Journal of King Saud University – Computer and Information Sciences xxx (xxxx) xxx

Contents lists available at ScienceDirect

Journal of King Saud University – Computer and Information Sciences

journal homepage: www.sciencedirect.com

GoSafe: On the practical characterization of the overall security posture of an organization information system using smart auditing and ranking

Jamal N. Al-Karaki [a,b], Amjad Gawanmeh [c,*], Sanaa El-Yassami [a]

[a] Dept. of Information Security Engineering Technology, Abu Dhabi Polytechnic University, Abu Dhabi, United Arab Emirates
[b] Dept. of Computer Engineering, The Hashemite University, Zarqa, Jordan
[c] College of Engineering and IT, University of Dubai, Dubai, United Arab Emirates

ARTICLE INFO

Article history:
Received 7 March 2020
Revised 15 August 2020
Accepted 18 September 2020
Available online xxxx

Keywords:
ISO/IEC 27001
Information security management system
ISMS
Security ratings
Security governance
Risk analysis

ABSTRACT

The lack of national security standardization bodies can have adverse impact on the adoption of international security standards and best practices. To assure security confidence among various organizations and to promote systematic adoption of standards and best standards, a practical framework that can support comparative measures is needed. This paper presents GoSafe, a novel practical cybersecurity assessment framework that is tailored to the ISO 2700x standard requirements for the development of Information Security Management System (ISMS). GoSafe can be used for both self-assessment and auditing/scoring tool by national cybersecurity authorities. Using GoSafe, organizations can evaluate their existing information security management systems against local and international standards by utilizing built-in pre-audit tools. As such, GoSafe will help organizations evaluate and enhance their readiness for evolving risks and threats. In GoSafe framework, a novel mathematical model was also designed and implemented for the scoring/rating tool, namely, the national cyber security index (aeNCI). The aeNCI employs multiple parameters to determine the maturity of existing cybersecurity programs at national organizations and generate a classification and comparison reports. The efficacy of GoSafe proposed framework is demonstrated using a practical case study. The results enabled the stakeholder to verify the security configuration of their systems and identify potential attack/risk vectors.

1. Introduction

The digital revolution has dramatically changed governance, communication, commerce, and industry worldwide. Digital information advent has given the rise of the ability of being accessed without the need for physical presence (Shah, 2014). However, it has become evident that use of technology comes with risks and security issues. Nevertheless, the world is increasingly becoming reliant on the cyber domain to provide services that keep nations running. Fig. 1 presented in (Improving Critical Infrastructure Cybersecurity) describes a common flow of information and decisions in today's organizations with three levels, namely, executive, business/process, and implementation/operations. These levels allow inter-communication to identify business priorities and apply risk management process taking into consideration business needs.

The ISO 2700x family of the standards, illustrated in Fig. 2, were introduced to govern information security management and practice (ISO/IEC, 2016). Among the family, the ISO/IEC 27001 standard (About ISO) was proposed to provide requirements for establishing, implementing, maintaining and continuously improving an Information Security Management System (ISMS).

The adoption of this standard is influenced by the organization's needs, objectives, security requirements and the organizational processes used; in addition to size and structure of the organization. The ISO/IEC 27002 standard sets the fundamental guidelines that are adopted for initiating, implementing, maintaining, and improving information security management standards. Conformity to these standards makes the systems more resilient, safe, and reliable. The actual standard controls shall implement the security requirements that are highlighted throughout a risk assessment framework. The ISO/IEC 27000 family of standards

* Corresponding author.
E-mail addresses: jamal.alkaraki@adpoly.ac.ae, jkaraki@hu.edu.jo (J.N. Al-Karaki), amjad.gawanmeh@ud.ac.ae (A. Gawanmeh), sanaa.elyassami@adpoly.ac.ae (S. El-Yassami).

Peer review under responsibility of King Saud University.

Production and hosting by Elsevier

https://doi.org/10.1016/j.jksuci.2020.09.011
1319-1578/

Please cite this article as: J.N. Al-Karaki, A. Gawanmeh and S. El-Yassami, GoSafe: On the practical characterization of the overall security posture of an organization information system using smart auditing and ranking, Journal of King Saud University – Computer and Information Sciences https://doi.org/10.1016/j.jksuci.2020.09.011

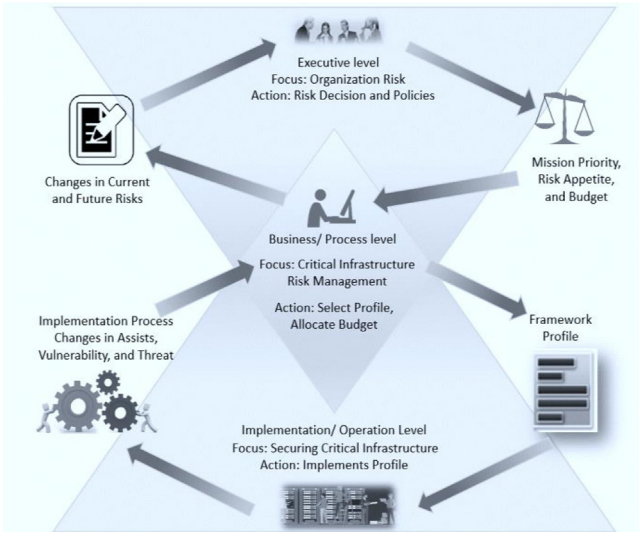


Fig. 1. Information Flows within an Organization and associated risks (Improving Critical Infrastructure Cybersecurity).

Fig. 2. The ISO 2700x Family Standards.

outlines controls and mechanisms that help maintain the security of information assets.

The ISO 2700x has certain obligations that each organization should follow with a major goal of enhancing cybersecurity posture. The security elements in ISO2700x standards are divided into People, Processes, and Technology. People are individuals who use or have an interest in our information security (e.g. owners, staff, clients, suppliers, contractors, etc.). Processes, which can be described in procedures, are work practices or workflows, the steps or activities needed to accomplish business objectives. Information technologies include all physical and logical tools used to perform business (e.g. data/voice networks). On the other hand, the ISMS is a systematic approach used to control and manage an institute's information and maintain its security (ISO/IEC, 2016). It defines the set of policies and procedures used to minimize the identified risks and ensure business continuity by proactively eliminating information security breaches.

The ISO/IEC 27002 Standards adopt the Plan-Do-Check-Act (PDCA) model (ISO/IEC, 2013) to construct the ISMS requirements, which is illustrated in Fig. 3. The scope of ISO/IEC 27001 and the requirements of the assessments and treatment of information security risks tailored for a specific organization described in detail in (ISO/IEC, 2013). The ISO/IEC 27001 Strategic Framework is

Fig. 3. ISO 2700x Implementation: Process cycle.

divided into three levels: strategic, tactical, and operational. The first addresses security policies, strategies and structure, while the second handles security controls, risks, and feedback. Finally, the last level is concerned with communication strategies as well as raising awareness through various channels. Fig. 4. Demonstrates these levels.

Towards this end, United Arab Emirates (UAE) published the local information security standards engineered by UAE local security governing bodies, namely, Electronic Security Authority (NESA) (Real security in a variety world, , 2015), Abu Dhabi Systems and Information Center (ADSIC) (Abu Dhabi Systems and Information Center), and Dubai Electronic Security Center (DESC) (Dubai Cyber Security Strategy, 2020). ADSIC proposed the information security standards in 2009 and the latest version has been revised in 2013 (Abu Dhabi government, 2013). The applicability of these standards is designed to meet the need of Abu Dhabi government personnel, contractors, and other interested third-party organization who is responsible for the creation, transmission, and destruction of Abu Dhabi government information assets. On the other hand, the UAE's National Electronic Security Authority (NESA) is aimed to protect Abu Dhabi's governmental information assets and to improve the national cyber security. NESA's risk assessment controls are very close to those of ISO/IEC 27001 where organization needs first to identify the context and scope, and then decide on the risk criteria and the risk methodology accordingly.

NESA is tasked with protecting the UAE's critical information infrastructure and improving national cyber security. To achieve

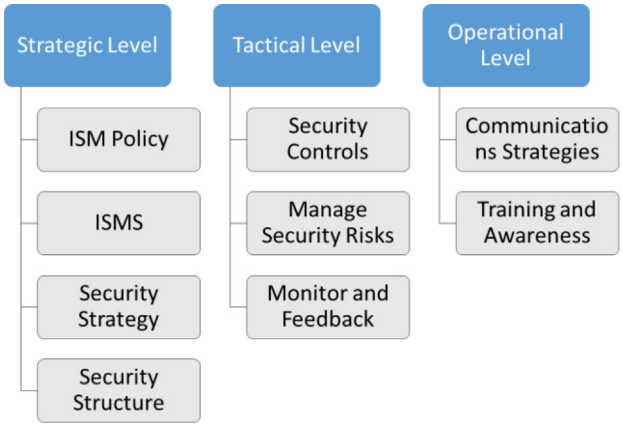


Fig. 4. ISO/IEC 27001 Strategic Framework.

this, compliance with their standards is mandatory. NESA information assurance standards provide requirements to implement information security controls to ensure protection of information assets and supporting systems across all entities in the UAE (Real security in a variety world, 2015). To comply with the NESA UAE, several stages are required. These stages can be summarized as: (1) gap audit to determine the status of the intended organization. (2) Training: to build the required knowledge in personnel. (3) Risk assessment: this refers to the M2 control family (4) Implementation: where internally, the recommended practices and procedures are deployed, and finally (5) the annual compliance audit which guarantees the organization to remain compliance by providing external and independent audit. Finally, Dubai Electronic Security Center (DESC) aims to protect information systems and telecommunication systems in the modern city of Dubai (Strategy and Center, 2017). We have performed a mapping exercise to show these meet international standards (i.e. ISO/IEC 27001. Table 1 below shows the mapping results. It is obvious that these local standards map to most control numbers of ISO 27001 standard.

