appropriate framework. According to [39], each SME is unique, hence the need to utilize a model that aligns with its needs and wants. To this end, the authors presented specific cybersecurity models for organizations in different industries, including education, health care, and commerce. A holistic model that covers the different models to enhance coordination was also presented. A major weakness of the study was that it merely presented the models and did not evaluate their effectiveness and efficiency. Nevertheless, the adoption of these models can help SMEs in Saudi Arabia improve their cybersecurity implementation processes. Alsahafi et al. [40] stated that there is a need for institutions to implement ISMS such as ISO/IEC 27001 to minimize the risks of cyberattacks on their information assets. The ISO/IEC 27001 acts as a baseline cybersecurity framework. A central hypothesis of the study could be whether universities with ISO/IEC 27001 are fully compliant with NCA-ECC. The assumption here is that it is not fully understood to what extent Saudi institutions with ISO/IEC are compliant with the NCA-ECC. The study design was a qualitative survey. Instrumentation included the use of interviews presented in an interview table from which the answers (data) were collected and analyzed. The sample size used was three universities, whose cybersecurity officers were interviewed on each clause and sub-clause. Research results indicated that ISO/IEC 27001 universities are approximately 64% compliant with the NCA-ECC. Another proposed framework by Almomani et al. [41] found that most cybersecurity models for high-education institutions lacked practical mechanisms for the continual assessment of security levels. Accordingly, they presented a new comprehensive and customized framework, "SCMAF", aligned with international and local security standards. The research method adopted in this study encompassed evaluating current cybersecurity maturity frameworks in Saudi Arabia, mapping local and international frameworks, developing the SCMAF model, implementing it, demonstrating the utilization of SCMAF, and highlighting the approach for keeping the framework updated.

Table 1 presents a comparative analysis of related studies for cybersecurity compliance and the maturity model, for both international and national standards, in terms of the general idea and the technique used; the focus areas were both international or national, the followed standard, and if the proposed solution included ECC . This enabled the organization to measure the maturity level of cybersecurity among the international and Saudi standards using a user self-assessment tool. Part of the presented maturity models was based on international standards, for instance, those [9,18,20,23,24]. To improve cybersecurity in Saudi Arabia other approaches were presented [39,41,42]. The table shows the rest of the comparisons.

Although there are many existing attempts to propose compliance assessment tools and maturity models, there is an apparent absence of studies that highlight the compliance assessment process of the NCA-ECC. Therefore, due to the shortage in the related literature and the importance for organizations to comply with the security regulations in Saudi Arabia, this research takes the existing ECC cybersecurity compliance process as a baseline to build a comprehensive and customized risk-based cybersecurity compliance assessment system (RC2AS). As a result, RC2AS provides an accurate cybersecurity assessment that reflects the organization's current status considering its domain and risk ranges.

Table 1. Comparative analysis of the related works.

Ref.	General Idea	Approach Used	Focus Area	Standards	NCA-ECC?
[9]	Present a five-level maturity model that assesses twenty-three areas, which include the twenty-two categories of NIST CSF and the compliance assessment to measure the implementation regularly and maintain the target security posture.	Compared the scales and domains evaluated by different maturity models to identify the gap in NIST CSF.	International	• NIST CSF • ISO27001 • ISF • COBIT 5	No
[14]	Propose IT governance model for universities in Bavaria. The model defines governance relationships between cooperative IT service providers, CIOs, universities, and all Bavaria stakeholders.	Universities taught applied sciences and CIO boards of higher learning institutions in Bavaria.	International	COBIT 2019	No
[18]	Design framework for maturity assessment (HCYMAF) that higher education institutions in the UK can use to assess their ISMS by using a web-based self-assessment model.	The study combined structured interviews, case study evaluations, feedback, and an online seminar.	International	• GDPR • PCI DSS • DSPT NISD	No
[20]	Propose a maturity model that can be used to plan, implement, review, and enhance an ISMS based on ISO 27001.	Used design science researcher paradigm; an iterative approach; and model adoption techniques such as configuration, specialization, aggregation, and analogy.	International	ISO 27001	No
[21]	Propose a model for assessing and appraising network security in higher education using six components drawn from ISO 27033 framework.	The study relied on the standardized ISO 27033 assessment questionnaire.	International	ISO27033	No
[23]	Find solution that entails creating a maturity model that can be used to assess the information security management systems in universities.	Used design research approach and evaluated cumulative factors statistically to determine their contribution to the proposed model followed ISO 27001 standards.	International	ISO27001	No
[24]	Proposed use of ISO/IEC 21827 maturity model for assessing the IT security posture and security controls.	A questionnaire based on ISO 27033 standards was developed and distributed to network security teams in different learning institutions.	International	ISO21827	No
[26]	Develop a maturity framework that can be used to assess and measure the information security management systems of higher learning institutions in Indonesia for conformity to the ISO 27001 standard.	The research evaluated 35 universities in Indonesia and assessed their compliance with ISO 27001:2013 standards.	International	ISO 27001:2013	No
[29]	Present an approach that combines different frameworks to improve the effectiveness of security maturity management assessments.	A case study on one university in Indonesia.	International	• COBIT 4.1 • ISO27001 • ITIL v3	No
[30]	Propose an information security governance (ISG) model for colleges and universities. The model proposes three maturity levels: low, medium, and high.	Evaluate the maturity of information security governance through a questionnaire survey.	International	None	No
[31]	Present an ICT maturity model for higher education in Ethiopia comprising eight levels.	Adopted action research founded on an iterative approach focused on problem identification, planning, action, and evaluation. The study surveyed education institutions.	International	None	No

Table 1. *Cont.*

Ref.	General Idea	Approach Used	Focus Area	Standards	NCA-ECC?
[32]	Propose an information security management framework comprising five constructs for HEIs in Malaysia.	Interviews and surveys were conducted to gain relevant insights.	International	• COBIT • ISO27001	No
[37]	Propose a model for evaluating the maturity of business continuity and disaster-recovery practices for information technology organizations in SA.	The study adopted an iterative approach to link existing theories to emerging data.	National	ISO22301	No
[39]	Incorporate three models and a combined model for cyber security countermeasures within SMEs in education, healthcare, and commerce in Saudi Arabia.	The study considered organizational special needs and asset sensitivity.	National	NIST	No
[41]	Propose a lightweight cybersecurity maturity assessment framework for HEI in SA.	The study developed a comprehensive policy that bridges local needs and international standards.	Both	• NCA-ECC • CRF • GDPR • NIST • PCI DSS • DSPT	Yes
[40]	Measure the extent to which certified ISO/IEC 27001 Saudi organizations adhere to the NCA-ECC and propose a framework for complying with not fully implemented controls.	The study design is a qualitative survey that included the use of interviews presented in an interview table from which the answers (data) were collected and analyzed.	Both	• NCA-ECC • ISO 27001	Yes
RC2AS	Propose a risk-based cybersecurity compliance assessment system based on ECC.	A comprehensive and customized risk-based cybersecurity compliance assessment system was provided that reflects the current status of the organization, considering its domain and risk ranges.	National	NCA-ECC	Yes

4. Risk-Based Cybersecurity Compliance Assessment System (RC2AS)

This section starts by discussing the existing ECC assessment and compliance tool. Then, it introduces the proposed RC2AS with all its services.

4.1. Existing ECC Assessment and Compliance Tool

The objective of this sub-section is to fully understand and highlight the ECC-1:2018 assessment and compliance tool by studying their domains/controls, scope, objective, and compliance assessment process. A better understanding of the tool will facilitate and pave the way toward establishing the foundation of the RC2AS solution. The list of main functions listed in this section was used as a starting point to build the functions of the proposed system. Before diving into these functions, the key points of the ECC are:

- Description: Minimum cybersecurity standards were customized and developed after reviewing international cybersecurity standards, controls, frameworks, previous cybersecurity attacks incidents, and international practices in cybersecurity to minimize the risk of cyberattack to enterprises' information and technical assets that are created by external and internal threats.
- Scope: It is mandatory for all Saudi Arabian entities within the government and private sectors.
- Objective: The essential objectives must be focused on to protect the information and assets of organizations: confidentiality, availability, and integrity of information, with attention paid to the pillars that cybersecurity focuses on (strategy, people, procedures, and technology).

- ECC Domains and Structure: As shown in Figure 2, ECC consists of 5 main cybersecurity domains, 29 cybersecurity subdomains, and 114 cybersecurity controls.

Currently, each organization should evaluate and assess its compliance with ECC through self assessments and by using the compliance tool [13] . The only and latest release of ECC is (ECC-1:2018). The current ECC self-assessment tool is based on an Excel spreadsheet that is officially posted by the NCA.

(ECC-1:2018 Tool) [43]. The main domains of ECC are placed on separate Excel sheets (ECC.1 Assessment, ECC.2 Assessment, ECC.3 Assessment, ECC.4 Assessment, and ECC.5 Assessment). In addition, the subdomain(s) related to that main domain are also displayed. Table 2 shows the structure of each subdomain and a sample subdomain.

