ISSN 1330-3651 (Print), ISSN 1848-6339 (Online) https://doi.org/10.17559/TV-20220307162849
Preliminary communication

# Compliance with Saudi NCA-ECC based on ISO/IEC 27001

Tahani ALSAHAFI, Waleed HALBOOB*, Jalal ALMUHTADI

**Abstract:** Organizations are required to implement an information security management system (ISMS) for making a central cybersecurity framework, reducing costs, treating risks, and so on. Several ISMS standards have been issued and implemented locally and internationally. In Saudi Arabia, the most widely implemented international ISMS is ISO/IEC 27001. Currently, the Saudi National Cybersecurity Authority (NCA) issued a local framework called Essential Cybersecurity Controls (NCA-ECC). Therefore, many ISO/IEC 27001 certified organizations in Saudi Arabia are trying to convert from ISO/IEC 27001 to NCA-ECC or comply with both frameworks. Nevertheless, cybersecurity experts need to know which cybersecurity controls are already implemented, based on the ISO/IEC 27001, and which are not. This paper first measures the extent to which certified ISO/IEC 27001 Saudi organizations comply with the NCA-ECC. Second, it presents a framework for complying with the required unimplemented or partially implemented NCA-ECC controls. The framework can also help organization to be in compliance with both frameworks, if required. Three ISO/IEC 27001-certified Saudi public universities are selected as samples. The data is collected by interviewing the cybersecurity officers in the selected universities. This research shows that certified ISO/IEC 27001 organizations are approximately 64% in compliance with the NCA-ECC. The presented framework can help any ISO/IEC 27001 certified Saudi organization convert from ISO/IEC 27001 to NCA-ECC in a quick and cost-effective manner by considering only NCA-ECC nonconformities.

**Keywords:** compliance; digital forensics; essential cybersecurity controls (ECC); governance; incident response; information security management system (ISMS); ISO/IEC 27001; risk management

## 1 INTRODUCTION

Protection of information and communications technologies (ICTs) is one of the most important issues of the times, where the success of any organization depends on the information and services it owns and provides, respectively. Assets (hardware, software, documents, staff, etc.) that store information or process the e-services are continuously at risk [1, 2]. Therefore, each organization needs to implement an information security management system (ISMS), such as ISO / IEC 27001 [3], to reduce the risks to its information assets.

For example, colleges, universities, and academic institutions are widely relying on ICTs to store their information and provide several offline/online systems and e-services to their staff, students, etc. As a result, the likelihood of cyber risks from intentional and unintentional acts such as intrusions, attacks, negligence, lack of awareness, and cognitive impairment is increasing overtime. The academic institutions are targeted by cyber-attackers for several reasons, such as possessing intellectual content, accessing unpublished research, using data from a large number of students, etc. According to Hearn [4], about 87 percent of colleges and universities have been attacked by outsiders. This does not include attacks and policy volitions launched by insiders (staff and students).

Organizations must treat cyber security risks to their information assets using a specific information security management system (ISMS) standard or framework. This provides several benefits, such as having a central cybersecurity framework for managing all cybersecurity domains, e.g., technology, people, and process; protection of all information assets; confidentiality, integrity, and availability of security services; resilience against cyber attacks and natural disasters; and improvement of the awareness and culture of the staff [5, 6].

In Saudi Arabia, organizations mostly implement ISO IEC 27001 for managing cybersecurity aspects. For example, most Saudi universities are already ISO/IEC 27001 certified. But now they must also implement the local ISMS, called essential cybersecurity controls or NCA-ECC [7], to comply with government regulations. In fact, all public organizations in Saudi Arabia must comply with NCA-ECC and base on their ISO/IEC 27001, if it is already implemented. It is not clear now to what extent they are in compliance with the NCA-ECC based on their implemented ISO/IEC 27001. Moreover, some organizations choose to implement both frameworks, and they need to know which controls are not implemented (or at least partially implemented) based on ISO/IEC 27001. In other words, there is a need to understand what exactly to do to be in compliance with both frameworks. According to Tofan [5], the implementation of more than one management system can lead to several conflicting issues.

This paper investigates the issue of converting from ISO/IEC 27001 to the NCA-ECC. The first goal is to measure the compliance level with NCA-ECC based on the ISO/IEC 27001. The second is to propose a framework to govern the unimplemented and partially-implemented NCA-ECC's controls. Such a framework can assist Saudi ISO/IEC 27001-certified organizations in implementing the NCA-ECC framework in a quick and efficient manner. In addition, this research can help in addressing any conflicted issues arise during implementing both cybersecurity frameworks.

The data is collected from three public universities, which are selected as samples, and their cybersecurity officers are interviewed. The names of these universities are anonymous here for security purposes. All are IS0/IEC 27001-certified and well known as three of the top ten Saudi public universities. Their implemented ISMS, based on ISO/IEC 27001, is studied to measure the compliance level with NCA-ECC.