Furthermore, the new Cyber security strategy of UAE was launched on 2019. The mission is to protect the cyber space in the country against security threats, risks and all challenges to national security including government sectors, private sectors, citizens as well as international cyberspace. The national cyber security strategy also introduced obligations for the Security of the network and information systems of all organizations. These governing bodies must assess the compliance of all organizations against these obligations and standards requirements. More specifically, in order to manage risks related to the security of network and information systems used in government activities, the UAE national law states that the National Electronic Security Authority (NESA), acting as the governing body for cybersecurity, in collaboration with the UAE Computer Emergency Response Team (aeCERT) and other organizations and entities as appropriate shall assess the technical and organizational measures implemented by organizations. Additionally, NESA shall assess the suitability of the measures implemented for the avoidance and the minimization of the impact of incidents affecting the security of government services and ensure their business continuity.

Table 1
Mapping of ISO/IEC 27001 to ADSIC and NESA standards.

Control Number	ISO 27001 Control	ADSIC	NESA
A.5	Information security policies	Information Security Governance	
A.6	Organization of information security		Mitigation of identified information security risks
A.7	Human resource security	Human Resources Security	Human Resource Security
A.8	Asset management	Information Asset Management	Asset Management
A.9	Access control	Identity & Access Management	Access Controls
A.10	Cryptography		
A.11	Physical and environmental security	Physical and Environmental Security	Physical and Environmental Security
A.12	Operations Security	Information Operations Management	Operations Management
A.13	Communications security		Communications Security
A.14	System acquisition, development and maintenance	Information Systems Design, Development & Testing	IS Acquisition Development and Maintenance
A.15	Supplier relationships	Third Party Supplier Security	Third Party Security
A.16	Information security incident management	Information Security Incident Management	Information Security Incident Management
A.17	Information security aspects of business continuity management	Information Systems Continuity Management	Information Systems Continuity Management
A.18	Compliance: internal such as policies, and external, such as laws		Compliance with UAE regulations

The development of IT security framework has attracted many researchers in recent years. The need for more better theoretical and practical approaches to security framework development is still at high stake. This paper is presenting a practical security assessment framework to meet certain security requirements published local and international standards. The national security requirements of the framework are those that have been published by NESA and others. Essentially, they were grouped for categories that covers main areas like: information security policy, asset management, risk assessment, risk management strategy, self-assessment and improvement, policies, processes and procedures for the protection of essential government services, identity management and access control, physical and environmental security, systems and applications security, data security, backups, security technologies, systems testing, awareness and training, threat detection, incident management, business continuity, and disaster recovery. The applicable controls for each group shall be recognized, analyzed, and assigned to the proper maturity level.

To accomplish the proposed objectives of the national security bodies, an assessment framework, called GoSafe, is proposed in this paper. The proposed framework also provides support for testing compliance of organizations' ISMS to local standards. GoSafe incorporates the following characteristics:

1. Cover the full extent of the national security requirements of NESA and others.
2. Check Compliance against the ISO2700X obligations
3. Can be used as a self-assessment tool
4. Can be used as a basis for an independent assessment to rate and compare across all organizations
5. Provide clear results regarding the security posture of the organizations
6. Can be used as a benchmarking tool per industry, type of organization and area of operation
7. Can be used as a guide for security requirements
8. Easy implementation by the various organizations

To accomplish the above characteristics of the proposed framework and in order to facilitate the fulfillment of the NESA and other bodies objectives, especially the measurable ones, a set of tools were developed as part of the framework. These include online survey, online pre-audit tool, and security index rating tool. In particular, a tool to standardize the possible security maturity levels of the organizations was needed. For this purpose, the national cyber security index (called aeNCI) was designed and tested for implementation as a major component of the overall assessment framework. Although aeNCI was developed for UAE, it can be easily generalized and applied to any other country worldwide. The National Cybersecurity Index (*aeNCI*) is a diagnostic and scoring tool to measure the level of commitment of each organization inside UAE and determine the maturity of their cybersecurity programs with comparison. The aeNCI could help identify the strengths and weaknesses of an organizations processes and examine how closely these processes comply to related identified best practices or guidelines in comparison to all other organizations.

The *aeNCI* tackles five main areas of an organization security posture, namely, legislative, technological, organizational, human and institutional capacity, and cross-cooperation. The five important broad categories. The *aeNCI* will be a benchmark ranking measuring the cybersecurity development capabilities of several UAE organizations. The index is essentially a composite index combining multiple indicators. These indicators and sub-groups will be used to rank organizations against the benchmark provided in each indicator. The proposed *aeNCI* includes 15 indicators selected based on relevance to the five *aeNCI* main areas, data availability, and possibility of cross verification. Furthermore, a pre-audit tool was developed and used be various organizations as part of the assessment framework that help to do self-audit of the security controls against which the organizations processes are appraised and the scale, based on which the rating of compliance of the organizations processes is evaluated.

1.1. Paper contribution

Currently, much of the security analysis schemes is done manually by a security expert or consulting companies. In this process, a lot of time and cost is consumed, and it can also introduce human errors. Hence, automation is needed to reduce the cost and time, as well as reducing human errors. To address the problems, we propose a practical security evaluation and measurement framework for security management across various organizations. The paper mainly introduces a practical framework for characterization of security posture of an organization using various tools and methods (e.g. surveys, preaudit tools, and scoring/rating methodology) with focus on the compliance with local or international information security standards (e.g. ISO/IEC 2700x). We summarize the contributions of our study as follows:

- We formalize the concepts of national security index to rank security readiness of various organizations based on comprehensive criteria and practical measures.
- We propose a novel practical framework for cybersecurity maturity assessment at organizational level based on ISO 27001 standards.
- We provide various tools within the framework for empirical evaluation of information security management system implementation and evaluation including a web-based pre-audit tool to assess organizations security posture against local standards for governance and compliance
- The proposed framework can be used in general to assess any ISMS of any organization that relies on ISO27001 requirements.
- The proposed framework provides organizations with the necessary tools to dynamically choose and derive enhancements in cybersecurity risk assessment
- The proposed framework is adaptive to provide a flexible and risk-based implementation that can be used with a broad array of cybersecurity risk management processes.
- To evaluate the applicability and practical use of the GoSafe framework over a large multi-campus academic institution. Policies and security controls are first evaluated and assessed, then risks and vulnerabilities are identified, and security recommendations are suggested accordingly.

1.2. Paper organization

The rest of the paper is organized as follows. In Section 2, we describe the framework components: The Framework Core, the Tiers, and the Profiles. We briefly describe ISMS, ISO/IEC 27001 family, adoption of international standards by local bodies in the UAE, namely, NESA, ADSIC, and DESC. The mapping of international standards to local standards of NESA and ADSIC as well as the structure and components of the proposed framework are also described in detail in Section 3. The implementation of the framework to the case study (IAT) is also introduced in Section 3. In Section 4, the definition of the national security index is introduced, and its use and interpretation are described. Results of Assessment and recommendations are also presented in this section. The conclusions and future pathways are outlined in Section 5.

2. Related work

In this section, we summarize related literature to the subject of security assessment frameworks. Authors in (About ISO) describe a cybersecurity capability maturity model as a means by which an organization can assess its current level of maturity of its practices. They provide a comparative study of cybersecurity capability maturity models that builds on a previous review (Education, 2016). The research presents an assessment of the differences, advantages and disadvantages of a systematic review of published studies from 2012 to 2017. The method was based on a modified taxonomy of software improvement environments across five categories as proposed in (ISO/IEC, 2013).

There are several interests in the security community in mapping local security policies into ISO standards (Peltier, 2016). Several works have been conducted in the recent years in this direction. For instance, the work (Barafort et al., 2017; Ali, 2014; Beckers et al., 2014) which addressed the issue of establishing security requirements and mapping them into ISO standards. Meanwhile, other works presented models for information security governance in accordance with ISO standards (Williams et al., 2013; Erin et al., 2020; Jennex and Durcikova, 2020). All existing trials are based on the security requirements of small organizations. However, none of these models was intended to capture nationwide security requirements.

The authors in Souag et al. (2016) presented a systematic mapping study and an analysis of existing security requirement engineering methods that employ the reuse of knowledge. The major objective of the works was to ensure that security requirements engineering methods rely on the reusability of knowledge. The work in Haufe et al. (2016) proposed a process mapping the study for Information Security Management System core processes. Several criteria for ISMS core processes were identified including: Regularity, Operation, Transformation, Accountability/responsibility and value generation. Implementation issues of the ISO/IEC 27001: ISMS Standard were discussed in Layton (2016); Humphreys (2016), where both authors highlighted that ISO/IEC 27001 allows for scoping, which provides wide level of flexibility at the implementation level. This however may create sever inconsistencies when the implementation diverts from standard.