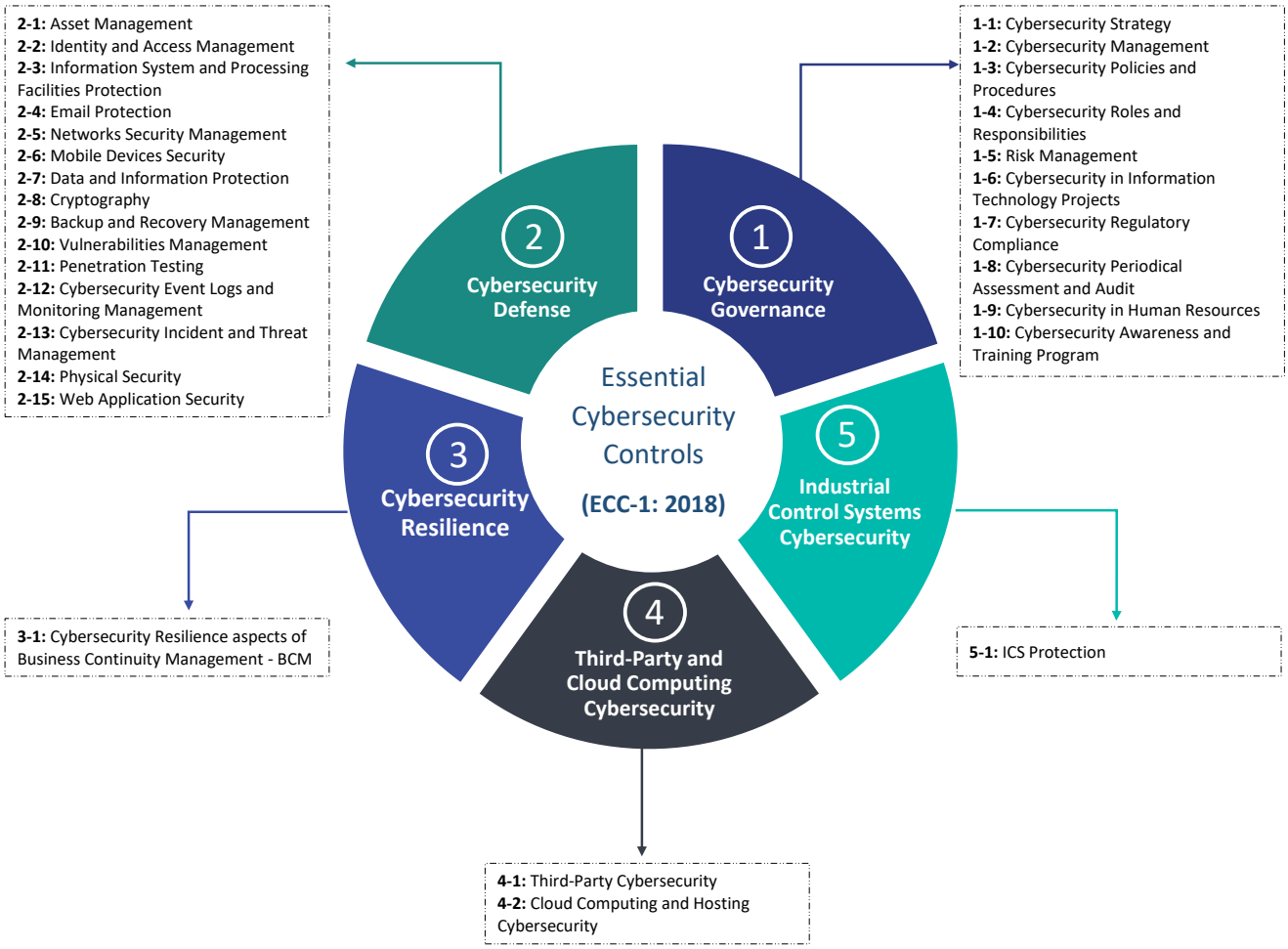

Figure 2. Current ECC-1:2018 domains and subdomains.

Table 2. Current ECC subdomain structure.

Subdomain Structure		
Ref. No.	subdomain's Name	
Control Ref. No.	Control Clause	Compliance Status
Sample of subdomain Structure		
1-1	Cybersecurity Strategy	
1-1-1	A cybersecurity strategy must be defined, documented, and approved. It must be supported by the head of the organization or his/her delegate (referred to in this document as authorizing official). The strategy goals must be in-line with related laws and regulations [13].	Implemented
1-1-2	A roadmap must be executed to implement the cybersecurity strategy [13].	Not Implemented
1-1-3	The cybersecurity strategy must be reviewed periodically according to planned intervals or upon changes to related laws [13].	Not Implemented

The compliance fulfillment of an organization is represented by one of the following statuses: "Implemented", "Partially Implemented", "Not Implemented", or "Not Applicable". Organizations measure and assess how they comply with each control clause's requirement(s). The "Implemented" status means that all of the requirements for this control clause are fully implemented. The "Partially Implemented" status means that some of the control requirements have not been implemented; in other words, the implementation percentage is greater than 0% and less than 100%. If all of the control requirements have not been implemented, then the status will be "Not Implemented". Lastly, the "Not Applicable" status applies to any control that does not apply to the organization. Table 3 shows the compliance status along with the implementation percentage.

Table 3. Current ECC compliance statuses along with implementation percentages.

Compliance Status	Implemented	Partially Implemented	Not Implemented	Not Applicable
Implementation Percentage	100%	>0% to <100%	0%	NA

Currently, the self-assessment tool applies a color-coding technique for the compliance status. Four different colors are used depending on the compliance status. Each status has one color. The "Implemented" status is indicated by the color "Green", "Partially implemented by "Orange" color."Not implemented" status is colored "Red", and the "Gray" color is used for "Not Applicable". Table 4 illustrates the compliance status along with the color coding.

Table 4. Current ECC compliance status along with the color-coding.

Compliance Status	Implemented	Partially Implemented	Not Implemented	Not Applicable
Color-Coding				

Finally, after an organization fills out its compliance status in the self-assessment, a summary of the compliance evaluation results will be generated, as shown in Figure 3. The left side includes **(a)** the total number of security controls under each compliance status, and **(b)** a chart indicating the percentage of controls in each compliance status. There will also be a summary for each domain (five main domains) on the same sheet. For example, Figure 4 illustrates the summary of the overall result for domain 1: "Cybersecurity Governance".

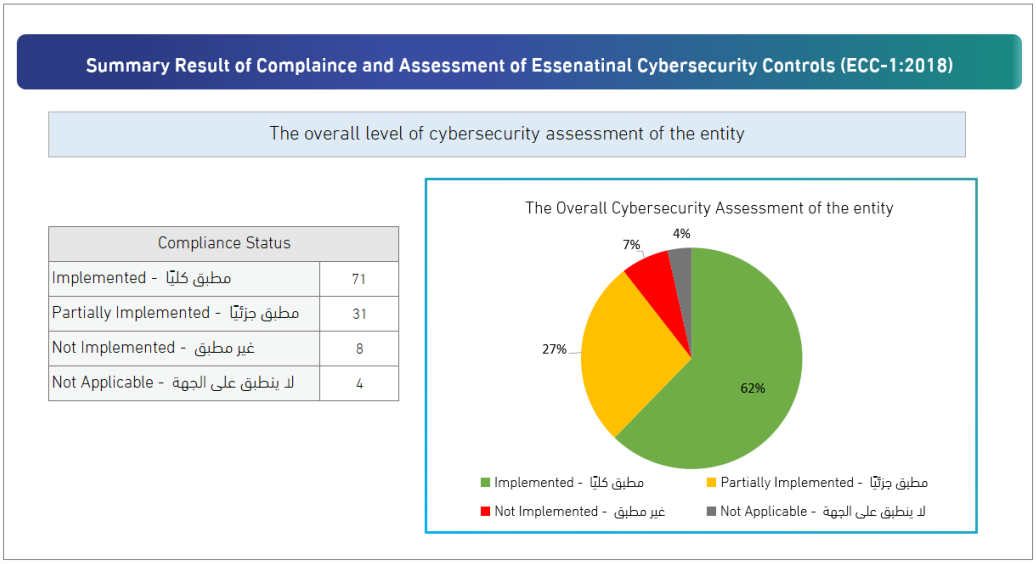

Figure 3. Current ECC—Summary of the results of the overall assessment, Note: the current tool is only available in the Arabic language. For this reason, we translated several sentences into English in Figures 3 and 4 for illustration purposes.

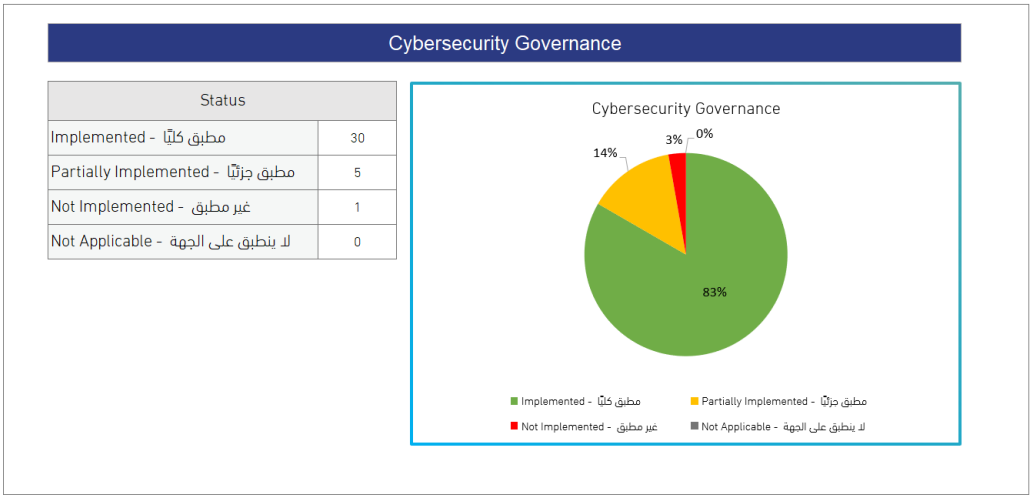

Figure 4. Current ECC—Summary of the results of the main domain "Cybersecurity Governance", Note: the current tool is only available in the Arabic language. For this reason, we translated several sentences into English in Figures 3 and 4 for illustration purposes.

The summary result of the compliance with ECC (Figure 3) shows the percentage of each compliance status of security controls as there is no overall compliance score provided in the current ECC tool. In the pie chart, each compliance status percentage (%) is calculated based on the number of main controls on specific "compliance status" out of the total of main controls (114 controls). For instance, the percentage of "Implemented" in Figure 3 is calculated based on the number of "Implemented" controls (71). So, by using Equation (1), the compliance percentage for "Implemented" compliance status is calculated as follows ($\frac{71}{114} * 100$), corresponding to (62%). The remaining compliance statuses are calculated in the same way. The below Equations (1)–(4) illustrate the formula for how each compliance status percentage is calculated as follows:

$$Implemented = \frac{\sum(F_{Control})}{T_{Controls}}\% \quad (1)$$

$$Partially\ Implemented = \frac{\sum(P_{Control})}{T_{Controls}}\% \quad (2)$$

$$Not\ Implemented = \frac{\sum(N_{Control})}{T_{Controls}}\% \quad (3)$$

$$Not\ Applicable = \frac{\sum(NA_{Control})}{T_{Controls}}\% \quad (4)$$

where; F = fully implemented control(s); P = partially implemented control(s); N = not implemented control(s); NA = not applicable control(s); T = total controls.