The outline of this paper starts with reviewing the related works in Section 2, followed, in Section 3, by introducing the ISMS concepts along with presenting the ISO/IEC 27001 and NCA-ECC frameworks in more detail. The compliance assessment of the three selected universities, with NCA-ECC and based on the ISO/IEC 27001 implementation, is presented in Section 4. Then, a conversation analysis from ISO/IEC 27001 to NCA-ECC

is presented in Section 5. Section 6 introduces the suggested mapping framework. In Section 7, the conclusion and future works are presented.

## 2 RELATED WORKS

Until now, there has been no research proposed in the literature that studies the relation between ISO / IEC 27001 and NCA-ECC. But, several studies in the literature investigated cybersecurity issues in academic institutions in terms of ISMS. This section reviews these works with more focus on efforts to apply ISMSs to universities.

Modiri et al., [8] proposed a cybersecurity framework for guarding universities' online exams and introducing some new technical security designs to support the framework. The ISO/IEC 27001 standard is used as a baseline but several new controls are added to meet the online exam protection requirements. The new controls cover different domains such as access control, physical security, bring your own devices (BYOD), incident management, etc.

In 2002, Bamfleh [9] studied the cybersecurity status of the libraries of Umm Al-Qura University in Saudi Arabia. The author measured the ability of cybersecurity solutions applied to the library network and systems to identify the strengths and weaknesses and to determine how the cybersecurity solutions and procedures can be improved. The study suggested that the focus be on staff training, solutions updates, incident management, and awareness programs.

In 2013, Rehman et al. [10] provided a general cybersecurity framework for academic institutions in Pakistan. The study also presented some guidelines for more easily implementing the proposed framework.

Tiganoaia [11] studied the cybersecurity risks in university information assets based on the ISO/IEC 27001. Data were collected through questionnaires for staff and interviews with members of the executive committee. Research showed that the information assets stored user data and passwords are highly vulnerable compared to other information assets. It also found that poor security management (no backup, log file, monitoring, incident management, business continuity management, and reporting) leads to cybersecurity risks and disasters. The research also recommends several cybersecurity management solutions which can, if used, lead to improving the cybersecurity status of public colleges and universities.

Al-Shetty [12] presented a study to evaluate the information security and privacy policies of academic institutions in Saudi Arabia, and concentrated on Qassim University as an example. The study concluded that awareness and training programs along with the implementation of well-known cybersecurity controls are extremely important.

Itradat et al. [13] evaluated the cybersecurity level of the Jordanian universities by choosing the Hashemite University (HU) as a case study. They focused on analyzing the risks (organizational and technical) to the information systems and services used by the Hashemite University (HU) by adopting two main assessment techniques, namely vulnerability assessment and penetration testing. The evaluation process is performed according to the ISO/IEC 27001:2005 standard [3].

Mumtaz [14] discussed the effect of applying the asset management concept in improving the cybersecurity systems of public universities of Pakistan. The researcher visited several universities, observed the status of cybersecurity practices, and collected more data using a distributed survey. Finally, the researcher suggested having an assets management policy along with other controls in place to ensure assets management in the targeted universities.

In a study conducted by Al-Bakri [15], the cybersecurity of the libraries in Nile and Nile Valley universities, in Sudan, is assessed. The researcher used the historical method, by looking at the published literature related to the subject under study, and observing the security status based on several cybersecurity controls.

Al-Omairi and Al-Saleme [16] explained the reality of cybersecurity practices in the main library of Sultan Qaboos University, and its compatibility with ISO/IEC 27001. Their study collects data via field visits, interviews, observations (tracking documents and websites), and audit forms (so-called audit assessment forms or sheets). It showed that most of the cybersecurity practices in the main library are in conformity with the best practices of ISO/IEC 27001. Furthermore, the highest level of compliance is in human resource cybersecurity controls (100%), followed by physical security controls (94.4%) and then technology security controls (90.5%). The study came up with a set of recommendations, the most important of which are: the need to continue training and awareness of staff; work to develop cybersecurity policies based on the ISO/IEC 27001; manage the backup of systems and software in a safe building outside the library; and finally provide an alternative source of energy for computer equipment in the event of power failure.

Hissi et al., [17] designed a cybersecurity governance model to secure the scientific research data and systems in universities in Morocco. The designed model is proposed based on three different standards, specifically COBIT, ISO/IEC 27001, and ISO/IEC 38500. The proposed model governs the relevant data and information systems while taking into account the national context of the Moroccan universities. The suggested model supports three levels of cybersecurity governance, namely, the top, executive, and operational management levels.

Almomani et al. [18] proposed a framework, called SCMAF, for evaluating higher education institutes in Saudi Arabia in terms of cybersecurity. The suggested framework can be used as a self-assessment tool to identify the level and weaknesses as well as to guide the implementation migration plan.

## 3 ISMS: AN OVERVIEW

The importance of protecting information from any leakage, modification, or disruption, while protecting the media used to store, process, and transmit it, has led to the use of several technical security solutions. But, these solutions are not sufficient since the security is a continuous process, not a product. In the other words, there is no final security solution even if it is a comprehensive one to treat all risks. Therefore, there is a need to consider

all cybersecurity aspects (namely technology, processes, people, etc.) and manage all controls such as authentication, encryption, incident management, digital forensics, staff awareness and training, business continuity, etc.