Fabian et al. (2010) identified different categories for security requirements mapping, such as multilateral, UML-based, goal-oriented approaches, problem frames-based, risk analysis-based, and common criteria based. The work in Elahi (2009) adopted a classification for mapping depending on whether the method focuses on threats and vulnerabilities or on security requirements and countermeasures. Anton and Earp (2004) proposed a requirements taxonomy for reducing Web site privacy vulnerabilities. They evaluated 25 Internet privacy policies from several industries. This type of study helps in identifying the main goals and vulnerabilities from security point of view. The work in Souag et al. (2015) presented the conceptual space of security, where the authors identify the major concepts used in security and the relations among them. This allows exploiting vulnerabilities that are mitigated by security requirements, hence, fulfilled by countermeasures. Several frameworks for identifying security risks at institutional levels were also developed (Cavusoglu et al., Jun.,

2015; Dzombeta et al., Jul., 2014). In addition, standards for the management of information security and collections of best practice measures were developed in Mirtsch et al. (2020), International Organization for Standardisation and International Electrotechnical Commission (2013).

The notion of national security index has also been proposed in many studies. Many security indices have been developed by international organizations in partnership with the private sector. These indices tackle issues like regulations, organizational measures, national strategies, and cooperation (Cyber, 2015; Global Cybersecurity Agenda). In general, there are two types of indices. The first one is intended to perform comparison across organizations nationwide to embark on their security posture. The second one uses a scoring mechanism based on a group of indicators. In this paper, we propose an index that combines both approaches. Overall, these indices can help to shed light on cybersecurity gaps and practices at the country level. Table 2 summarizes various indices used for security assessment worldwide. The table also lists our proposed index, called UAE National Cyber Security Index (*aeNCI*), in the last row as comparable to other ones. Details of this proposed index is found in Section 4.

As a key piece of a robust security evaluation program, security ratings or security indexing are useful tools for evaluating cyber risks and facilitating collaborative, risk-based conversations between organizations (Crespo et al., 2018). Such tools will also act as diagnostic test to measure the level of commitment of an organization towards organization security, and to determine the maturity of its cybersecurity programs. To increase the degree of confidence in any security ratings/indexing measures, any proposed approach should promote quality and accuracy, fairness in reporting, and establish guidelines for appropriate use and disclosure of the scores and ratings. One major benefit of such tools will help to determine the continued compliance of the organization's Information Security Management System to a security standards and best practices (e.g. the ISO/IEC 27001 standard). In addition, such cybersecurity activities can help policymakers understand the importance and complexity of the arena (Jazri et al., 2018; Hohmann et al., 2017). To this end, a security evaluation framework with proper well-crafted security index to diagnose and measure the level of commitment of each organization at local and worldwide levels is needed. As demonstrated in Table 2, existing cyber securities indices lack comprehensive coverage for wide scope of assessment criterion. For instance, a few address economic impacts, ranking, profiles, and recommendations. Indices that address some of these lack fundamental ones, such as threats and technical aspects. Hence, the framework presented in this work is intended to fill gap and provide and comprehensive coverage for all metrics.

Watkins and Hurley (2015) proposed a method to examine the reliability and security of networks in terms of scientific-based risk metrics. The risk metrics are built with Base Score using the Analytic Hierarchy Process. Gadyatskaya et al. (2016) proposed to bridge the gap between practical risk assessment methods and academic research methods. This gap explains why the practical impact of academic results is somewhat limited according to the authors. Hence authors proposed a framework called TRICK for security risk assessment.

The recent work in Schmid and Pape (2019), Schmitz and Pape (2020) proposed a method for measuring the information security maturity, which is necessary to establish a knowledge-based information security management system within government organizations. Authors proposed to assess information security by applying a maturity model and assess the level of controls. The method is based on the analytic hierarchy process (AHP) that compares the information security controls' level of maturity within an organization and then provide a rank for each. The method was validated using real security data in the area of media and technology. Following this, LiSRA, a lightweight, domain-specific framework to support information security decision-making was also proposed by the same team. This shows the interest in establishing formal frameworks for security assessment, hence, our work will capitalize on this and address the lack of security assessment framework for government organizations based on their own security standards and controls.

3. GoSafe cybersecurity framework

In this section, we describe the research problem of this paper and also the general organization of the proposed security framework and show how local initiatives are being mapped to the international standard of ISO 27001.

3.1. Problem formulation

In this paper, we address the problem of security assessment of an organization utilizing practical approach and utilizing some useful tools embedded in the proposed framework. These tools work together within the framework that we propose is called GoSafe. The problem that the proposed framework is addressing is as follows:

Given a set of organizations $\mathbf{X} = \{x_1, x_2, x_3, .., x_n\}$, the proposed framework will provide tools and methods to do self-assessment and also for national authority to do measurement and rating across all organizations that comprise the cyber space of a given country:

1. For self-assessment, an organization selects an audit tool from the framework (online survey or preaudit tool).
2. Each organization $x \in \mathbf{X}$ can pre audit its security program and ISMS against local and international standards. Go safe tools will generate a report showing weaknesses and strengths of the organization ISMS against the local standard or international standard.
3. The national security authority (e.g NESA) uses *aeNCI* scoring schema, a report will be generated to rank all organizations in set **X** with respect to well-defined indicators and domains while identifying the weaknesses of ISMS implementation of the organization.

3.2. Methodology of framework design

In order to design the GoSafe, a combination of literature review regarding security requirements and a review of existing frameworks related to cybersecurity was conducted. At the time of the conduction of this review, there was only a limited number of established frameworks in the field, although recently, some more have been introduced. These documents were published by organizations like NIST, ISO, ISACA and others. Furthermore, the proposed framework makes use of auditing survey that are conducted online to map the international standards with existing security controls in the organization. The framework implemented an internal mapping between national security standards in the UAE and the international standards (e.g. ISO/IEC 2700x). The framework isn't just for government use, but it can be adapted to businesses of any size. Fig. 5 shows the three main components of the GoSafe framework.

The proposed framework will contain three fundamental components: the core, implementation tiers, and the profiles. The framework core is "a set of activities to achieve specific security outcomes, and references examples of guidance to achieve those outcomes. The implementation tiers identify levels organizations can use when implementing the framework. Each organization

Table 2
The indices matrix for assessment worldwide (Cybersecurity Index of Indices, 2015).

	Cyber Maturity	Cyber Threats	Score	Ranking	Indexing	Framework	Policy	Organizational	Technical	Economical	Recommendations	Profiles
Global Cyber Security Index	x		x	x	x		x	x				
Cyber Maturity (Asia Pacific Region)	x		x		x		x	x				x
The Cyber Index: International Security Trends and Realities	x					x	x					x
Cybersecurity: Global Rules	x		x		x		x	x			x	x
Cyber Policy Making at Turning Point	x					x	x	x				
Cyber Operation Maturity Framework	x	x				x		x				
Cyber Readiness Index 2.0	x		x		x		x			x		
Cybersecurity Intelligence Index		x			x				x		x	
Index of Cybersecurity		x			x				x			
Cybersecurity Index		x	x		x				x			
Gibson Index		x			x				x			
Information Risk maturity Index 2014	x		x		x			x				
Risk and Responsibility in a Hyper-connected world	x	x				x		x		x	x	
Cybersecurity Capability Maturity Model	x					x	x	x				
Cyber Power Index	x		x	x	x		x	x	x			
EU Cybersecurity Dashboard	x				x		x	x				x
UAE Cyber Security Index (aeNCI)*	x	x	x	x	x	x	x	x	x	x	x	x

*More details about this proposed aeNCI index is found in Section 6.

should maintain two profiles: current and target. These profiles can help an organization to find weak spots in its cybersecurity implementations and make moving from lower to higher tiers easier. These requirements can be compared against the current operating state of the organization to gain an understanding of the gaps between the two.

The proposed framework is not meant to replace existing processes in organizations. It is used to align business processes and ensure that cybersecurity programs address all elements of a cybersecurity program as defined in the framework core. Additionally, the Cybersecurity Framework assists organizations in adhering to compliance requirements using the concept of the profiles. When the GoSafe framework is implemented, a continuous and cyclic roadmap shall be followed as explained in Fig. 6. For instance, if analysis and reporting require more evidence, then more field work can be performed. The current state profile and target state profile are essentially the main two-state journey our framework is providing to organizations to better understand their security posture. To move from current state (weak) to target state (strong), each organization shall follow the roadmap explained in Fig. 6 of the GoSafe framework. By assessing and reviewing current security policies and practices against compliance requirements, current state Profile is identified. These include weak points of security. Next, the organization's target state profile is defined to address the weak points. The target profile defines goals for the organization's cybersecurity program to follow in order to align with standards/framework subcategories to reach the target state profiles. The framework defines a systematic approach to follow in order to close the gap between the two profiles. This approach is described in Fig. 7 as a roadmap with well-defined activities for all departments to follow in order to improve cybersecurity posture. The tool embedded in the framework generates reports for current and target state profiles. In the next section, we demonstrate an auditing tool that we built to help organizations in UAE check their compliance with local standards.