4.2. Proposed Risk-Based Cybersecurity Compliance Assessment System (RC2AS)

As mentioned earlier, compliance with ECC is mandatory for all national Saudi organizations (public and private) with IT systems. So, all entities should evaluate and measure their compliance by using the publishing tool (ECC-1:2018 Tool) [43].Many service provider companies help national entities to assess and measure their compliance level through dedicated services and tools. These tools help an entity to demonstrate its commitment to different standards or regulations and enable it to perform gap assessments of its weaknesses and strengths. This will result in enabling the entity to develop its road map based on its priorities.

Therefore, this research takes the existing ECC cybersecurity compliance tool as a baseline to build a comprehensive and customized risk-based cybersecurity compliance assessment system (RC2AS). RC2AS is developed to be compatible with the current ECC tool. This system offers a self-assessment tool that helps the organization evaluate and check its compliance with ECC. Moreover, RC2AS supports weakness identification and provides better planning accordingly to enhance its compliance level based on its priorities for future improvements. Lastly, RC2AS proposes several calculation methods for the overall compliance score of ECC.

This section presents the proposed system that provides various services by highlighting: (a) the RC2AS overall workflow, and (b) the RC2AS supporting tool that provides a well-structured and comprehensive questionnaire derived from ECC controls. Such a tool will provide a practical way to encourage entities to complete the questionnaire and obtain their compliance level, (c) the proposed calculation methods of the overall cybersecurity compliance of ECC, (d) the RC2AS compliance status color-coding scheme, and (e) the rich dashboards RC2AS offer to reflect the current status of compliance with ECC, accurately. Moreover, setting a clear improvement and action plan will allow them to reach their ECC target compliance level.

Additional details of the RC2AS and the services it offers are described in the following:

4.2.1. RC2AS Workflow

The proposed system is offered as an offline version of the self-assessment tool that organizations or auditors can use. To start using the system, there will be high-level questions to establish the applicable domain by answering predefined questions. Accordingly, based on the answers, the appropriate domains/subdomains will be displayed to facilitate and speed up the assessment process by hiding the controls that do not apply to the organization's domain. In addition, the users will choose the recommended and preferable calculation method (one or more) from the options list: (a) strict compliance, (b) semi-strict compliance, (c) weighted compliance, or (d) RC2AS weighted compliance. Table 5 shows a sample of the RC2AS high-level questionnaire.

Table 5. RC2AS High-level questionnaire.

RC2AS High-Level Questionnaire				
Entity Name:				
General Question				
1. Does the entity use cloud computing?	☑	Yes	☐	No
2. Does the entity have a third party?	☑	Yes	☐	No
3. Does the entity use industrial control systems and operational technology (ICS/OT)?	☑	Yes	☑	No
Calculation Compliance Mode				
Select the compliance calculations method:	☑	Strict compliance		
	☐	Semi-strict compliance		
	☐	Weighted compliance		
	☑	RC2AS weighted compliance		

The proposed system assesses the domains one by one. Then, the subdomain(s) of this domain will be fulfilled individually. If the subdomain is applicable to the organization and this subdomain has dependent questions, the associated questions of this subdomain will be shown. If the answers are yes, then the remaining questions will be displayed. The next domain (if any) will appear only in case all questions have been answered, and so forth. Once this domain's subdomain(s) are examined, the following domain will repeat the same steps. Ultimately, when all of the domains' questions are answered, the compliance level will be calculated and displayed through rich dashboards. Figure 5 illustrates the workflow of the proposed system.

4.2.2. RC2AS Supporting Tool

To facilitate the assessment process, the RC2AS supporting tool uses a questionnaire approach. Accordingly, each control will have one or more questions to assess and measure the organization's compliance with a specific control. Table 6 highlights the RC2AS with subdomain structure.

Table 6. RC2AS supporting tool with subdomain structure.

Ref. No. of Subdomain	**Name of Subdomain**			
Control Ref. No.	Control Clauses	Question(1) Question(2) … Question(n) [1]	RC2AS compliance answer(1) RC2AS compliance answer(2) … RC2AS compliance answer(n) [1]	Compliance Status

[1] n: means the number of questions related to this control.

The questions on a particular control could depend on each other. An example of questions' dependency is shown in Table 7. Only the first question on control (1-2-1) will be presented. Only if the answer is "Yes" or "Partially Implemented" will Q2 and Q3 be displayed. The following question will not appear if the answer to Q1 is "No". This will expedite the assessment process and make it more convenient. On the other hand, there might be no dependency between the questions, as shown in control (1-2-2), where each question does not depend on the others.

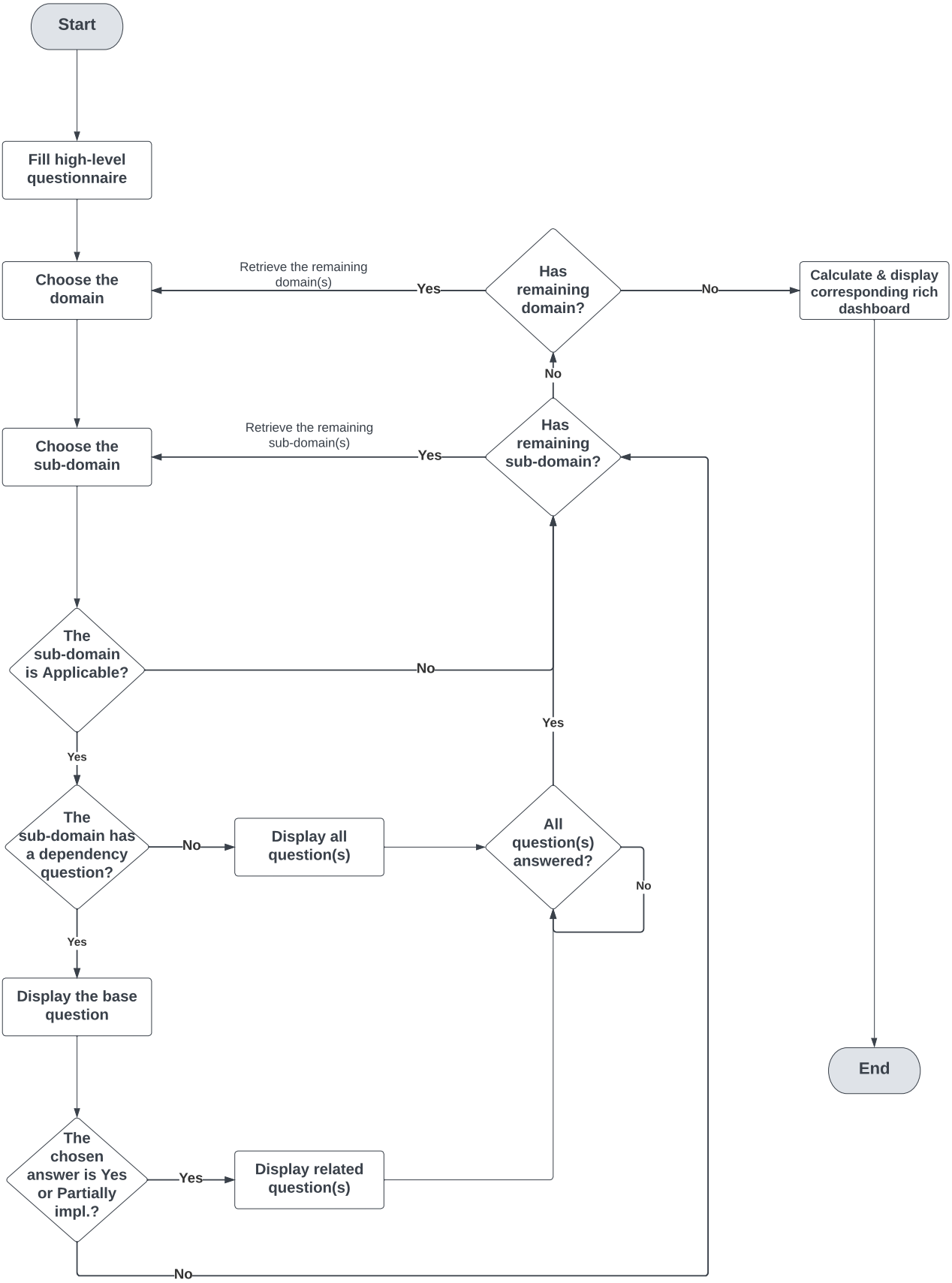

Figure 5. The proposed risk-based cybersecurity compliance assessment system (RC2AS) workflow.

Table 7. Sample of RC2AS subdomain structure (with and without dependency).

1-2	Cybersecurity Management	
	Sample of Control's Question(s) with Dependency	
1-2-1	A dedicated cybersecurity function (e.g., division, department) must be established within the organization. This function must be independent of the information technology/information communication and technology (IT/ICT) functions (as per the Royal Decree number 37140 dated 14/8/1438H). It is highly recommended that this cybersecurity function reports directly to the head of the organization or his/her delegate while ensuring that this does not result in a conflict of interest [13].	**Q1:** Does the entity have a cybersecurity department?
		Q2: Is the cybersecurity department independent of information technology management in the entity?
		Q3: Does the cybersecurity department report directly to the organization's head or his/her delegate while ensuring that this does not result in a conflict of interest?
	Sample of Control's Question(s) without Dependency	
1-2-2	The position of cybersecurity function head (e.g., CISO), and related supervisory and critical positions within the function, must be filled with full-time and experienced Saudi cybersecurity professionals [13].	**Q1:** Is the cybersecurity department function headed by full-time and experienced Saudi cybersecurity professionals?
		Q2: Do the related supervisory and critical positions in the cybersecurity department function with full-time and experienced Saudi cybersecurity professionals?

Accordingly, the organization answers each question to measure its compliance level. The answer could be one of the following options. (a) If the organization accomplished all of the requirements of an associated question, then the chosen answer is 'Yes'. (b) If the organization partially implements the requirements, then the organization selects the percentage of this implementation (>0% to $\leq$ 35%, >35% to $\leq$ 85%, or >85% to <100%). Otherwise, (c) the answer selection will be 'No'. Lastly, (d) if it is not applicable, the answer 'NA' will be selected. These RC2AS compliance answers are derived and inspired by the current compliance status of the ECC assessment tool shown in Table 3. The different RC2AS answer options are shown in Table 8.

Table 8. RC2AS compliance answer options.