As a consequence, having several ISMSs are issues being discussed by international bodies and government agencies. An ISMS can be defined as a set of policies, and procedures that define security controls - called also requirements. These policies and procedures are interrelated, and coordinated [19]. Once defined, they need to be implemented. In the end, the whole process is audited at least once a year.

To manage an ISMS task and to achieve best security practices, an organization must identify the targeted ISMS first. The following sub-sections discuss the most well-known and implemented international and local ISMSs in Saudi Arabia.

### 3.1 International ISMSs

Many organizations around the world are seeking to implement international standards for managing cybersecurity. The most internationally recognized cybersecurity standards or ISMSs are [3, 20]:

- ISO/IEC 27001: It is part of the ISO 27000 series of standards issued by the International Organization for Standardization (ISO), and it can be implemented by both public and private organizations in any country.
- Best Practice Standard: Published by the Information Security Forum in 1992, covering best practices in cybersecurity, but it is less well-known than the ISO/IEC 27001.
- Payment Card Industry-Data Security Standard (PCI-DSS): A standard used by financial organizations, such as banks, to protect credit card data, online payments, client data, etc.

As discussed earlier, the most well-known and implemented international standard is ISO / IEC 27001 [3], which specifies several requirements (called clauses) that must be documented and implemented to ensure the organization to be certified in the ISO/IEC 27001. These clauses are categorized into ten main ones which are scope, normative references, terms and conditions, context of the organization establishment, leadership, planning, support, operation, performance evaluation, and improvements requirements. The sub-clauses will be listed and discussed in the next section.

ISO/IEC 27000 serious includes ISO/IEC 27002 which identifies the security controls. However, also in ISO/IEC 27001 standard an annex (called Annex A) is provided to list all security controls. These controls are in fact taken from the ISO/IEC 27002 standard.

### 3.2 Saudi Arabia ISMSs

In Saudi Arabia, the following cybersecurity standards have been issued so far [7, 21]:

- SAMA Cybersecurity Framework: Issued by the Saudi Arabian Monetary Authority (SAMA) and applied to all financial organizations in the Kingdom.
- Essential Cybersecurity Controls (NCA-ECC): Issued in October 2018, by National Cybersecurity Authority (NCA) to be implemented by all public organizations and private ones that provide services, specifically IT services, to the public ones. The authority also issued another standard for critical systems, which is outside the scope of this research.

The NCA-ECC controls are distributed into five main domains, which are:

- Cybersecurity Governance.
- Cybersecurity Defence.
- Cybersecurity Resilience.
- Third-party and cloud computing security.
- Cybersecurity of industrial control systems.

The above five domains have 29 main controls, which then have 114 sub-controls. However, these main domains will be listed in the next section.

Compared to ISO/IEC 27001: 2013, the NCA-ECC combines requirements and controls. In ISO/IEC 27000 serious, the requirements are defined in ISO/IEC 27001 while the controls are specified in ISO/IEC 27002. However, the ISO/IEC 27001: 2013 document refers to the list of controls (described in ISO/IEC 27002) in an annex (called Annex A), as mentioned earlier. Also, unlike ISO/IEC 27001 which focus only on three cybersecurity pillars (people, process, and technology), NCA-ECC focus also on the strategy as a fourth pillar. Many of the differences between these two standards will be discussed in this paper successively when the compliance assessment and framework are presented.

## 4 COMPLIANCE WITH NCA-ECCBASED ON ISO/IEC 27001

This section studies the compliance of the three universities with NCA-ECC based on their implemented ISO/IEC 27001 standard. The names of these universities are kept private here. For the interview, all ISO/IEC 27001 clauses, and their sub-clauses, are listed in an interview table and their data are collected based on answers to questions. Finally, the interview questions for each clause are prepared and written in the same interview table. The entire interview table cannot be presented here due to the limited space provided. Instead, the result of only the main clauses and its immediate sub-clauses is presented. The interviews are made with cybersecurity officers in all three universities. The answer to each control can be one of the following three statuses:

- Implemented: The clause is completely documented and implemented.
- Partially implemented: The clause is not documented or implemented. For instance, it can be documented but not implemented. Another reason the clause can have many sub-clauses, and only some of them are documented and/or implemented.
- Not implemented: The clause and its sub-clauses are not documented and implemented at all.
- Non-applicable: The clause is not applicable to the specific organization.