Table 3 illustrates the six mandatory stages of ISO27000 checklist that are interleaved in the implementation phase of the ISMS in our framework. We will adopt this check list in our mapping for security requirements in this paper.

4. Audit tools in the GoSafe framework

In this subsection, we describe tools that were built and added to the proposed GoSafe framework. These include the self-survey tool, which is to be explained further later in this section, and a

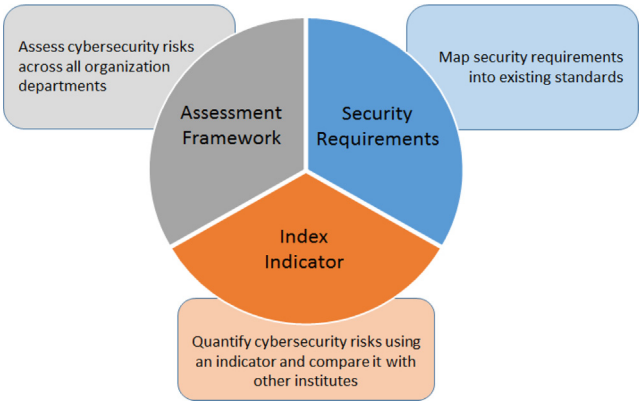


Fig. 5. Components of the proposed GoSafe architecture.

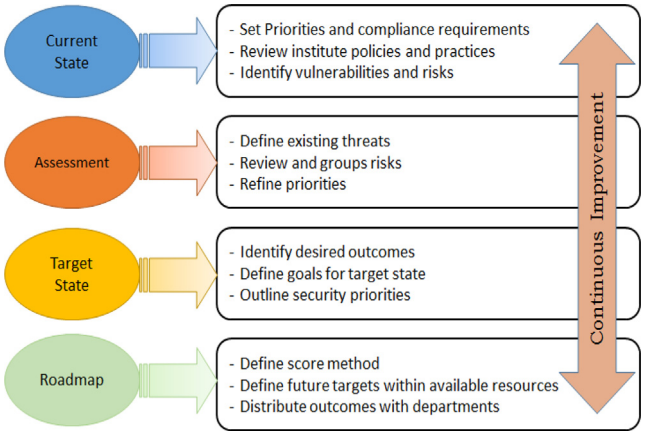


Fig. 7. The Security Assessment roadmap Methodology.

web-based Pre-Audit tool for ISO/IEC 2700x related local standards compliance e.g., NESA. The pre-audit assessment tool, which is implemented as part of the proposed framework, can simplify the process of assessing the information security level/posture of targeted organization. While ISMS auditing is a required challenge for government, public sectors, corporate sectors, and many other entities are struggling to understand the process and how to initiate it. The tool acts as a quick status check for any IT or non-IT management to understand organization's preparedness and compliance towards security standards (e.g. ADSIC, NESA, and DESC). Such tools are lacking currently in UAE. Knowing that UAE's official language in Arabic, the tool was developed in both Arabic and English. We find the Arabic version to be helpful in Government institutions where most current processes are documented in Arabic. Consequently, the security awareness campaigns are strengthened with a UAE national flavor. Below are the main characteristics of the developed tool:

- Provide Multilanguage support (e.g. Arabic support)
- Pre-audit can be completed within an hour along with a summary report.
- Graphical Summary Report for CxO or Government top officials.
- Summary report will provide status and also the areas to be focused.
- Within short time, an entity can strategize the ISMS initiatives and start program to align with ADSIC, NESA, and DESC standards.
- Self-Audit for an official organization audit and hence avoid huge consultation cost
- Act as a handy indicator to highlight areas lacking in preparation for an audit
- Wide adoption in Government, Ministries, Public sectors in UAE where processes are documented in Arabic
- Complement security awareness initiatives of UAE Government

Furthermore, the tool has a huge scope for further development. The performance of the tool can be further enhanced by including more organizational details such as complexity of organization structure, volume of transaction, process complexity etc. The assessment should be performed by an information security officer who is familiar with the environment. The user will be guided through a questionnaire to collect relevant details of various sections in ADSIC controls. For each item, the tool will flag the status of compliance as per score of (0–5) as in Table 4 for each security standard item, respectively. There are a total of 100 questions and it takes on average about 3 h to complete the assessment. The self-assessment can be done at the frequency the organization feels appropriate to track its security maturity. The assessment tool uses scale of 0–5 for scoring maturity as shown in Table 4, with 5 being the highest level of maturity. Levels of maturity include: Not Performed, Performed Informally, Planned, Well Defined, Quantitatively Controlled, and finally Continuously Improving. The organization can achieve the same maturity rating by substituting ADSIC, DESC, COBIT, NIST, NESA or another maturity framework that may be more familiar, with the same numeric 0 through 5 score.

The tool will show a quick flag at the end of the assessment by turning red or green or yellow to indicate status of compliance with ADSIC standards. Fig. 8 illustrates a snapshot of one assessment exercise for risk management (ISO 27005) with partial results.

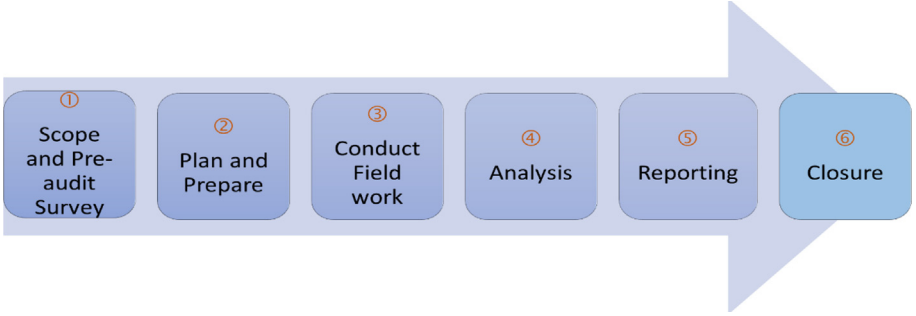


Fig. 6. The six mandatory stages of ISO2700x checklist in ISMS.

Table 3
The 4-steps action plan for protection.

Steps
[1]. Understand the ISO 27001 governance and compliance requirements.
[2]. Start planning a roll out of an information classification and retention policies and tools to the organization to help users identify, classify and protect sensitive data and assets.
[3]. Ensure that records related to information security are protected from loss, deletion, modification or unauthorized access by creating Audit and Accountability policies as part of your Standard Operating Procedures (SOPs).
[4]. Define administrative and security roles for the organization, along with appropriate policies related to segregation of duties.

Table 4
Assessment tool uses scale of 0–5 for scoring maturity (5 the highest level of maturity).

Score	ISO/IEC 2700x	Definition
0	**Not Performed**	The controls and security plans are **nonexistent**.
1	**Performed Informally**	Base practices of the control area are generally performed on an **ad hoc** basis. The practices are not formally adopted, tracked, and reported on.
2	**Planned**	The base security requirements for the control area are planned, implemented, and **repeatable**.
3	**Well Defined**	The processes are more mature than Level 2, **repeatable, documented**, **approved, and implemented organization wide**.
4	**Quantitatively Controlled**	The process is **measured and verified** (e.g., auditable).
5	**Continuously Improving**	The standard processes are **regularly reviewed and updated**. Improvements reflect an understanding of, and response to, a vulnerability's impact.

The tools in this framework were also used to demonstrate a case study of a large education organization in Abu Dhabi, namely, IAT that has campuses across all UAE. IAT is mandated to meet the ADSIC standards security requirements. Details of this case is explained in the next section.

5. Implementation of the proposed framework: A case study

In this section, we show how the proposed framework including the pre-audit tools can be applied to one large education institution in the UAE (ISO/IEC, 2013).

5.1. About IAT

IAT mainly uses web content, Learning Management System (LMS), Student Information System (Banner), and Enterprise Resource Planning (ERP). The ERP system will integrate all educational and non-educational operations and services so that to manage its business and to automate back office functions as in technology, services, finance, student services, and human resources. The Learning Management System (LMS) handles electronic educational technology contents including data administration, documentation, tracking, reporting, course delivery and assessment. Some of the systems used are also propriety software such as Microsoft products. Hence, it cannot be altered in any way by the IAT except for changing its policies.

Fig. 9 shows the current IAT services and architecture technology architecture across. These services provide support for all academic and non-academic operations across campuses in addition to large collaboration among all faculty, staff, and students of IAT. It also outlines which security measures or components are being adopted as of currently; hence, indicating areas of potential security improvement. Security architecture manages the three main layers using *Defense in Depth* concept from different technologies. On the other hand, data life cycle management, identity management, and end point security are the core component of the third layer. All the technologies from all layers are feeding logs to centralized server for event correlation, alerting, report, dashboard, audit, etc. It is governed by comprehensive policies, procedures, guidelines, standards, and security awareness that are supposed to be in compliance with standards such as ISO 27001:2013, ADSIC, and NESA. Fig. 10 shows the framework components and interactions of IAT IT services and applied security controls.