RC2AS Compliance Answer	**Yes**	**Partially Implemented with**			**No**	**NA**
Implementation Percentage	100%	>0% to $\leq$35%	>35% to $\leq$85%	>85% to <100%	0%	NA

4.2.3. Proposed Calculation Methods for the Overall Compliance Score of ECC

As we have mentioned in Section 4.1, what has been published by NCA and presented in the current compliance and assessment tool of the ECC tool does not provide an overall compliance score. Therefore, RC2AS proposes several possible calculation methods to provide the overall compliance score:

- Method (1): Strict compliance.
- Method (2): Semi-strict compliance.
- Method (3): Weighted compliance.
- Method (4): RC2AS Weighted compliance.

Now, we will describe each method and the attributes and factors that are needed to calculate the overall compliance score.

(A) **Strict Compliance**

This is the most strict method as it only considers the fully implemented controls. The "Partiality Implemented" and "Not Implemented" controls are discarded. The fully implemented control will have a weight value of (1), and the rest will have a (zero) value.

This means that only fully implemented controls will be counted (100% implementation), and other controls will not be counted (from > 0% to < 100% implementation). Equation (5) shows how the compliance score of this method is calculated:

$$Compliance\ Score = \frac{\sum(F_{Control})}{TA_{Controls}}\% \quad (5)$$

where;

F = No. Fully Implemented Control(s); TA = No. of Applicable Control(s);

(B) **Semi-Strict Compliance**

This method is less strict than the above method. Here, the compliance status "Implemented" will have the same weighted value, which is (1), whereas "Partially Implemented" has a weight value equal to (0.5). Otherwise, no weight value is given (zero value). Accordingly, Equation (6) calculates the overall compliance score for this method:

$$Compliance\ Score = \frac{\sum(F_{Control} + 1/2P_{Control})}{TA_{Controls}}\% \quad (6)$$

where;

F = No. Fully Implemented Control(s); P = No. Partially Implemented Control(s); TA = No. of Applicable Control(s);

(C) **Weighted Compliance**

Before we present the attributes of this compliance score equation, referring to the RC2AS compliance answer options mentioned above in Table 8, where there are three different levels of compliance status based on the implementations percentage of the control, which are (a) >0% to <=35%, (b) >35% to <=85%, and (c) >85% to <100%. Thus, weighted "Partiality Implemented" is embedded in this equation to impact the calculation of the overall compliance score. We map each of these RC2AS compliance answer options to dedicated weight values depending on the percentage of implementation of this control as detailed in Table 9:

Table 9. Mapping RC2AS compliance answer options with weight values.

RC2AS Compliance Answer	Yes	Partially Implemented with			No	NA
Implementation Percentage	100%	>0% to <=35%	>35% to <=85%	>85% to <100%	0%	NA
Weight Value	1	0.75	0.5	0.25	0	-

Therefore, the overall compliance score is calculated in Equation (7):

$$Compliance\ Score = \frac{\sum_{i=1}^{n}(Weight\ Value_i)}{TA_{Controls}}\% \quad (7)$$

where;

n = No. of total Control(s); TA = No. of Applicable Control(s);

(D) **RC2AS Weighted Compliance**

A better understanding of the organization's domain and status is needed to reflect compliance levels accurately. Therefore, this method differentiates organizations by different scopes, business functionality, and criticality level. For this reason, the overall compliance score should not be measured similarly.

This method includes the risk level of the subdomains to calculate the overall compliance score. This means that the regulator predates a risk level for each subdomain in ECC (29 subdomains) depending on different criteria and conditions. To clarify more, each organization will have a risk level of one of the following (high, medium, or low) according

to the risk impact in case the subdomain controls are not implemented. However, the organization can officially request the regulator to change the risk level of the subdomains (if required).

The following example elaborates more on how this method is used. There are two organizations: the first is a university, and the second is a CNI (Critical National Infrastructure) organization. Both organizations are not fully implementing control in a subdomain (2-10). Accordingly, the impact of not fully implementing this control is definitely not the same for both organizations. Thus, both organizations will be assigned to a different risk level for the subdomain; subsequently, the overall compliance score will be affected by the risk value of that subdomain. The above formula (Equation (7)) will be modified to consider the risk value as shown in Equation (8):

$$Compliance\ Score = \frac{\sum_{i=0}^{n}(Risk\ Based\ Weight\ Value_i)}{TA_{Controls}}\% \quad (8)$$

where

n = No. total Control(s); TA = No. of Applicable Control(s);

As mentioned before, there are three different risk levels (high, medium, and low), each with a risk value (1, 0.75, and 0.5), respectively. To calculate the "Risk-based Weight Value", the compliance status weight value and the risk value are multiplied as shown in Equation (9):

$$Risk\ Based\ Weight\ Value = Weight\ Value * Risk\ Value \quad (9)$$

Table 10 describes the difference in the weight value, in case the risk is considered or not.

4.2.4. RC2AS Color-Coding Scheme

Influenced by the current color coding highlighted in Table 4, RC2AS enhances the color-coding scheme to reflect the risk level of the compliance status. So, in the case of low risk, lighter degrees of the color are used, whereas, in the case of high risk, darker degrees of the color are used. This new color-coding scheme is applied only to the "Implemented" and "Partially Implemented" compliance statuses. There are no changes for the "Not Implemented" and "Not Applicable" statuses. To elaborate, Table 11 shows the used color depending on two factors: the compliance status and the risk-based weight value.

Table 10. RC2AS compliance answers along with the corresponding weight value while considering the risk level or not.

RC2AS Compliance Answer	Weight Value	Risk Level	Risk Value	Risk-Based Weight Value
Yes (100%)	1	High Medium Low	1 0.75 0.5	1.00 0.75 0.5
Partially (>85% to <100%)	0.75	High Medium Low	1 0.75 0.5	0.75 0.56 0.38
Partially (>35% to <=85%)	0.50	High Medium Low	1 0.75 0.5	0.50 0.38 0.25
Partially (>0% to <=35%)	0.25	High Medium Low	1 0.75 0.5	0.25 0.19 0.13
No (0%)	0	High Medium Low	0	0.00
Not Applicable (NA)	NA	High Medium Low	NA	NA

Table 11. RC2AS color-coding scheme.

Compliance Status	Risk-Based Weight Value	Color
Implemented	100%	
	75%	
	50%	
Partially Implemented	>85% to <100%	
	>35% to ≤ 85%	
	>0% to ≤ 35%	
Not Implemented	0	
Not Applicable	N/A	

4.2.5. RC2AS Rich Dashboards

Lastly, the dashboard page will be displayed after filling out the self-assessment and answering all of the questions related to all subdomains. First, the user needs to select the model from the following options: (strict compliance, semi-strict compliance, weighted compliance, and RC2AS weighted compliance) along with the date range. Accordingly, comprehensive dashboards will be generated and displayed. These dashboards include (a) the overall compliance score with ECC based on the selected model. Moreover, they include the overall compliance score across all models (Figure 6), and (b) the compliance score for each main domain per compliance statute is also based on the selected model (Figure 7). Accordingly, they provide the organization with insight into its cybersecurity posture per domain, and they provide a detailed view of each main domain and the compliance level for each control. This helps the organization to gain valuable insight into the most critical compliance concerns, which will support it in building its activities and actions to enhance its cybersecurity controls and prepare action plans accordingly. (c) The RC2AS evaluation of the organization among dates ranges across the main domains based on the selected model (Figure 8), which allows for the close monitoring of the changes within the domain controls along with the selected duration, and (d) the proposed action plan for the organization based on its current compliance status.

As mentioned before, the ECC has 29 subdomains. Each subdomain has a risk level (high, medium, and low) that the regulator redefines. Accordingly, based on compliance level, the subdomains will be divided among these risk levels using the proposed color-coding scheme. The visualized action plan helps the organization understand its current compliance status with ECC. A complete summary is provided for all domains and subdomains, including their compliance and risk levels. Additionally, this plan helps the organization to identify its weaknesses and design a well-structured strategy to enhance its level based on its priorities and resources. To illustrate more, the chart in Figure 9 allows the organization to prioritize its actions. For example, the subdomains that are not fully implemented and have a high risk level should be considered first. Therefore, this will be used as an action plan to draw future implementations based on the risk and compliance levels. Moreover, such a summary encourages the organization to continuously implement the subdomains that are categorized as high-risk and fully implemented.

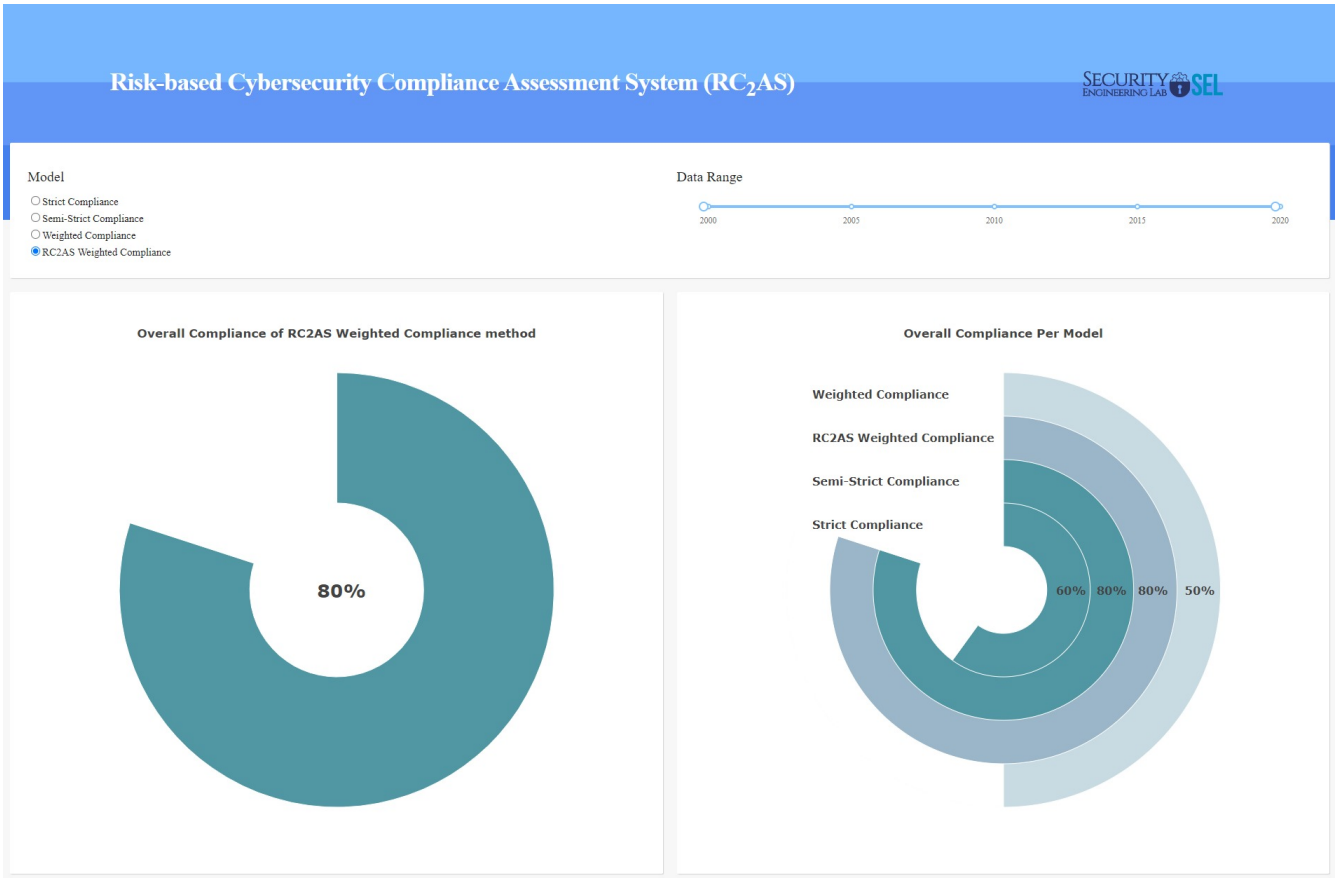

Figure 6. RC2AS dashboard of ECC—(a).