**Table 1** Compliance with ISO/IEC 27001

| No. | Main clauses title (number) | Sub-clauses title (number) | Samples (universities) | | |
|---|---|---|---|---|---|
| | | | U1 | U2 | U3 |
| 1 | Context of the Organization (4) | Understanding the organization and its context (4.1) | Y | Y | Y |
| 2 | | Understanding the needs and expectations of interested parties (4.2) | Y | Y | Y |
| 3 | | Determining the scope of the information security management system (4.3) | Y | Y | Y |
| 4 | | Information security management system (4.4) | Y | Y | Y |
| 5 | Leadership (5) | Leadership and commitment (5.1) | Y | Y | Y |
| 6 | | Security Policy (5.2) | Y | Y | Y |
| 7 | | Organizational roles, responsibilities and authorities (5.3) | Y | Y | Y |
| 8 | Planning (6) | Actions to address risks and opportunities (6.1) | Y | Y | Y |
| 9 | | Information security objectives and plans to achieve them (6.2) | Y | p | Y |
| 10 | Support (7) | Resources (7.1) | Y | Y | Y |
| 11 | | Competence (7.2) | Y | Y | Y |
| 12 | | Awareness (7.3) | P | P | P |
| 13 | | Communication (7.4) | Y | Y | Y |
| 14 | | Documented information (7.5) | Y | Y | Y |
| 15 | Operation(8) | Operational planning and control (8.1) | Y | Y | Y |
| 16 | | Information security risk assessment (8.2) | Y | Y | Y |
| 17 | | Information security risk treatment (8.3) | Y | Y | Y |
| 18 | Performance evaluation (9) | Monitoring, measurement, analysis and evaluation (9.1) | Y | Y | Y |
| 19 | | Internal audit (9.2) | Y | Y | P |
| 20 | | Management review (9.3) | Y | Y | Y |
| 21 | Improvement (10) | Nonconformity and corrective action (10.1) | Y | Y | Y |
| 22 | | Continual improvement (10.2) | Y | P | N |

Notes: • Y: Implemented • N: Not implemented • P: Partially implemented

**Table 2** Compliance with the NCA-ECC based on the ISO/IEC 27001

| No. | Main NCA-ECC controls | Sub NCA-ECC controls | Matched ISO/IEC 27001 clauses title (number) | Samples (universities) | | |
|---|---|---|---|---|---|---|
| | | | | U1 | U2 | U3 |
| 1 | Cybersecurity Governance | Cybersecurity strategy | Information security objectives and plans to achieve them (6.2) | N | N | N |
| 2 | | Cybersecurity management | Leadership and commitment (5.1) | Y | N | P |
| 3 | | Cybersecurity policies & procedures | Information security management system (4.4) | Y | Y | Y |
| 4 | | Cybersecurity roles and responsibilities | Organizational roles, responsibilities and authorities (5.3) | Y | Y | Y |
| 5 | | Cybersecurity risk management | Information security risk assessment (8.2) and Information security risk treatment (8.3) | Y | Y | Y |
| 6 | | Cybersecurity in information technology projects | Information security in project management (A.6.1.5) | N | N | N |
| 7 | | Cybersecurity regulatory compliance | Understanding the needs and expectations of interested parties (4.2) | Y | Y | Y |
| 8 | | Cybersecurity periodical assessment and audit | Internal audit (9.2) | Y | Y | Y |
| 9 | | Cybersecurity in human resources | Humen resources security (A7) | Y | Y | Y |
| 10 | | Cybersecurity awareness and training program | Competence (7.2), and awareness (7.3) | Y | Y | Y |
| 11 | Cybersecurity Defense | Asset management | Access management (A.8) | Y | Y | Y |
| 12 | | Identity and access management | Access control (A.9) | | | |
| 13 | | Information system and processing facilities protection | Operation security (A.12), and avalaibility of information processing facilities (A.17.2.1) | Y | Y | Y |
| 14 | | E mail protection | Communication security (A.13) | Y | Y | Y |
| 15 | | Networks security management | Communication security (A.13) | Y | Y | Y |
| 16 | | Mobile devices security | Mobile device policy (A.6.2.1) and comunication security (A.13) | P | P | P |
| 17 | | Data and information protection | Cryprography (A.10) | Y | Y | Y |
| 18 | | Cryptography | Cryprography (A.10) | Y | Y | Y |
| 19 | | Backup and recovery management | Backup (A.12.3) | P | P | P |
| 20 | | Vulnerabilities management | Tecnicial vulnrability management (A.12.6) | Y | Y | Y |
| 21 | | Penetration testing | Tecnicial vulnrability management (A.12.6) | Y | Y | Y |
| 22 | | Cybersecurity event logs and monitoring management | Logging and monitoring (A.12.3) | Y | Y | Y |
| 23 | | cybersecurity incident and threat management | Information security incident management (A.16) | Y | Y | Y |
| 24 | | Physical security | Physical and enviromental security (A.11) | Y | Y | Y |
| 25 | | Web application security | Security in develpment and support process (A.14.2) | Y | Y | Y |
| 26 | Cybersecurity Resilience | Business continuity | Information security aspects of bussiness contunity management (A.17) | Y | Y | Y |
| 27 | Third-party and cloud computing security | 3rd parties | Understanding the needs and expectations of interested parties (4.2) | Y | Y | Y |
| 28 | | Cloud computing | Understanding the needs and expectations of interested parties (4.2) | Y | Y | Y |
| 29 | Cybersecurity of industrial control systems | Cybersecurity of Industrial Control Systems | Not Required | N/A | N/A | N/A |

Notes: • Y: Implemented • N: Not implemented • P: Partially implemented • N/A: Not applicable