5.2. Implementation of GOSafe in IAT

The proposed framework was implemented in two phases:

(a) Conduct internal audits and management reviews of ISMSs using comprehensive surveys and match findings with the findings of the pre audit tool. The second part of this section shows the results of the audit survey performed for IAT information systems and assets in compliance with ISO/IEC 27001

ID No.	Questions	Current Maturity Level	Current Score	Desired Maturity Level	Desired Score	Notes
	Risk Management (ISO 27005:2013)		3.33		3.00	
1	Does the organization have a person or group has the role and responsibility for an ongoing process of evaluating the probability that known threats will exploit vulnerabilities and the resulting the impact on valuable assets. Risk management also assigns relative priorities for mitigation plans and implementation.	Yes	5	Yes	5	
2	Does the organization have a process for identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper, or other records containing sensitive information?	Well Defined	3	Well Defined	3	
3	Does the organization conduct routine risk assessments to identify the key objectives that need to be supported by the information security program?	Planned	2	Performed Informally	1	

Fig. 8. Snapshot of the Pre-audit tool Dashboard.

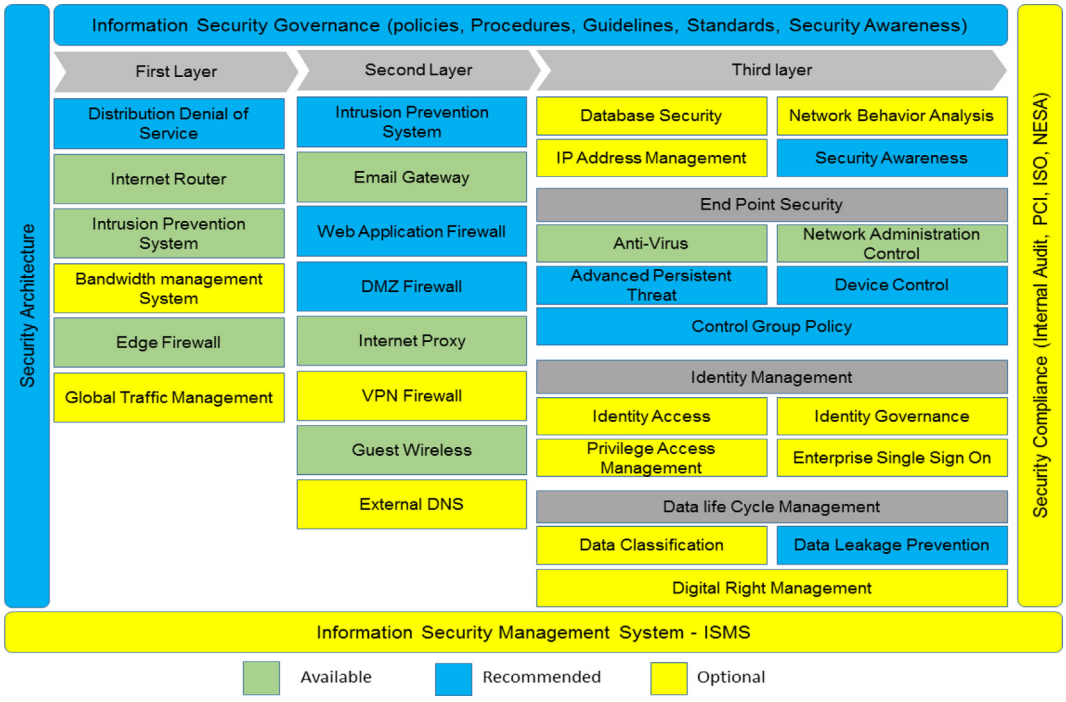


Fig. 9. Current IAT information technology architecture across all campuses with implemented security elements of ISMS.

(b) Apply the pre-audit tool to review compliance of IT architecture and services to the ISO/IEC 27000 family of standards, i.e., ISO/IEC 27001 and ISO/IEC 27002.

The audit performed is related directly to the organization's business requirements for information security. Examples of IAT's assets are hardware, software, network, personnel, and site. Each of these assets does expose differently the IAT information security to possible risks according to the possible vulnerabilities associated with. Table 5 demonstrates vulnerabilities classification based on the ISO/IEC 27005 standards. The framework also allows for vulnerability assessment and penetration testing (VAPT) for the organization ISMS. It identifies and quantifies possible vulnerable points in the organization's software and hardware architecture where exploitations are probable.

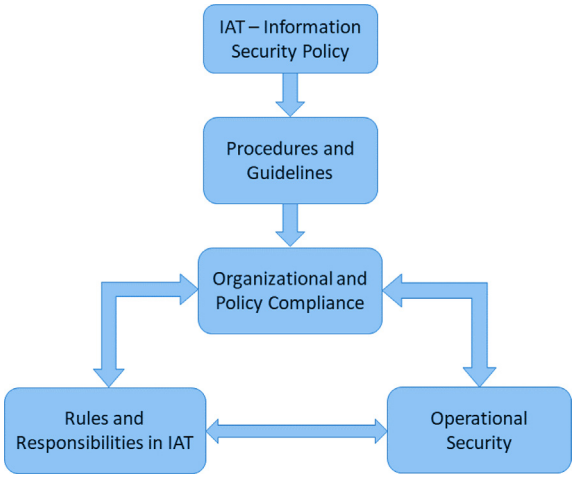


Fig 10. Schematics diagram showing the framework components and interactions for the case study.

Note that audit tool and proposed framework allows for a checklist to enable IAT to benchmark against other educational institutes nationally and internationally using a ranking process that is presented in Section 5 of this paper.

To meet the requirements of ISO/IEC 27001, an action plan for information protection was developed and implemented using the process outlined in Table 5 and by utilizing a comprehensive survey tool that is explained below.

5.2.1. IAT case study survey

An online comprehensive survey was used to evaluate the information security readiness of IAT and all associated entities. The motivation of this survey is to help understand the view of various stakeholders of the information systems security and posture.

The study aimed at identifying areas of weakness in terms of ISO 27001 family compliance so that proper mitigation mechanisms can be proposed accordingly. Furthermore, the results of the survey will help to understand the levels of Information Security in terms of ISO 27001 standards compliance. The data is collected using mainly the online survey using google forms and in rare cases data were collected using in-person interviews. The sample size of the survey includes all types of users in IAT who use IT services or systems (e.g. instructors, administrators, students, IT staff, etc.). An email invitation was sent to around 2000

Table 5
Vulnerabilities vs. Assets Classification.

Asset	Vulnerabilities
Hardware	Any exploitable weakness in the computer systems (e.g. hardware based attacks, unprotected storage)
Software	Lack of audit trail, poor design and coding, insufficient validation and testing
Network	Insecure lines of communication, lack of encryption, lack of non-repudiation, insecure network architecture
Personnel	Lack of security awareness program
Site	Lack of reliable source of power, area is subject to flood or volcano

users, among which 60% responded to the invitation. The survey was left open for a month and several reminders were sent to various users on weekly basis. The survey results were then analyzed using simple weighted average techniques.

The survey was divided into several areas for the assessment as per defined in ISO 27001:2013 ISMS requirements listed below:

(a) *Organizational Information security management system (ISMS) – Management.*
(b) *Asset Management*
(c) *Application Security*
(d) *Human resources security*
(e) *Physical and environmental security*
(f) *Access control*
(g) *Information security incident management*
(h) *Compliance*

Below are the results of this comprehensive survey. Fig. 11 shows assessment results of successful implementation of ISMS at IAT for various parts of the ISMS listed above. The x-axis represents rated percentage of respondents to each question and y-axis shows the questions for each domain.

The aspects of the survey that are reported in Fig. 11 are categorized as follows:

(a) Information Security policy domain
(b) Procedure and Guidelines
(c) Roles and Responsibilities
(d) Operational Security
(e) Compliance

Fig. 11(a) and 10(b) illustrate that over 50% of the participants were not aware that IAT has a defined ISMS policy. This would suggest that no formal documentation applies on the ISMS and it has not been disseminated properly among employees. However; 42% of participants who acknowledged the ISMS, agreed that its components are meaningful and adequate for the information security risk evaluation. Fig. 11(c) and (d) show equality between responses about the security measures and controls utilized in the IAT. Most of the IAT respondents are not aware of the cryptographic communication availability. Proper policy dissemination must apply so that employees are aware of the communication infrastructure they are using from security perspective.

It is shown that IAT do maintain a proper physical protection as in external cables, security locks and CCTV. This demonstrates the readiness that IAT owns to formulate the required ISMS and to be disseminated properly among employees. The presence of the security admin role enforces to log activities of different activities related to different roles. This is demonstrated in Fig. 11(d). Fig. 11(e) demonstrates that almost 35% of the respondents acknowledged the high level of protection maintained for the organizational records from destruction and falsification. However; around 43% of the respondents agreed that the IAT regulatory and contractual of the information security are not well identified to include the new business requirements. Fig. 11(f) shows overall assessment results of successful implementation of ISMS at IAT where 50% shows incompatibility with the standards. In addition, current IAT employees do agree that the IAT inventory is not fully up-to-date and accurate. Consequently, any new update on the inventory list is not being taken into consideration in case new and patched security controls should apply. This is demonstrated in Fig. 11(c).