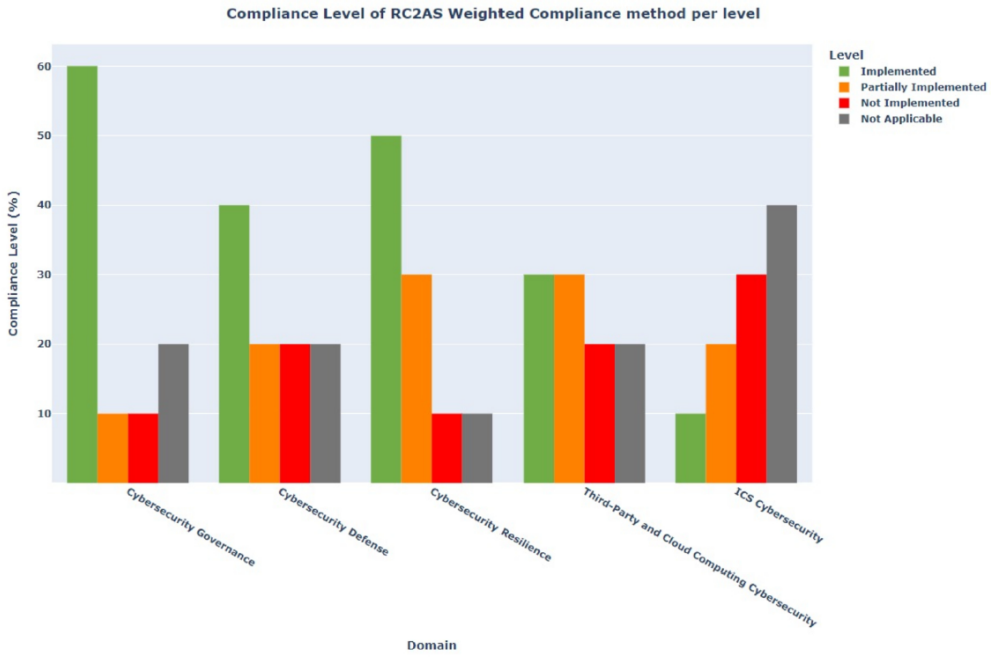

Figure 7. RC2AS dashboard of ECC—(b).

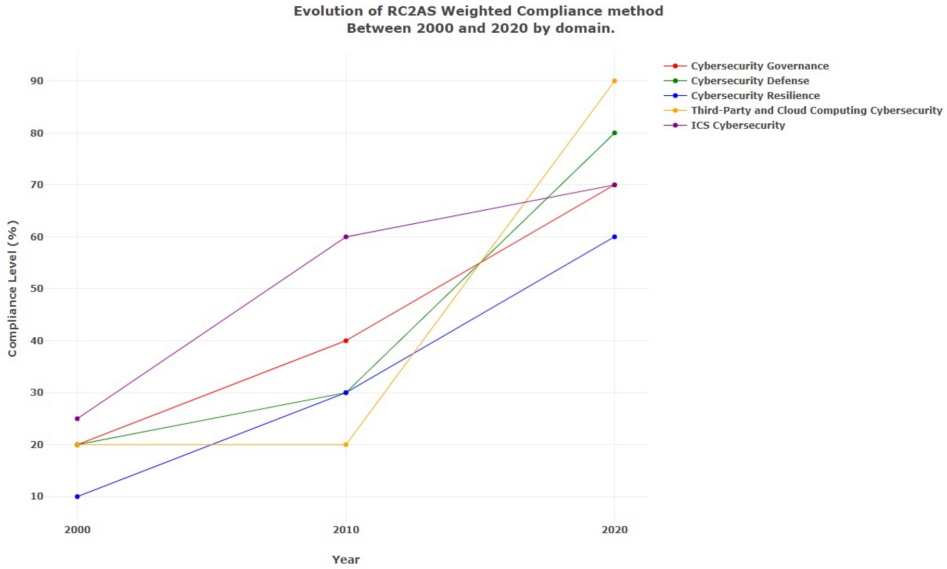

Figure 8. RC2AS dashboard of ECC—(c).

Figure 9. RC2AS dashboard of ECC—(d).

5. Proposed System Evaluation and Results Discussion

As highlighted before, the current ECC did not publish any compliance score calculation methods. Therefore, to evaluate the effectiveness of the proposed risk-based cybersecurity compliance assessment system (RC2AS) and examine all of its proposed calculation methods, several scenarios have been considered. These scenarios aim to conduct a deep comparative analysis OF these methods. Two entities, X and Y, will be utilized in implementing the different calculation models. For simplicity, one of the ECC subdomains is chosen to run these scenarios, which is subdomain (1-2) -"Cybersecurity Management", as shown in Table 12.

Table 12. Subdomain (1-2)-"Cybersecurity Management".

1-2	Cybersecurity Management
Control No.	**Control Clauses**
1-2-1	A dedicated cybersecurity function (e.g., division, department) must be established within the organization. This function must be independent of the information technology/information communication and technology (IT/ICT) functions (as per the Royal Decree number 37140 dated 14/8/1438H). It is highly recommended that this cybersecurity function reports directly to the head of the organization or his/her delegate while ensuring that this does not result in a conflict of interest [13].
1-2-2	The position of cybersecurity function head (e.g., CISO), and related supervisory and critical positions within the function, must be filled with full-time and experienced Saudi cybersecurity professionals [13].
1-2-3	A cybersecurity steering committee must be established by the authorizing official to ensure the support and implementation of the cybersecurity programs and initiatives within the organization. Committee members, roles and responsibilities, and governance framework must be defined, documented, and approved. The committee must include the head of the cybersecurity function as one of its members. It is highly recommended that the committee reports directly to the head of the organization or his/her delegate while ensuring that this does not result in a conflict of interest [13].

5.1. Comparison Using the "Strict Compliance" Method

Assume that there are two entities (entity X and entity Y). Both entities implement controls (1-2-1 and 1-2-2) in subdomains (1-2). On the other hand, control (1-2-3) is "Partially Implemented" by entity X, while in entity Y it is "Not Implemented". Table 13 compares the number of each compliance status for subdomain (1-2) between the entities X and Y.

Table 13. Comparison of the number of each compliance status between two entities (X and Y).

Compliance Status	Implemented	Partially Implemented	Not Implemented	Not Applicable
Entity X	2	1	0	0
Entity Y	2	0	1	0

Accordingly, applying (Equation (5)) of the compliance score for both entities will result in achieving the same score value. Table 14 compares the overall compliance score for entities X and Y using the "Strict Compliance" method. This equation considers only the number of fully implemented controls out of the total controls. In this scenario, the number of fully implemented controls for both entities is (2); then, the compliance score is calculated as follows: $(\frac{2}{3} * 100)$ = (66.67%).

Consequently, it is observed that this method does not reflect the accurate, current state of compliance with subdomain (1-2). The implementation percentage on this subdomain is supposed to measure the overall compliance score. However, this method counts only the fully implemented controls and ignores everything else. So, "Partially Implemented" and "Not Implemented" statuses are not included.

Table 14. Comparison of the overall compliance score between the two entities, using "Strict Compliance" method.

Method Name	Entity X	Entity Y
Strict Compliance Method	66.67%	66.67%

5.2. Comparison Using the "Semi-Strict Compliance" Method

In this scenario, both entities have the same compliance status for all controls (1-2-1, 1-2-2, and 1-2-3), which are ("Implemented", "Implemented", and "Partially Implemented"). The main difference is in the implementation percentage for control (1-2-3). As illustrated in Table 15, entity X implemented around 70% of this control, whereas entity Y implemented 30%.

Table 15. Comparison of the number of each compliance status between two entities (X and Y).

Compliance Status	Implemented	Partially Implemented	Not Implemented	Not Applicable
Entity X	2	1 (70%)	0	0
Entity Y	2	1 (30%)	0	0

Nevertheless, by using (Equation (6)), the overall compliance score for entity X is the same as entity Y. To be specific, the compliance calculated for both entities will be $(\frac{2+0.5}{3} * 100)$ = (83.33%). In summary, both entities' "Partially Implemented" status will be treated the same (weight value 0.5) even though the implementation percentage is different. Therefore, this method still does not accurately reflect the overall compliance score, as described in Table 16.

Table 16. Comparison of overall compliance score between two entities by using "Semi-Strict Compliance Method".

Method Name	Entity X	Entity Y
Strict Compliance Method	66.67%	66.67%
Semi-Strict Compliance Method	83.33%	83.33%

5.3. Comparison Using the "Weighted Compliance" Method

In this method, we include the weight of the "Partially Implemented" status as part of the calculation. We will continue with the same scenario in the above method (Section 5.3), but in this case, we will evaluate the weights for the level of "Partially Implemented" (3 levels), which are ((a) >0% to <=35%, (b) >35% to<=85%, (c) >85% to <100%) taken into account in the overall calculation compliance score. The RC2AS self-assessment for entity X is shown in Table 17, while entity Y is shown in Table 18.