Tab. 1 shows the result of data collection and analysis. In other words, the result of assessing the three universities in terms of their compliance with ISO/IEC 27001. However, the names of all universities are ignored and U1, U2, and U3 samples are used instead. All universities are ISO/IEC 27001-certified. But and in general, there is a need for implementing stronger awareness programs. Awareness programs in universities help not only protect university information assets, but also provide students and researchers with a greater awareness of cybersecurity, which can help improve it wherever they work. At the time of this writing, the cybersecurity awareness in the interviewed universities relies only on regular email messages sent to faculty, staff, and students. There are no scheduled awareness training sessions. Secondly, the continual improvement of such ISMSs in all universities is not taken seriously. For example, one university did not recertify itself after the first year of certification process. Therefore, in terms of ISO/IEC 27001, all universities are already certified and are already in compliance with most of the requirements, except for security awareness and continual improvement, which require more efforts.Tab. 2 shows the extent to which ISO / IEC 27001 certified universities are in compliance with NCA-ECC. The three universities are assessed based on the NCA-ECC controls (called clauses in the ISO/IEC 27001). The assessment process uses the NCA's assessment tool [22] and covers all domains along with their main controls and sub-controls. However, due to the limited space provided here, only the results of the main controls (total 29 controls) are discussed. Based on the result presented in Tab. 2, it is clear that implementing the ISO/IEC 27001 standard is not sufficient to be in compliance with the NCA-ECC as many main controls are only partially implemented or not implemented at all. Fig. 1 shows that among 29 main controls, only 12 (41%) main controls are implemented, 13 partially implemented (45%), 3 not implemented, and finally (4%) are not applicable for universities. It can be concluded that the ISO/IEC 27001-certified organizations are only 64 present (as 41% controls are totally implemented and 45% controls are partially implemented, counted as 23%, so 64% on average) in compliance with the NCA-ECC.

## 5 CONVERTING FROM ISO/ECC 27001 NCA-ECC: ANALYSIS

For developing the converting framework, the results of implementing the ISO/IEC 27001 clauses (listed in Tab. 1) are discussed and linked to their relevant controls, if any, in the NCA-ECC.

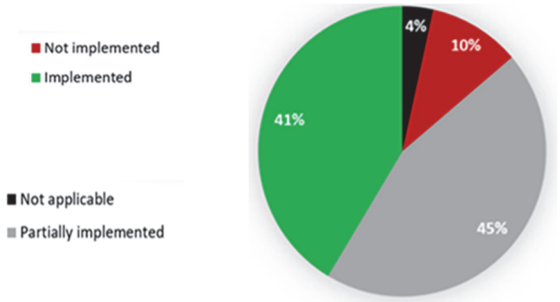


**Figure 1** Compliance with the NCA-ECC based on the ISO/IEC 27001

### 5.1 Clauses Mapping

First, for implementing the ISO/IEC 27001 standard, a document called ISMS manual is prepared. This document lists all clauses and highlights how they are implemented briefly inside the ISMS manual or, mostly, by referring to another document (e.g., policy, procedure, record, etc.) for details. However, having such manual is not required when implementing the NCA-ECC framework. The clauses 0 (introduction) just introduce the standard and its implementation within an organization, and such introduction cannot be reused while implementing the NCA-ECC framework.

Clause 1 (scope) sets the purpose of implementing the ISO/IEC 27001 standard, the type of organization, and finally in which departments in the organization the standard is implemented. Based on our study, all investigated three universities apply the ISO/IEC 27001 standard to their IT department/deanship only. Most public and private organizations do the same to reduce implementation cost (in terms of staff, resources, and time). All three universities refer in their ISMS manual to a document called ISMS scope to explain in more detail the scope of implementing the ISO/IEC 27001 standard. To be more specific, the ISMS scope document explains the departments that are managed by the standards, the description and organizational chart of these departments, geographical locations, relevant third parties, personnel included in the scope, etc. However, the scope of applying the NCA-ECC is for all of an organization and the cybersecurity team cannot exclude any department. So, there is no need for identifying the scope at all. Therefore, the ISO/IEC 27001 scope document is not helpful here and never assists in addressing any NCA-ECC controls.

The clause 2 (normative references) refers to the related ISO documents (namely ISO/IEC 27001 and 2700) inside the ISMS manual. Finally, clause 3 (terms and definitions) requires listing or referring to the terms used in the implemented ISMS. Like clause 2, the clause 3 is also documented inside the ISMS manual and not required by the NCA-ECC framework.

It can be concluded that the ISO/IEC 27001 first four clauses (0 - 3) are not useful for implementing the NCA-ECC framework. The other clauses are discussed in details in the next sub-sections.

### 5.2 Clauses 4 (Context of the Organization)

This clause requires documenting several ISO/IEC 27001 requirements, whereas all of them are required during implementing the NCA-ECC frameworks but in a different manner. Tab. 3 shows these requirements and how and where they can be applied in the NCA-ECC framework.