The results were discussed in closed meeting with security team of IAT. The various department of IT department also attended the meeting. The major outcome of the meeting is that the framework and tool helped various teams to better understand IAT's cybersecurity goals and how these may be attained in a cost-effective manner over the span of the next few years. The team also noted that the framework provided them with more convenient tools to share information across the organization. In addition,

(a) Information Security policy domain (b) Procedure and Guidelines (c) Roles and Responsibilities

(d) Operational Security (e) Compliance (f) Overall Assessment Survey results of IAT

Fig. 11. Overall Assessment Survey results of IAT.

the IAT was able to support several individual departments with differing cybersecurity requirements to enhance posture. IAT stated that "since the framework outcomes can be achieved through individual department activities, rather than through prescriptive and rigid steps, each department is able to tailor their approach based on their specific departmental needs."

5.2.2. Insights and recommendations based on survey results

In this subsection, we will outline our recommendations to IAT institution based on the survey results as well as steps to be taken towards the implementation of these recommendations:

Phase 1 – *identify business objectives:* ensure that information-related business operations continue to be carried out in line with the ISO/IEC 27001 standard and to improve and strengthen the overall capabilities of the information security management system at IAT with prioritizing objectives. This step to gain management support.

Phase 2 – *obtain management support:* Moving towards ISMS, IAT should continuously support and make commitment by the organization's top management; adopt a common strategy and policy across the entire organization; IAT ISMS should have defined security objectives and activities to be based on business objectives and requirements and led by business management.

Phase 3 – *select the proper scope of implementation of ISMS:* Information assets of IAT should have a central authority for administrating and managing them.

Phase 4 - *define the proper scope of risk assessment:* IAT needs to define and document a method of risk assessment to meet the requirements of ISO/IEC 27001. Since ISO/IEC 27001 standards do not specify a specific risk assessment method, any international risk guide can be used.

Phase 5 – *prepare, rank, and protect an inventory of information assets according to risk classification and assessment:* Important IAT assets with associated services should be classified and stored in an inventory where inventory, ownership of an asset, movement of physical IT assets, shall be updated and clearly stored. The loss, theft of IAT assets shall be reported immediately to the IT manger or Security officer.

Phase 6- *prepare SOA*: The Statement of Applicability (SoA) is a document that describes which of the list of controls of ISO 27001 are applicable to the IAT organization. The chosen controls to be implemented and applied.

Phase 7 – *manage the risks and create risk treatment plan.* IAT shall develop a Risk Treatment Plan (RTP) that will act as a coordination point and define actions needed to reduce unacceptable risks while implementing the required controls to protect information assets within the IAT organization.

Phase 8 – setup policies and procedure to control risks

Phase 9 – allocate resources and train the staff.

One final note is that the ISMS implementation process must gain full commitments from IAT management by allocating enough resources to manage, develop, maintain and implement the ISMS.

While the main target of the work is to present a framework that supports quantitative cybersecurity assessment using an index based indicator, it is also important to provide ranking schema among various organizations on how they comply with requirements for various standards, i.e. DESC and ADSIC. This is the topic addressed in next section.

6. Development of the UAE national security index (aeNCI)

In this section, we will define the notion of national security index in the UAE. This indicator is designed based on a well-defined security standard that acts as a common reference for various security requirements of different entities. This is necessary in order to have a normalized indicator, and hence be able to assess various entities using the same standard. The National Cybersecurity Index (*aeNCI*) is a diagnostic test to measure the level of commitment of each organization inside the UAE towards organization security and to determine the maturity of their cybersecurity programs.

As a key piece of a robust security evaluation program, security ratings or security indexing are useful tools in evaluating cyber risk and facilitating collaborative, risk-based conversations between organizations. To increase confidence in security ratings, any proposed approach should promote quality and accuracy, fairness in reporting, and establish guidelines for appropriate use and disclosure of the scores and ratings.

The proposed Security Index (*aeNCI*) objectives are:

(a) To determine the continued compliance of the organization's Information Security Management System to a security standards and best practices (e.g. the ISO/IEC 27001 standards);
(b) To evaluate the ability of the organization's Information Security Management System to meet clients' applicable statutory, regulatory and contractual requirements, where applicable;
(c) To evaluate the effectiveness of the organization's Information Security Management System to ensure that clients are continually meeting their specified objectives;
(d) To identify areas of improvement of the organization's Information Security Management System, as applicable;
(e) To verify the effective implementation of corrective actions arising from the findings of the previous audit. Fig. 12 shows the reference model for the proposed national security index framework.

The *aeNCI* acts using five broad indicators that covers legislative, technical, organizational, capacity building, and cooperation. The five main areas of the *aeNCI* are briefly explained further in Table 6 below:

6.1. Existing cybersecurity indices

Many initiatives have been developed across the world to address the issue of measuring trust of existing ISMS at national levels. Examples include the index of cybersecurity, cybersecurity index, and the Gibson index (See table 1).

6.2. Methodology

The *aeNCI* is a framework that measures the cybersecurity commitment in various organizations. In addition, it should be ranked relative to other organizations within the UAE. This includes the type of cybersecurity, its level, and development over time. The

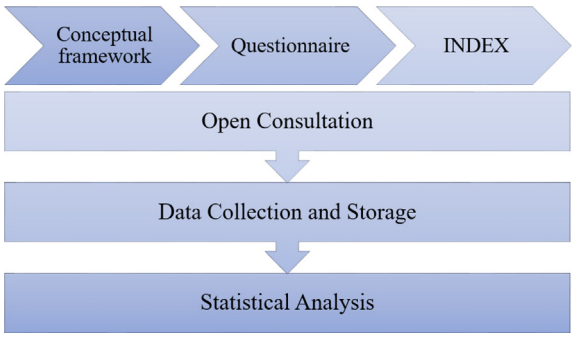


Fig. 12. Reference Model for aeNCI.

index will also provide an underground for continuous improvement while enhancing ranking, and as a result, will increase the overall level of commitment to cybersecurity in the UAE. The methodology adopted in this paper consists of four phases:

1. Data collection: Two methods for data collection have been used. Primary data is collected by an individual directly, and in the other, secondary data is collected through offices and institutions.

2. Data processing: This involves actions to verify, organize, transform, integrate, and extract data to obtain an appropriate output.

3. Data Analysis: This involves methods to describe facts, detect patterns, develop explanations and test hypotheses from analyses of data. Methods can include statistical data analysis, data modeling, and interpretation of results.

4. Reporting: In this phase, results of the previous three phases are published.

6.3. Conceptual framework

The *aeNCI* is a framework that can be used for ranking various benchmarks that are adopted for cybersecurity development within UAE organizations. The index framework combines multiple indicators.

There are several indicators that have been identified to rank organizations against the benchmark used. The *aeNCI* includes 15 indicators selected based on the following criteria:

- Relevance to the five *aeNCI* main areas
- Data availability
- Possibility of cross verification

Conceptually, the number of indicators is not limited. In the future conceptual framework, new indicators could be added, and existing ones could be deleted or updated. Fig. 13 shows the *aeNCI* assessment platform steps of operation. The listed components are evaluated using several metrics. First, there must be the existence of a legal framework that can handle cybersecurity legal issues quantitatively. Second, the existence of Information Technology related measures dealing with cybersecurity in the organization must be in place. The organizational component being evaluated, is based on the existence or absence of strategies or initiatives related to cybersecurity development at the organization.

Capacity building is evaluated based on the number of educational and training programs, research, and development related to cybersecurity. The cooperation component is evaluated based on the number, scope and type of partnerships, cooperative frameworks, and information sharing networks. Fig. 14 shows the categorization of the aeNCI domains and factors. In addition, these factors are further explained in Table 7.

6.4. The security index

The index has been developed following the below steps:

- Identification of fundamental cyber threats at the national level,
- Identification of the national capacity and security measures necessary for cyber security,
- Selection of important and measurable capacities and measures,
- Development of cyber security indicators according to security capacities and measures,
- Grouping of cyber security indicators,
- Application of criteria for each option and measurement in the expected performance. After that, evaluation of consequences of each option against its criterion,
- Evaluation of weights for each factor to reflect their relative importance to the index,
- Combination of weights and associations of scores for each domain to derive an overall value.

Index development is achieved through three phases, namely, data collection, scoring and ranking. Fig. 15 illustrates the cybersecurity index lifecycle.

Phase 1: Data collection

The *aeNCI* measures indicators that can be proven by clear evidence. Evidences in this index are presented as official web links or/and official documents. This phase is done in two steps:

(1) *Data collection process*

Data collection includes an online questionnaire that is used to gather responses along with a feature to upload documents, which is used to collect supporting documents and links provided by organizations as evidence.

The aeNCI questionnaire responses are verified and qualitative evaluation is performed to identify possible missing elements (e.g. missing responses, missing supporting documents, or missing links, etc.). The accuracy of responses is then enhanced by contacting the concerned organizations and providing them with guidance when filling out the questionnaire. Once formal approval is received from organizations attesting that they have no more data to provide, the questionnaire will be considered as valid and will be used for analysis, scoring, and ranking.