Table 17. Sample of RC2AS self-assessment of entity X.

1-2		Cybersecurity Management		
Control No.	Control Clauses	Question	RC2AS Compliance Answer	Compliance Status
1-2-1	A dedicated cybersecurity function (e.g., division, department) must be established within the organization. etc. [13].	**Q1:** Does the entity have a cybersecurity department?	Yes (100%)	Implemented
		Q2: Is the cybersecurity department independent of information technology management in the entity?	Yes (100%)	
		Q3: Does the cybersecurity department report directly to the organization's head or his/her delegate while ensuring that this does not result in a conflict of interest?	Yes (100%)	
1-2-2	The position of cybersecurity function head (e.g., CISO), and related supervisory and critical positions within the function, etc. [13].	**Q1:** Is the cybersecurity department function headed by full-time and experienced Saudi cybersecurity professionals?	Yes (100%)	Implemented
		Q2: Have the related supervisory and critical positions in the cybersecurity department functioned with full-time and experienced Saudi cybersecurity professionals?	Yes (100%)	
1-2-3	A cybersecurity steering committee must be established by the Authorizing Official to ensure the support and implementation of the cybersecurity programs and initiatives within the organization. Committee members, roles, etc. [13].	**Q1:** Does the entity have a cybersecurity steering committee to ensure the support and implementation of cybersecurity programs and initiatives within the organization?	Yes (100 %)	Partially Implemented
		Q2: Does the entity have defined, documented, and approved the committee members, roles and responsibilities, and governance framework?	Partially Imp. (>85% to <100%)	
		Q3: Does the committee in the entity include the head of the cybersecurity function as one of its members?	Yes (100%)	
		Q4: Does the committee report directly to the head of the organization or his/her delegate while ensuring that this does not result in a conflict of interest?	No (0%)	

Table 18. Sample of RC2AS self-assessment of entity Y.

1-2		Cybersecurity Management		
Control No.	Control Clauses	Question	RC2AS Compliance Answer	Compliance Status
1-2-1	A dedicated cybersecurity function (e.g., division, department) must be established within the organization. This etc. [13].	**Q1:** Does the entity have a cybersecurity department?	Yes (100%)	Implemented
		Q2: Is the cybersecurity department independent of information technology management in the entity?	Yes (100%)	
		Q3: Does the cybersecurity department report directly to the organization's head or his/her delegate while ensuring that this does not result in a conflict of interest?	Yes (100%)	
1-2-2	The position of cybersecurity function head (e.g., CISO), and related supervisory and critical positions within the function, etc. [13].	**Q1:** Is the cybersecurity department function headed by full-time and experienced Saudi cybersecurity professionals?	Yes (100%)	Implemented
		Q2: Have the related supervisory and critical positions in the cybersecurity department functioned with full-time and experienced Saudi cybersecurity professionals?	Yes (100%)	
1-2-3	A cybersecurity steering committee must be established by the authorizing official to ensure the support and implementation of the cybersecurity programs and initiatives within the organization. Committee members, roles and responsibilities, etc. [13].	**Q1:** Does the entity have a cybersecurity steering committee to ensure the support and implementation of the cybersecurity programs and initiatives within the organization?	Yes (100%)	Partially Implemented
		Q2: Does the entity have defined, documented, and approved the committee members, roles and responsibilities, and governance framework?	Partially Imp. (>0% to <35%)	
		Q3: Does the committee in the entity include the head of the cybersecurity function as one of its members?	No (0%)	
		Q4: Does the committee report directly to the head of the organization or his/her delegate while ensuring that this does not result in a conflict of interest?	No (0%)	

In summary, the difference in the implementation percentage for control (1-2-3) will be presented in this method. To illustrate this further, the implementation percentage for entity X on this control is around (70%), while for entity Y it is around (30%). Hence, by using (Equation (7)), the weight value for entity X in control (1-2-3) will be $(\frac{1+0.75+1+0}{4})$ = (0.69%), so the overall compliance score for entity X in subdomain (1-2) will be followed, $(\frac{2+0.69}{3} * 100)$ = (89.67%). In the same way, the weight value for entity Y in control (1-2-3) will be $(\frac{1+0.25+0+0}{4})$ = (0.31%), so the overall compliance score for entity X in subdomain (1-2) will be $(\frac{2+0.31}{3} * 100)$ = (77.00%).

Therefore, this method has two main advantages: (a) the reflective color coding for the compliance status; and (b) the overall compliance score of this subdomain, which better integrates the partially implemented control in the score calculation. Table 19 compares a case of including the weight value for "Partially Implemented" status on subdomain (1-2): "Cybersecurity Management".

Table 19. Comparison of overall compliance score between two entities by using "Weighted Compliance" Method.

Method Name	Entity X	Entity Y
Strict Compliance Method	66.67%	66.67%
Semi-Strict Compliance Method	83.33%	83.33%
Weighted Compliance Method	89.67%	77.00%

5.4. Comparison Using "RC2AS Weighted Compliance" Method

In the same way, we will continue with the example mentioned before in Section 5.2. However, here we will evaluate the overall compliance score while considering (a) the weight for the level of "Partially Implemented" status, and (b) the risk level of the subdomain that the regulator has predefined. Assume the risk level of subdomain (1-2) is "Low" for both entities. The self-assessments for both entities are shown in Tables 20 and 21.

This method presented the difference in compliance for both entities, specifically for control (1-2-3) with the risk values included. The overall compliance score of the subdomain (1-2) for both entities has been reduced due to the risk value for this subdomain being

"Low". For more illustrations, the risk-based weight value for both entities in controls (1-2-1) and (1-2-2) using Equations (8) and (9) will be reduced from value 1 without risk to 0.5 after a low-risk value. At the same time, the overall compliance score for entity X in control (1-2-3) will be $(\frac{0.5+0.38+0.5+0}{4})$ = (0.343%). So, the overall compliance score for subdomain (1-2) will be $(\frac{0.5+0.5+0.343}{3} * 100)$ = (44.79%). Similarly, the risk-based weight value for entity Y in control (1-2-3) will be $(\frac{0.5+0.34+0+0}{4})$ = (0.16%). So, the overall compliance score for entity X in subdomain (1-2) will be followed, $(\frac{1+0.16}{3} * 100)$ = (38.54%).

Table 20. Sample of RC2AS self-assessment of entity X.

1-2	Cybersecurity Management			
	Risk Level:	Low		
Control No.	Control Clauses	Question	RC2AS Compliance Answer	Compliance Status
1-2-1	A dedicated cybersecurity function (e.g., division, department) must be established within the organization, etc. [13].	**Q1:** Does the entity have a cybersecurity department?	Yes (100%)	Implemented
		Q2: Is the cybersecurity department independent of information technology management in the entity?	Yes (100%)	
		Q3: Does the cybersecurity department report directly to the head of the organization or his/her delegate while ensuring that this does not result in a conflict of interest?	Yes (100%)	
1-2-2	The position of cybersecurity function head (e.g., CISO), and related supervisory and critical positions within the function, etc. [13].	**Q1:** Is the cybersecurity department function headed by full-time and experienced Saudi cybersecurity professionals?	Yes (100%)	Implemented
		Q2: Do the related supervisory and critical positions in cybersecurity department function with full-time and experienced Saudi cybersecurity professionals?	Yes (100%)	
1-2-3	A cybersecurity steering committee must be established by the authorizing official to ensure the support and implementation of the cybersecurity programs and initiatives within the organization. Committee members, roles, and etc.[13].	**Q1:** Does the entity have a cybersecurity steering committee to support and implement cybersecurity programs and initiatives within the organization?	Yes (100%)	Partially Implemented
		Q2: Does the entity have defined, documented, and approved the committee members, roles and responsibilities, and governance framework?	Partially Imp. (>85% to <100%)	
		Q3: Does the committee in the entity include the head of the cybersecurity function as one of its members?	Yes (100%)	
		Q4: Does the committee report directly to the head of the organization or his/her delegate while ensuring that this does not result in a conflict of interest?	No (0%)	

Accordingly, by using this method it has been noticed that **(b)** the overall compliance score has been reduced here as this is an indicator that the entity needs to focus first on the subdomain with the highest level of impact. Furthermore, **(a)** the color coding for the "Implemented" and "Partially Implemented" statuses are lighter than the normal ones, as been affected by risk value as illustrated in Table 11. The comparison between the compliance level by including "Risk Value" is shown in Table 22.

As another example, we will provide the advantage of adding the risk level to the compliance score calculation method. Let us assume that we have two entities whose compliance statuses are similar for subdomain (1-2). However, the risk level is different as classified by the regulator. The risk level for subdomain (1-2) for entity X is "High", while for entity Y it is "Medium". The self-assessment for entity X is presented in Table 23:

Table 21. Sample of RC2AS self-assessment of entity Y.

1-2	Cybersecurity Management			
	Risk Level:	Low		
Control No.	Control Clauses	Question	RC2AS Compliance Answer	Compliance Status
1-2-1	A dedicated cybersecurity function (e.g., division, department) must be established within the organization. This etc. [13].	**Q1:** Does the entity have a cybersecurity department?	Yes (100%)	Implemented
		Q2: Is the cybersecurity department independent of information technology management in the entity?	Yes (100%)	
		Q3: Does the cybersecurity department report directly to the head of the organization or his/her delegate while ensuring that this does not result in a conflict of interest?	Yes (100%)	
1-2-2	The position of cybersecurity function head (e.g., CISO), and related supervisory and critical positions within the function, etc. [13].	**Q1:** Is the cybersecurity department function headed by full-time and experienced Saudi cybersecurity professionals?	Yes (100%)	Implemented
		Q2: Have the related supervisory and critical positions in the cybersecurity department function with full-time and experienced Saudi cybersecurity professionals?	Yes (100%)	
1-2-3	A cybersecurity steering committee must be established by the authorizing official to ensure the support and implementation of the cybersecurity programs and initiatives within the organization. Committee members, roles, etc. [13].	**Q1:** Does the entity have a cybersecurity steering committee to support and implement cybersecurity programs and initiatives within the organization?	Yes (100%)	Partially Implemented
		Q2: Does the entity have defined, documented, and approved the committee members, roles and responsibilities, and governance framework?	Partially Imp. (>0% to <35%)	
		Q3: Does the committee in the entity include the head of the cybersecurity function as one of its members?	No (0%)	
		Q4: Does the committee report directly to the head of the organization or his/her delegate while ensuring that this does not result in a conflict of interest?	No (0%)	

Table 22. Comparison of overall compliance score between two entities by using the "RC2AS Weighted Compliance" method in case of low-risk control.