### 5.3 Clauses 6 (Planning)

This clause has two main sub-clauses, which are: actions to address risks and opportunities; and Information security objectives and planning to achieve them. For the first sub-clause, the organization has to develop a risk management policy, and procedures along with a risk management sheet. The sheet must be used to identify,

asset, evaluate, and treat all risks associated with information assets. The same risk management policy, procedure, and sheet can be used in the NCA-ECC framework with the following new sub-controls:

- The risk management process needs to be re-executed in many cases, e.g., delivering new services, major changes in the IT infrastructure, and contacting new third parts.
- The risk management process needs to be reexecuted at least every six months, unlike the ISO/IEC 27001 in which reexecuting the risk management process every year is an acceptable procedure.

**Table 3** Mapping the context of the organization

| No. | ISO/IEC 27001 clauses | ISO/IEC 27001 implementation | Relevant NCA-ECC implementation |
|---|---|---|---|
| 1 | Clause 4.1 (Understanding the Organization and its context) | Determine the internal and external issues that are relevant to the ISMS | Not mandatory but they can also be determined inside the cybersecurity strategy as challenges. |
| 2 | Clause 4.2 (Understanding the needs and expectations of interested parties) | Th expectation of the internal and external parties including the Legal & regulatory requirements | Not required in the NCA-ECC but it is better to list all 3rd parties in the risk assesemnt sheet as well as treat the risks associtaed with them. |
| 3 | Clause 4.3 (Determining the scope of the information security management system) | Here, ISMS objectives and boundaries are identified. The objectives must be supported by action plans. The boundaries mean listing all exclusive clauses that are not applicable. | The objectives are identified inside the cybersecurity strategy and need to be supported with initiatives, projects, and budgets. The exclusive controls are marked inside the NCA assessment tool, which is used normally for assessing and auditing the progress. |
| 4 | Clause 4.4 (Information security management system) | Confirming, in a statement inside the ISMS manual, the implementation, monitoring, and improving the ISMS. | The organization must implement, monitor, and improve its compliance with the NCA-ECC. |

### 5.4 Clauses 7 (Support)

This clause has five sub-clauses, practical resources, competence, awareness, communication, and documented information. Tab. 4 presents how this clause can be mapped to the implementation of the NCA-ECC.

**Table 4** Mapping the support clause implementation into the NCA-ECC

| No | ISO/IEC 27001 clauses | ISO/IEC 27001 implementation | Relevant NCA-ECC implementation |
|---|---|---|---|
| 1 | Clause 5.1 (Leadership and commitment) | The commitment of the top management is documented in a management review procedure. | Many main controls must be reviewed periodically. The ISO/IEC 27001 management review procedure can be used. |
| 2 | Clause 5.2 (Policy) | A general policy must be documented, approved, and communicated. | A policy called cooperate cybersecurity policy is prepared as a main policy for all other policies. |
| 3 | Clause 5.3 (Organizational roles, responsibilities and authorities) | The roles and responsibilities are recorded in a document called the roles and responsibilities document. | Beside documenting the roles and responsibilities, you need also another document called cybersecurity steering committee regulating. |

### 5.5 Clauses 8 (Operation)

This clause is about executing the security controls that were documented while complying with the previous clauses. These security controls include solutions required for securing the organization's assets and based on the documented policies, procedures, and risk management. However, the controls listed in the ISO/IEC 27002 document are used for this purpose. But, with the NCA-ECC, the security controls are listed as sub-controls in each control. This means that the NCA-ECC did not provide a separate specification for security controls. For most NCA-ECC controls, the sub-controls have to be documented and then implemented. So, converting from the ISO/IEC 27001 to NCA-ECC requires analyzing all existing security policies and procedures to ensure that all NCA-ECC's sub-controls are documented, and implemented.

### 5.6 Clauses 8 (Performance Evaluation)

In ISO/IEC 27001, the organization must evaluate the performance and effectiveness of its ISMS. This is done through executing the following tasks:

- An internal audit process (every six months or annually) followed by an annual external audit executed by a certification body.
- Frequently, holding a management review meeting to evaluate the status of the ISO/IEC 27001.

With the NCA-ECC, the above processes can be followed with few changes such as the following:

- In terms of internal audit, it is mandatory to be executed every six months, the auditing plan is not mandatory, and the NCA assessment tool is the most preferred.
- For management review, most controls must be periodically reviewed by the cyber security steering committee. Falling to do that will lead to non-compliance with about 21 sub-controls over 114 sub-controls.

### 5.7 Clauses 9 (Improvements)

In the ISO/IEC 27001, the organization must ensure the continued improvement of its ISMS through correcting all noncompliance found during the internal and external audits. The whole ISMS should be improved over time by targeting new objectives, applying more secure controls, etc. With the NCA-ECC, it is observed that the improvement is granted through auditing and targeting new

objectives in each new strategy. But the improvement in the NCA-ECC is widely measured and evaluated through several KPIs linked to the cybersecurity strategy.