(2) *Questionnaire*

The questionnaire elaborates several sub-index categories by including several binary questions. The values for the 15 indicators

Table 6
aeNCI indicators.

Legal
Legal measure needs a legislative framework that sets standards for behavior and facilitate the development of cybersecurity capabilities at national level.
Technical The technical indicator defines technical capabilities to detect and respond to cyberattacks/threats against an organization defense.
Organizational Organizational measures embody setting a broad strategic objective along with a comprehensive plan in implementation, delivery and measurement of those objectives.
Capacity Building This indicator measures the know-how across the organization and formulate appropriate plans to promote the development of competent professionals.
Cooperation To enable the development of strong cybersecurity capabilities, deter repeated and persistent threats, and enable better investigation, cooperation plan is needed across the organizations.

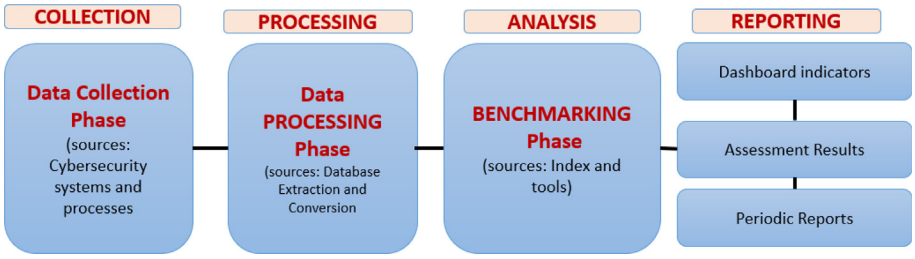


Fig. 13. The aeNCI Assessment Phases and Platform.

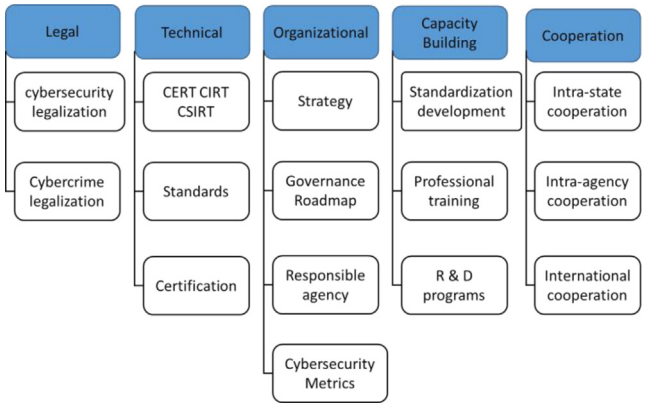


Fig. 14. *aeNCI* Domains and Factors.

are therefore constructed through a set of binary questions. To eliminate opinion-based evaluation, binary answers are used. This allows quicker and more comprehensive evaluations that do not require lengthy responses from organizations and save largely the time. As such, the process of providing answers will be accelerated and streamlined. Organizations should simply confirm or deny the presence of certain in-place solutions.

In the future framework, and to encourage organizations, we plan to use also partial answers and include even non-fully established in progress solutions.

Phase 2.I: processing/Scoring

The *aeNCI* uses the weighted arithmetic mean to compute cybersecurity commitment scores. We associate assessment factors that were explained in Table 7 with some weights. For each assessment factor that was fully operational, the corresponding weighting is granted. For a partially operational, half of the assigned weighting is granted as will be explained later in this section. Table 8 describes the parameters used to generate an overall score.

To elaborate, each domain has a weight $\boldsymbol{w_j}$ and a set of associated assessment factors. Each assessment factor belongs to a domain and has a specific weight noted as $\boldsymbol{w_{j,i}}$. The assessment factors multiplied by their weight and added together give the score of each domain. The domains scores multiplied by their weights and added together give the final score $\boldsymbol{S}$.

Cybercriminal legislation and Regulation & compliance are the two assessment factors associated with Legal capacity which its score $\boldsymbol{L}$ is calculated using Eq. (1). Where $w_{1,1}$ and $w_{1,2}$ represent respectively the weights assigned to Cybercriminal legislation and Regulation & compliance.$u(a_{1,1})$ and $u(a_{1,2})$represent the scores of the two assessment factors.

$$L = \sum_{i=1}^{2} \left(w_{j,i} * \left(u(a_{j,i})\right)\right) \tag{1}$$

$$L = w_{1,1} * u(a_{1,1}) + w_{1,2} * u(a_{1,2})$$

Technical capacity score $\boldsymbol{T}$ is calculated using Eq. (2). Where, $w_{2,1}$, $w_{2,2}$, and $w_{2,3}$ are the weights assigned to the three assessments factors associated with Technical capacity.$u(a_{2,1})$, $u(a_{2,2})$ and $u(a_{2,3})$ represent the scores of the three assessment factors.

$$T = \sum_{i=1}^{3} \left(w_{j,i} * \left(u(a_{j,i})\right)\right) \tag{2}$$

$$T = w_{2,1} * u(a_{2,1}) + w_{2,2} * u(a_{2,2}) + w_{2,3} * u(a_{2,3})$$

In Eq. (3), organizational capacity score $\boldsymbol{O}$ is calculated based on the summation of the scores of its four assessments factors represented by$u(a_{3,1})$, $u(a_{3,2}), u(a_{3,3})$and $u(a_{3,4})$. Where each factor score is multiplied by its weight $w_{3,1}$, $w_{3,2}$, $w_{3,3}, w_{3,4}$.

$$O = \sum_{i=1}^{4} \left(w_{j,i} * \left(u(a_{j,i})\right)\right) \tag{3}$$

$$O = w_{3,1} * u(a_{3,1}) + w_{3,2} * u(a_{3,2}) + w_{3,3} * u(a_{3,3}) + w_{3,4} * u(a_{3,4})$$

In Eq. (4), the capacity building score $\boldsymbol{B}$ is calculated by summing the weighted scores of the standardization factor, manpower factor, and R&D factor.

$$B = \sum_{i=1}^{3} \left(w_{j,i} * \left(u(a_{j,i})\right)\right) \tag{4}$$

$$B = w_{4,1} * u(a_{4,1}) + w_{4,2} * u(a_{4,2}) + w_{4,3} * u(a_{4,3})$$

Cooperation capacity score $\boldsymbol{C}$ is calculated in Eq. (5). Where, $w_{5,1}$, $w_{5,2}$, and $w_{5,3}$ are the weights assigned to the three assessments factors associated with Cooperation capacity. $u(a_{5,1})$, $u(a_{5,2})$and $u(a_{5,3})$represent respectively the scores of the intra-state factor, intra-agency factor and international cooperation factor.

$$C = \sum_{i=1}^{3} \left(w_{j,i} * \left(u(a_{j,i})\right)\right) \tag{5}$$

$$C = w_{5,1} * u(a_{5,1}) + w_{5,2} * u(a_{5,2}) + w_{5,3} * u(a_{5,3})$$

The overall score $\boldsymbol{S}$ is computed in Eq. (6) by multiplying the domains weights represented by w_1, w_2, w_3, w_4, w_5 by the domains scores represented by L, T, O, B, C then summed to get $\boldsymbol{S}$.

$$S = \sum_{j=1}^{m} \left(w_j \sum_{i=1}^{n} w_{j,i}\left(u(a_{j,i})\right) \right) \tag{6}$$

$$S = w_1 L + w_2 T + w_3 O + w_4 B + w_5 C$$

Phase 2.II: Ranking

An organization's rank reflects the number of organizations that sit above it. After we compute organizations' scores, we sort them from highest to lowest. The highest score gets a rank of #1 and the

Table 7
aeNCI factors explained.