Method Name	Entity X	Entity Y
Strict Compliance Method	66.67%	66.67%
Semi-Strict Compliance Method	83.33%	83.33%
Weighted Compliance Method	89.67%	77.00%
RC2AS Weighted Compliance Method	44.79%	38.54%

Although both entities have the same implementation percentage and the only difference between the two entities is the risk level of this control, the compliance score will be different since one entity has a "High" risk and the other has a "Low" risk level. Using Equation (8) to calculate the overall compliance score for both entities, the compliance score for entity X in subdomain (1-2) is calculated as $(\frac{1+1+0.69}{3} * 100) = (89.58\%)$, whereas the compliance score for entity Y is $(\frac{0.5+0.5+0.343}{3} * 100) = (44.79\%)$. Entity X obtains a higher compliance level for subdomain (1-2) than entity Y, even though entity Y implemented the controls for this subdomain (1-2) similar to entity X. The compliance level of this subdomain is affected by the risk level. The comparison of the overall compliance score is shown in Table 24.

Table 23. Sample of self-assessment of entity X (risk level: high).

1-2		Cybersecurity Management		
	Risk Level:	High		
Control No.	Control Clauses	Question	Answer	Compliance Status
1-2-1	A dedicated cybersecurity function (e.g., division, department) must be established within the organization, etc. [13].	**Q1:** Does the entity have a cybersecurity department?	Yes (100%)	Implemented
		Q2: Is the cybersecurity department independent of information technology management in the entity?	Yes (100%)	
		Q3: Does the cybersecurity department report directly to the head of the organization or his/her delegate while ensuring that this does not result in a conflict of interest?	Yes (100%)	
1-2-2	The position of cybersecurity function head (e.g., CISO), and related supervisory and critical positions within the function, etc. [13].	**Q1:** Is the cybersecurity department function headed by full-time and experienced Saudi cybersecurity professionals?	Yes (100%)	Implemented
		Q2: Do the related supervisory and critical positions in cybersecurity department function with full-time and experienced Saudi cybersecurity professionals?	Yes (100%)	
1-2-3	A cybersecurity steering committee must be established by the Authorizing Official to ensure the support and implementation of the cybersecurity programs and initiatives within the organization. Committee members, roles and, etc. [13].	**Q1:** Does the entity have a cybersecurity steering committee to support and implement cybersecurity programs and initiatives within the organization?	Yes (100%)	Partially Implemented
		Q2: Does the entity have defined, documented, and approved the committee members, roles and responsibilities, and governance framework?	Partially Imp. (>35% to <=85%)	
		Q3: Does the committee in the entity include the head of the cybersecurity function as one of its members?	Yes (100%)	
		Q4: Does the committee report directly to the head of the organization or his/her delegate while ensuring that this does not result in a conflict of interest?	No (0%)	

Table 24. Comparison between two entities with different risks.

Method Name	Entity X Risk Level: High	Entity Y Risk Level: Low
RC2AS Weighted Compliance Method	89.58%	44.79%

5.5. Real Case Study

As part of the validation of the new proposed system RC2AS, we conducted a real case study to provide a convincing argument for the efficacy of the proposed risk-based cybersecurity compliance assessment system and demonstrate its services through a real-life environment. We conducted a real study with a figure organization in Saudi Arabia in the academic sector. The selected organization's name is kept private here for confidentiality and privacy (anonymity) reasons and be referred to as (Alpha). The Alpha has won several accolades and distinctions for its outstanding academic and scientific achievements. An effective way to learn about the advantages and disadvantages of the proposed solution is to complete a case study with experts who are acquainted with the compliance assessment process. This strategy ensures that the appropriate individuals review the tool, provide inputs and insightful information about the suggested solution, and enhance its efficacy, leading to a more thorough and informative assessment. The evaluation process has been conducted with specialized experts at the Alpha organization. The phases of the evaluation process are as follows:

(A) **RC2AS Overview Description:** In this phase, before the specialized experts start using and experimenting with the proposed RC2AS self-assessment supporting tool, we arranged several workshops with the organization introducing the RC2AS tool and exploring its main features and functions. The proposed RC2AS tool has been offered as an offline version through a dedicated Excel file.

(B) **RC2AS Experiment:** This phase offered a live experiment, with the Alpa organization given a chance to perform a live examination of the RC2AS supporting self-assessment tool by itself and start answering the question(s) on each subdomain to assess its

cybersecurity compliance based on its domain. The RC2AS supporting tool uses a self-assessment questionnaire (SAQ) approach.

(C) **RC2AS Evaluation:** After finishing the assessment process, we conducted a final workshop with them to obatin their insights, recommendations, and feedback.

In conclusion, based on the feedback from the participants, the RC2AS is useful and valuable for the cybersecurity compliance assessment process, not only by expediting the assessment process but also by letting the organization choose between one of the proposed overall compliance-calculation methods based on their needs and resources. Finally, we have incorporated some of their recommendations to enhance the RC2AS tool functions and their user experience. Moreover, some of the suggestions will be considered for improvement in the proposed RC2AS solution in future work.

5.6. Results Discussion

Based on the comparisons conducted among the proposed calculation methods, it can be observed that the "RC2AS weighted compliance" method can provide organizations with a fair and accurate assessment that measures the current cybersecurity compliance level with ECC.

Additionally, there is no right or wrong method as each calculation method has a different purpose and usage based on the organization's needs and objectives and its business functions. Therefore, the main comparisons among the calculation methods with regard to purpose and usage are summarized in Table 25:

Table 25. The comparison among RC2AS proposed methods in terms of purpose and usage .

Method Name	Purpose and Usage
Strict Method	This method helps the organization to fully comply with the controls and requirements. Having a weak hole within the control will lead to exposing the entity and prevent achieving the objective of that control.
Semi-Strict Method	This method takes into consideration the efforts that the organization has made to comply with the requirements by increasing the compliance score of the control's requirements.
Weighted Compliance	This method differentiates between the level of implementation and gives a more specific score on the requirements that have been implemented. Thus, this will give a better idea of the progress of the entities' current status.
RC2AS Weighted Compliance	This method provides a better understanding of the organization's domain and status by differentiating between organizations with different scopes, business functionalities, and criticality levels. This method includes the risk level of the subdomains.

6. Conclusions and Future Work

Complying with the cybersecurity regulatory framework becomes essential to reduce the risk of security attacks and protect the nation's individuals, organizations, and economies. Such compliance is encouraged regionally and internationally. Therefore, Saudi Arabia is leading in defining a comprehensive cybersecurity regulatory standard that is followed and assessed through the introduced essential cybersecurity control (ECC).

The compliance assessments of international cybersecurity standards are general for all organizations regardless of their domains, business functionality, and criticality level. In addition, their current assessment approach does not consider that the risk level in case the security control is implemented or not in reference to the organization's scope. Having a unified compliance assessment process for all organizations may affect the national cybersecurity landscape. To ensure the protection of organizations with critical infrastructure, further factors need to be injected into the compliance assessment process.

Therefore, this research has been motivated to build a comprehensive and customized risk-based cybersecurity compliance assessment system (RC2AS) based on ECC, which is well-defined and inspired by many international standards. All national organizations having IT systems as part of their infrastructure need to orient themselves toward ECC using its assessment tool. RC2AS introduces a self-assessment tool that allows an organization to measure its compliance with the ECC and calculate the compliance score using different compliance-calculation methods that meet the organization's needs, criticality, and resources. This will provide a realistic, fair, and accurate assessment of the organization's compliance with the ECC. The offered assessment tool by RC2AS provides enhancements not only in regard to compliance score calculations but also to the assessment methodology,

carried out in a very convenient way with expressive color-coding schemes. The assessment results are visualized in rich dashboards that illustrate the organization's current status in fully complying with the ECC. The RC2AS tool guides the organization by addressing its weaknesses, setting a proper plan to maintain what has been achieved and suggesting possible solutions and ways to improve.

The proposed RC2AS has been evaluated by conducting several case studies that examine all of the suggested compliance-calculation methods, including "Strict Compliance", "Semi-Strict Compliance", "Weighted Compliance", and "RC2AS Weighted Compliance" methods, where each method has different features and equations. The selection of the method depends on the nature of the organization. A deep comparative analysis was conducted to differentiate between these methods and recommend their application scopes.

Even though the proposed RC2AS solution considers many factors that facilitate and help organizations assess their current cybersecurity compliance posture, it can be customized to meet the organization's needs, for instance, integrating the RC2AS with the existing internal mechanisms in the organization to avoid duplication of efforts. The employment of this feature will not only be effective but will also ensure a seamless experience for users.

For future work, an online version of RC2AS could be offered. In addition, RC2AS will be offered to be used by different types of organizations to take their inputs and suggestions for improvements. Finally, RC2AS can be adopted by other international standards and controls.

Author Contributions: Conceptualization, I.A. and A.A.; methodology, I.A.; software, A.A.; validation, A.A., I.A. and M.A.; formal analysis, A.A. and I.A; investigation, A.A., I.A. and M.A; resources, A.A. and I.A; data curation, A.A. and I.A; writing—original draft preparation, A.A, I.A and M.A.; writing—review and editing, I.A.; visualization, A.A., I.A. and M.A.; supervision, I.A.; project administration, I.A.; and funding acquisition, I.A. All authors have read and agreed to the published version of the manuscript.