## 6 THE FRAMEWORK

Fig. 2 summarizes the suggested framework. The framework steps are as follows:

1. Developing and implementing a cybersecurity strategy: The NCA-ECC requires a cybersecurity strategy that includes objectives, initiatives, projects, budgets, etc. The NCA website offers a template for cybersecurity strategies that can help Saudi organizations develop their strategies.
2. Cybersecurity Management: The NCA-ECC requires all Saudi organizations to establish a cybersecurity department separated from the IT department and linked directly to the top management.
3. Risk management: The NCA-ECC requires more sub-controls to ensure running the risk management process during launching new IT projects, delivering new e-services, changing the IT infrastructure, and contracting a new third party. Therefore, the execution of the risk management process in these four cases will ensure the compliance of the risk management process with the NCA-ECC requirements.
4. Cybersecurity in information technology projects: In ISO/IEC 27001, this control is not mandatory, but it must be implemented according to NCA-ECC by having a documented, approved, implemented and reviewed cybersecurity in technology projects policy and/or procedure.
5. Periodical assessment and audit: Periodical assessment and audit in the NCA-ECC must be executed every six months, while, in the ISO/IEC 27001, it can be executed annually. So, to meet the NCA-ECC requirements, the auditing process must be scheduled twice a year.
6. Email protection: A two-factor authentication (2FA) is required for authenticating email's users if accessed remotely.
7. National Cybersecurity Authority of Saudi Arabia. (2018). Essential cybersecurity controls (ECC 1: 2018). Available at https://nca.gov.sa/files/ecc-en.pdf (accessed 25 October 2021).
8. Cryptograph: The NCA-ECC also published a national cryptography standards document that defines some criteria for cryptography algorithms, systems, and protocols.
9. Event logs and monitoring management: Similarly, both standards require this control as an email protection control. However, in the ECC, a security information and event management (SIEM) solution must be used as well.
10. Incident response and digital forensics: With the ECC, all Saudi organizations have to comply with more controls compared to the ISO/IEC 27001. They need to register with the NCA and receive all security intelligence alerts, report any security incident to the NCA, and finally, their level of security in some aspects and in different times as directed by the NCA.

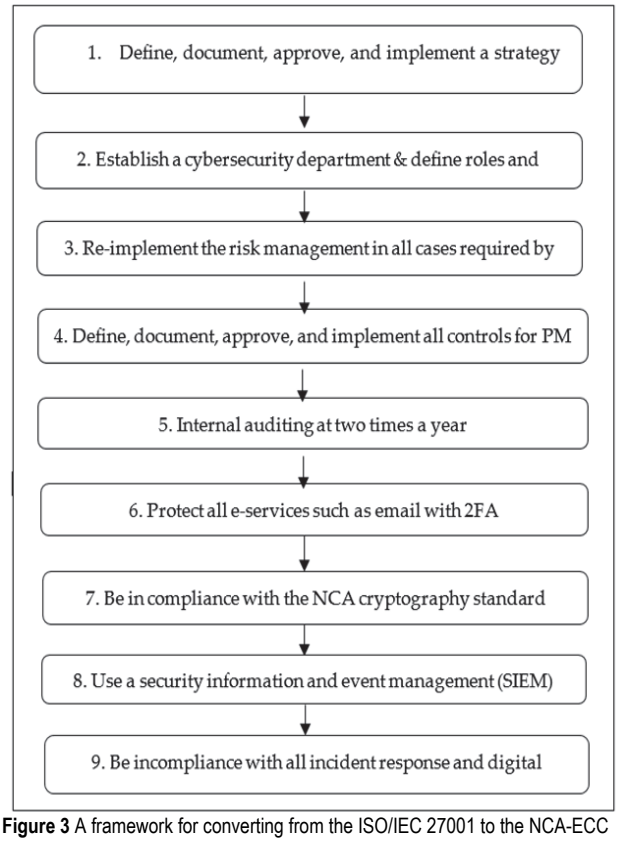


**Figure 3** A framework for converting from the ISO/IEC 27001 to the NCA-ECC

Another finding that is worth noting is that we typically found that the implementation of the ISO/IEC 27001 tends to be lenient and relaxed, since it is not a requirement for Saudi organizations, and some controls can be partially implemented or delayed to a later date, depending on management decision and risk acceptance. On the other hand, the NCA-ECC controls are implemented in a stricter fashion, with clearly less risk appetite, because the NCA-ECC is mandatory on all government sectors, including public universities.

## 7 CONCLUSIONS

This research paper investigates compliance of Saudi organizations with the NCA-ECC framework based on their ISO/IEC 27001 implementation. The study found that complying with ISO/IEC 27001 ensures only a partial compliance with the NCA-ECC. Three ISO/IEC 27001 certified Saudi public universities are chosen as samples and their NCA-ECC compliance is evaluated based on their ISO/IEC implementation. Then, all ISO/IEC 27001 clauses implemented are mapped with the relevant controls in the NCA-ECC. A framework for converting ISO/IEC 27001 to the NCA-ECC is presented. This framework can help not only universities but any Saudi organization in converting from the ISO/IEC 27001 to the NCA-ECC quickly and with less time and effort.

### Acknowledgements

The authors extend their appreciation to the Deanship of Scientific Research at King Saud University for funding this work through research group no (RG-1441-531).

The authors declare that they have no conflicts of interest.