Funding: The APC was funded by Prince Sultan University, Riyadh, Saudi Arabia.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors would like to thank the Security Engineering Lab members at Prince Sultan University for their technical support.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

NCA	National Cybersecurity Authority
ECC	Essential cybersecurity controls
SAMA	Saudi Arabian Monetary Authority

References

1. Li, Y.; Liu, Q. A comprehensive review study of cyberattacks and cyber security; Emerging trends and recent developments. *Energy Rep.* **2021**, *7*, 8176–8186. [CrossRef]
2. He, W.; Zhang, Z.J.; Li, W. Information technology solutions, challenges, and suggestions for tackling the COVID-19 pandemic. *Int. J. Inf. Manag.* **2021**, *57*, 102287. [CrossRef] [PubMed]
3. AlDaajeh, S.; Saleous, H.; Alrabaee, S.; Barka, E.; Breitinger, F.; Raymond Choo, K.K. The role of national cybersecurity strategies on the improvement of cybersecurity education. *Comput. Secur.* **2022**, *119*, 102754. [CrossRef]
4. Dalal, R.S.; Howard, D.J.; Bennett, R.J.; Posey, C.; Zaccaro, S.J.; Brummel, B.J. Organizational science and cybersecurity: Abundant opportunities for research at the interface. *J. Bus. Psychol.* **2021**, *37*, 1–29. [CrossRef]

5. Perera, S.; Jin, X.; Maurushat, A.; Opoku, D.G.J. Factors Affecting Reputational Damage to Organisations Due to Cyberattacks. *Informatics* **2022**, *9*, 28. [CrossRef]
6. Fathi, S.; Hikal, N. A Review of Cyber-security Measuring and Assessment Methods for Modern Enterprises. *JOIV Int. J. Inform. Vis.* **2019**, *3*, 157–172. [CrossRef]
7. Bailey, T.; Greis, J.; Watters, M.; Welle, J. Cybersecurity Legislation: Preparing for Increased Reporting and Transparency. 2022. Available online: https://www.mckinsey.com/capabilities/risk-and-resilience/ourinsights/cybersecurity/cybersecurity-legislation-preparing-for-increased-reporting-and-transparency (accessedon 26 July 2022).
8. ISO/IEC 27001:2013; Information Technology—Security Techniques—Information Security Management Systems—Requirements, The International Organization for Standardization (ISO): Geneva, Switzerland, 2013.
9. Almuhammadi, S.; Alsaleh, M. Information Security Maturity Model for Nist Cyber Security Framework. In Proceedings of the Sixth International Conference on Information Technology Convergence and Services. Academy and Industry Research Collaboration Center (AIRCC), Sydney, Australia, 25–26 February 2017; pp. 51–62. [CrossRef]
10. Lee, Y.C. Financial Sector's Cybersecurity. 2021. Available online: https://docslib.org/doc/12762763/financial-sectors-cybersecurity-a-regulatory-digest (accessed on 20 September 2020).
11. Almudaires, F.; Rahman, M.H.; Almudaires, M. An Overview of Cybersecurity, Data Size and Cloud Computing in light of Saudi Arabia 2030 Vision. In Proceedings of the 2021 International Conference on Information Technology (ICIT), Amman, Jordan, 14–15 July 2021; pp. 268–273.
12. NCA. Global Cybersecurity Index 2020—International Telecommunication Union. 2020. Available online: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf (accessed on 20 February 2023).
13. NCA. Essential Cybersecurity Controls (ECC-1: 2018). 2018. Available online: https://nca.gov.sa/files/ecc-en.pdf (accessed on 20 July 2022).
14. von der Heyde, M.; Gerl, A.; Seck, R.; Groß, R.; Watkowski, L. Applying COBIT 2019 to IT Governance in Higher Education—Establishing IT governance for the collaboration of all universities and universities of applied sciences in Bavaria. In Proceedings of the Conference: INFORMATIK 2020, Karlsruhe, Germany, 2 October 2021. [CrossRef]
15. Corallo, A.; Lazoi, M.; Lezzi, M.; Luperto, A. Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review. *Comput. Ind.* **2022**, *137*, 103614. [CrossRef]
16. Asaithambi, S.; Ravi, L.; Kotb, H.; Milyani, A.H.; Azhari, A.A.; Nallusamy, S.; Varadarajan, V.; Vairavasundaram, S. An Energy-Efficient and Blockchain-Integrated Software Defined Network for the Industrial Internet of Things. *Sensors* **2022**, *22*, 7917. [CrossRef]
17. Sarabdeen, J.; Chikhaoui, E.; Ishak, M.M.M. Creating standards for Canadian health data protection during health emergency—An analysis of privacy regulations and laws. *Heliyon* **2022**, *8*, e09458. [CrossRef]
18. Aliyu, A.; Maglaras, L.; He, Y.; Yevseyeva, I.; Boiten, E.; Cook, A.; Janicke, H. A holistic cybersecurity maturity assessment framework for higher education institutions in the United Kingdom. *Appl. Sci.* **2020**, *10*, 3660. [CrossRef]
19. Zarour, M.; Alhammad, N.; Alenezi, M.; Alsarayrah, K. A Research on DevOps Maturity Models. *Int. J. Recent Technol. Eng.* **2019**, *8*, 4854–4862. [CrossRef]
20. Proença, D.; Borbinha, J. Information security management systems—A maturity model based on ISO/IEC 27001. In *Proceedings of the Lecture Notes in Business Information Processing*; Springer: Berlin/Heidelberg, Germany, 2018; Volume 320, pp. 102–114. [CrossRef]
21. Bolanio, J.B.; Paredes, R.K.; Yoldan, A.L., Jr.; Acapulco, R.E., II. Network Security Policy for Higher Education Institutions based on ISO Standards. *Mediterr. J. Basic Appl. Sci.* **2021**, *5*, 1–17. [CrossRef]
22. ISO/IEC 27033-1:2010;Information Technology—Security Techniques—Network Security—Part 1: Overview and Concepts. The International Organization for Standardization (ISO): Geneva, Switzerland, 2010.
23. Makupi, D.; Masese, N. Determining Information Security Maturity Level of an organization based on ISO 27001. *Int. J. Comput. Sci. Eng.* **2019**, *6*, 5–11. [CrossRef]
24. Yaokumah, W.; Dawson, A.A. *Network and Data Transfer Security Management in Higher Educational Institutions*; IGI Global: Hershey, PA, USA, 2019; pp. 1–19.
25. ISO/IEC 21827:2008; Information Technology—Security Techniques–Systems Security Engineering—Capability Maturity Model (SSE-CMM). The International Organization for Standardization (ISO): Geneva, Switzerland, 2008.
26. Mantra, I.; Rahman, A.A.; Saragih, H. Maturity Framework Analysis ISO 27001: 2013 on Indonesian Higher Education. *Int. J. Eng. Technol.* **2020**, *9*, 429–436. [CrossRef]
27. Tejay, G.; Goel, S. Editorial: Time to move away from compliance—Cybersecurity in the context of needs and investments of organizations. *Organ. Cybersecur. J. Pract. Process. People* **2022**, *2*, 1–2. [CrossRef]
28. Mijwil, M.; Filali, Y.; Aljanabi, M.; Bounabi, M.; Al-Shahwani, H.; ChatGPT. The Purpose of Cybersecurity Governance in the Digital Transformation of Public Services and Protecting the Digital Environment. *Mesopotamian J. Cybersecur.* **2023**, *2023*, 2–4.
29. Suwito, M.H.; Matsumoto, S.; Kawamoto, J.; Gollmann, D.; Sakurai, K. An analysis of IT assessment security maturity in higher education institution. In *Proceedings of the Information Science and Applications (ICISA) 2016*; Springer: Berlin/Heidelberg, Germany, 2016; Volume 376, pp. 701–713. [CrossRef]
30. Hung, C.; Hwang, M.; Liu, Y. Building a Maturity Model of Information Security Governance for Technological Colleges and Universities in Taiwan. *Appl. Mech. Mater.* **2013**, *284–287*, 3657–3661. [CrossRef]

31. Bass, J.M. An Early-Stage ICT Maturity Model derived from Ethiopian education institutions. *Int. J. Educ. Dev. Using Inf. Commun. Technol. IJEDICT* **2011**, *7*, 5–25.
32. Ismail, Z.; Masrom, M.; Sidek, Z.; Hamzah, D. Framework to Manage Information Security for Malaysian Academic Environment. *J. Inf. Assur. Cybersecur.* **2010**, 2010, 1–16.
33. Dehlawi, Z.; Abokhodair, N. Saudi Arabia's response to cyber conflict: A case study of the Shamoon malware incident. In Proceedings of the 2013 IEEE International Conference on Intelligence and Security Informatics, Seattle, WA, USA, 4–7 June 2013; pp. 73–75. [CrossRef]
34. Saudi GAZETTE Report. King Orders Setting Up of National Cyber Security Authority. 2017. Available online: https://saudigazette.com.sa/article/520782/SAUDI-ARABIA/King-orders-setting-up-of-National-Cyber-Security-Authority (accessed on 26 August 2022).
35. CITC. Cybersecurity Regulatory Framework. 2020. Available online: https://www.citc.gov.sa/en/RulesandSystems/CyberSecurity/Documents/CRF-en.pdf (accessed on 20 August 2022).
36. SAMA. Cyber Security Framework Saudi Arabian Monetary Authority. 2017. Available online: https://www.sama.gov.sa/enUS/Laws/BankingRules/SAMA20Cyber/20Security/20Framework.pdf (accessed on 20 July 2022).
37. Hamed, T.A.; Alenezi, M. Business Continuity Management & Disaster Recovery Capabilities in Saudi Arabia ICT Businesses. *Int. J. Hybrid Inf. Technol.* **2016**, *9*, 99–126. [CrossRef]
38. Nurunnabi, M. IFRS and Saudi accounting standards: A critical investigation. *Int. J. Discl. Gov.* **2017**, *14*, 4854–4862. [CrossRef]
39. Ajmi, L.; Hadeel; Alqahtani, N.; Rahman, A.U.; Mahmud, M. A Novel Cybersecurity Framework for Countermeasure of SME's in Saudi Arabia. In Proceedings of the 2nd International Conference on Computer Applications and Information Security, ICCAIS 2019, Riyadh, Saudi Arabia, 1–3 May 2019. [CrossRef]
40. Alsahafi, T.; Halboob, W.; Almuhtadi, J. Compliance with Saudi NCA-ECC based on ISO/IEC 27001. *Tech. Gaz.* **2022**, *29*, 2090–2097. [CrossRef]
41. Almomani, I.; Ahmed, M.; Maglaras, L. Cybersecurity maturity assessment framework for higher education institutions in Saudi Arabia. *PeerJ Comput. Sci.* **2021**, *7*, e703. [CrossRef] [PubMed]
42. Singh, H.P.; Alshammari, T.S. An Institutional Theory Perspective on Developing a Cyber Security Legal Framework: A Case of Saudi Arabia. *Beijing Law Rev.* **2020**, *11*, 637–650. [CrossRef]
43. NCA ECC-1:2018 Assessment and Compliance Tool. Available online: https://nca.gov.sa/legislation?item=176&slug=controls-list (accessed on 20 July 2022).