## 8 REFERENCES


[1] Fernandez, A. & Garcia, D. F. (2016). Complex Vs. Simple Asset Modeling Approaches for Information Security Risk Assessment. Evaluation with MAGERIT Methodology. *6th International Conference on Innovative Computing Technology (INTECH)*. https://doi.org/10.1109/intech.2016.7845064

[2] Partheeban P. & Kavitha V. (2015). A Study with Security Concerns in Service Delivery Models of Cloud Computing. *Journal of Information Security Researc*h, *8*(4), 129-145.

[3] ISO/IEC 27001. (2013). https://www.iso.org/isoiec-27001-information-security.html

[4] Hearn, T. (2019). University Challenge: Cyber Attacks in Higher Education.

[5] Tofan, D. C. (2011). Information security standards. *Journal of Mobile, Embedded and Distributed Systems*, *3*(3), 128-135.

[6] Bourekkache, S., Kazar, O., & Aloui, A. (2019). Computer and Network Security: Ontological and Multi-agent System for Intrusion Detection. *Journal of digital information management*, *17*(3), 133-144.

[7] National Cybersecurity Authority of Saudi Arabia. 2018. Essential cybersecurity controls (ECC-1: 2018). https://nca.gov.sa/files/ecc-en.pdf.

[8] Modiri, N., Farahi, A., & Ketabi, S. (2011). Providing Security Framework for Holding Electronic Examinations in Virtual Universities. *7th International Conference on Networked Computing and Advanced Information Management*, Gyeongju, Korea (South), 73-79.

[9] Bamfleh, F. (2002). Information Security Protection in the Main Library of Om Al Qora University. *Future Directions in Libraries and Information*, *9*(18), 1-13.

[10] Rehman, H., Masood, A., & Cheema, A. R. (2013). Information Security Management in Academic Institutes of Pakistan. *2nd NCIA*, 47-51.

[11] Tiganoaia, B. (2013). Some Aspects Regarding the Information Security Management System within Organizations-Adopting the ISO/IEC 27001:2013 Standard. *Studies in Informatics and Control*, *24*(2), 201-210.

[12] Al- Shetty, E. (2014). Privacy Policies Evaluation in Saudi Arabia: Al-Qasim University as Case Study. *Egypt Information Journal*, *13*(14), 11-24.

[13] Itradat, S., Sulatn, M., Al-Junaidi, S., & Qaffaf, R. (2014). Developing an ISO27001 Information Security Management System for an Educational Institute: Hashemite University as a Case Study. *Jordan Journal of Mechanical & Industrial Engineering*, *8*(2), 102-118.

[14] Mumtaz, N. (2015). Analysis of Information Security Through Asset Management in Academic Institutes of Pakistan. *6th International Conference on Information and Communication Technologies (ICICT)*, 1-4.

[15] Al-bakri, Y. (2017). Information security in Sudan Public Universities. *23rd Annual Conference and Exhibition of Special Libraries Association/Arabian Gulf Chapter*, Manamah, Bahrain, 1-11.

[16] Al-Omeri, M. & Al-Saleme, J. (2017). The Status and Practice of Information Security in the Libraries of Sultan Qabous in Oman. *23rd Annual Conference and Exhibition of Special Libraries Association/Arabian Gulf Chapter*, Manamah, Bahrain, 33-41.

[17] Hissi, Y. E., Arezki, S., & Haqiq, A. (2018). Conceptualization of an Information System Governance Model Dedicated to the Governance of Scientific Research in the Moroccan University. *4th ICCTA*, 54-58.

[18] Almomani, I., Ahmed, M., & Maglaras, L. (2021). Cybersecurity Maturity Assessment Framework for Higher Education Institutions in Saudi Arabia. *Peer J Comput. Sci*.

[19] Dexter, J. (2002). The Cyber Security Management System: A Conceptual Mapping. https://www.sans.org/white-papers/591/

[20] PCI Security Standards Council. (2019). Payment Card Industry (PCI) Data Security Standard. https://www.pcisecuritystandards.org/

[21] Saudi Arabian Monetary Authority (SAMA). (2017). Cyber Security Framework. https://www.sama.gov.sa/en-US/Laws/BankingRules/SAMA%20Cyber%20Security%20Framework.pdf

[22] NCA-ESS Assessment Tool. (2018). https://nca.gov.sa/pages/ecc.html



**Contact information:**

**Tahani ALSAHAFI**
Department of Administration and Educational,
Arab East College for Graduate Studies,
Riyadh, Saudi Arabia
Al Qirawan, Riyadh 13544
E-mail: tahanialsahafi@hotmail.com

**Waleed HALBOOB**
(Corresponding author)
Center of Excellence in Information Assurance,
King Saud University,
Riyadh, Saudi Arabia
P.O Box 92144 Riyadh, 11653, Saudi Arabia
E-mail: Wmohammed.c@ksu.edu.sal

**Jalal ALMUHTADI**
Center of Excellence in Information Assurance,
King Saud University,
Riyadh, Saudi Arabia &College of Computer and Information Sciences,
King Saud University, Riyadh, Saudi Arabia
PJF9+5XV, King Saud University, Riyadh 12372
E-mail: jalal@ksu.edu.sal