***aeNCI* Domains and Factors**	
Legal Measures	
A legislative framework enables all organizations to establish a consistent law enactment in place. This will enable consistent harmonize practices and interoperable measures and will facilitate combat against cybercrime at all levels.	
1	**Cybercriminal legislation**
The Cybercrime legislation introduces laws to deal with the unauthorized access of computers, systems and data. These laws can be partial or comprehensive, where partial legislation refers to the simple existing criminal law or code, while comprehensive legislation has dedicated laws to deal with the specific aspects of computer crimes.	
2	**Regulation & Compliance**
These laws are used to deal with data protection, breach notification, certification, and standardization requirements.	
Technical Measures	
Technical measures are used to find if technical frameworks dealing with cybersecurity are endorsed by the organization at local or national levels.	
3	**CERT/CIRT/CSIRT**
This requires establishing a CERT (Computer Emergency Response Team), CIRT (Computer Incident Response Team), or CSIRT (Computer Security incident Response Team). Such teams provide the capabilities to identify, defend, respond and manage cyber threats and enhance cybersecurity in the organization.	
4	**Standards**
This indicator measures the ability to implement a framework that captures international cybersecurity standards.	
5	**Certification**
This indicator measures if an internationally recognized cybersecurity certification and accreditation program exists for professionals in the organization.	
Organizational Measures	
The existence of effective organizational structures to promote cybersecurity, including warning of cybercrime and incident response, to ensure cross-sector coordination between existing initiatives is crucial.	
6	**Strategy**
Securing Network and Information Systems to maintain resilient and reliable information infrastructure is needed. Such strategy will protect assets including people; address vulnerabilities in critical infrastructures and prevent potential cyber-attacks; and to have a reliable system, when a cyber-attack takes place, where recovery time is reduced, and disruption is minimized.	
7	**Governance Roadmap**
A strategy/policy for cybersecurity is needed to establish a roadmap for governance and identifies key stakeholders. In developing a high-level governance for cybersecurity, policy framework becomes a top priority in this effort.	
8	**Responsible agency**
A national agency for implementing a cybersecurity strategy/policy is needed through formulation of committees, working groups, advisory councils or centers. Such agencies can also handle the coordination of responses to cyber-attacks by providing the proper organizational structures.	
9	**Benchmarking**
Benchmarking is an indicator that can quantify the existence of any officially recognized benchmarking exercises or referential used to measure cybersecurity development.	
Capacity building	
This is related to the development of the most competent professionals, awareness campaigns and accreditation framework to enhance knowledge and know-how.	
10	**Standardization Development**
This indicator is used to measure the level of maturity of a cyber security program and associated technology. This is also important to address new emerging standards.	
11	**Manpower Development**
Manpower development used to measure the number of certificates issued under internationally recognized certification programs standards. And includes campaigns to spread cybersecurity culture to wide community	
12	**R&D Programs**
This performance indicator can be measured by the number of research and development and professional training programs.	
Cooperation	
Cybersecurity is a global problem and hence partnership and cooperation with national and international bodies is needed. In addition, cooperative frameworks and information sharing networks will support cooperation.	
13	**Intra-state Cooperation**
This indicator represents officially recognized partnerships for sharing cybersecurity assets. This is applied to initiatives for sharing assets at the national, regional, or international levels.	
14	**Intra-agency Cooperation**
Intra-agency refers to sharing cybersecurity assets within the public sector or between different sectors as well as within departments/ministries.	
15	**International Cooperation**
This indicator measures any participation taking place in an internationally recognized cybersecurity forums and gatherings.	

lowest score gets whatever rank corresponds to the number of units we rank in. To de-emphasize the differences between individual organization ranks, we also group organizations into quartiles according to their ranks separately. For each set of ranks, there are four quartiles that divide all units. The top 25% are the safest organizations with the best ranks. The bottom 25% are the riskiest organizations with the worst ranks; the other two quartiles are neutral.

Phase 3: benchmarking

The benchmarking is used to compare an organization's security level and compare it to some other organizations against the best practices in order to improve information security posture. The rating of each organization is based on the aeNCI Index, which is calculated based on several factors/indicators. The calculated security index is indicative of a level of cybersecurity posture. The index will allow an organization to compare its position with that of other organizations so that it can be a tool to improve information security awareness among others. It also acts as a gateway to assessment by third party such as ISMS conformity assessment and information security audit. The benchmark tool enables organizations to compare their scores with ideal/average scores or those of other organizations. Towards this end, the Gosafe benchmark tool is a comparative and quantitative assessment tool whose assessment results are presented in scores and charts, allowing an organization to benchmark their position in relation to that of other organizations or to an ideal score. Such benchmark provides unique opportunity for cyber security indices (e.g. aeNCI) to identify their capabilities by having proper reference to ISO standards. The aeNCI conforms to international standards ISO/IEC 27001. In the field of comparative assessment, the result may change

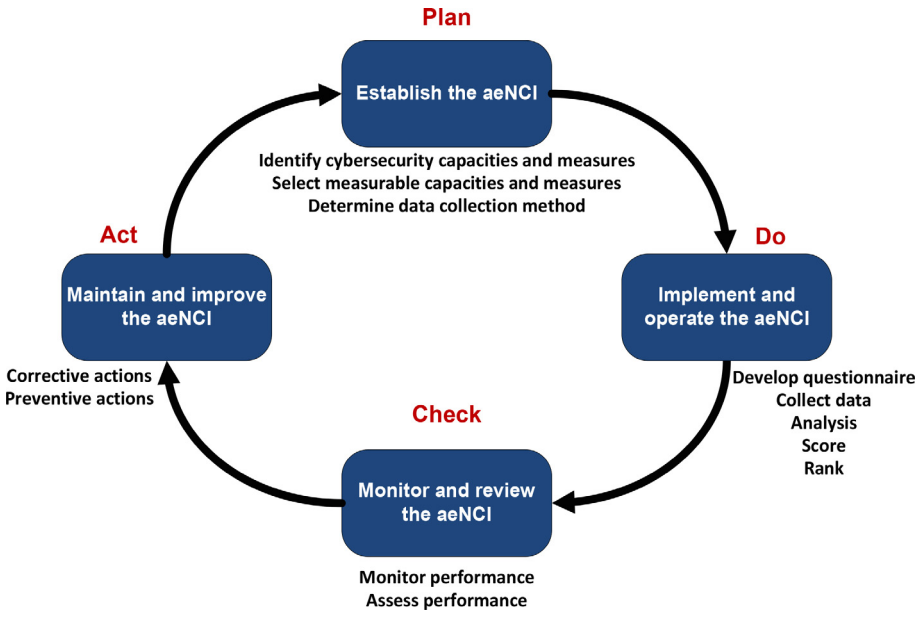


Fig 15. *aeNCI* Cybersecurity Index Process.

Table 8
aeNCI Data Dictionary.

Data Dictionary	
Identifier	*Description*
m	represents the number of categories or domains
n	represent the number of assessment factors
w_j	represents the weight assigned to domain j
$w_{j,i}$	represents the weight assigned to factor i
$u(a_{ji})$	represents the scoring function for criteria a_i that belongs to domain j.
S	represents the overall score
L	represents the legal capacity score
T	represents the technical capacity score
O	represents the organizational capacity score
B	represents the capacity building score
C	represents the cooperation capacity score

depending on the data collected from the entity. Considering rapidly changing information security environment, there might be a need to use old data for better diagnosis (i.e. phase 1).

The radar chart can typically shed light on the benchmark implementation status of the 15 security measures in Table 7. It shows not only the organizations's score for the 15 security measures, but it also shows average and ideal scores (See Fig. 16). The ideal score of 5 indicates score of top organizations in a certain group, while average score is set to 3. These values can be configured by the organization. Variations of comparisons can also be made, e.g., group-based comparison, size-based comparison, industry-sector based comparison, and time-series comparison where current posture/score can be compared with past. Entities that failed to reach the average of all group of entities can set the target at that average level. If an entity achieved that level, they can try to get to the ideal level. In this way, organizations can improve their security level gradually by identifying gaps in existing practices at different levels (See Fig. 16). If the organization has not reached the ideal level, recommended approaches will be displayed by the tool.

6.5. Case study

1. **Assessment factor rating scale**

To determine how organizations will be scored against the assessment factors, the *aeNCI* uses a three-level system instead of a binary system that evaluates only the existence or absence of a specific activity as shown in Table 9. The three-level system takes partial measures into consideration; insufficient evidence, partially operational or fully operational. The scoring function is normalized so the scores fall into a range from 0 to 1.

Normalizing the above constructed scale gives:

$$u(aji) = \begin{cases} 0, & \text{organization does not meet assessment} \\ 0.5, & \text{organization partially meet assessment} \\ & \textit{and} \\ 1, & \text{organization fully meet assessment} \end{cases}$$

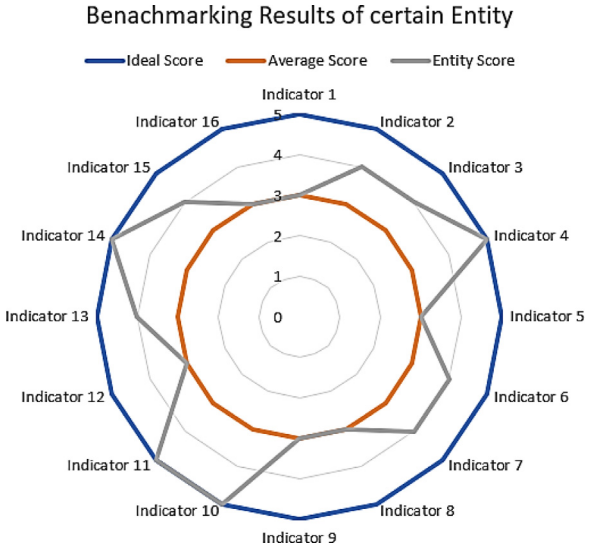


Fig. 16. Radar chart showing assessemnt benchamrking results.

Table 9
Rating scale for cybersecurity capabilities.

	Level	Score
○	***Insufficient Evidence:*** evidence is lacking or has yet to be located. It is possible, however, that the data exists but is not yet publicly available or is classified.	0
◍	***Partially Operational:*** there is evidence of policies, activities, and/or funding, however, the activity may be immature, incomplete, or still in the early stages of development. While these initiatives can be observed, it may be difficult to measure their functionality.	0.5
●	***Fully Operational:*** there is sufficient evidence to observe and measure a mature, functioning activity	1

Each domain has a set of questions organized by assessment factors. The questions have yes/no responses. If the response is yes, the respondent must provide evidence for each question as supporting information. Then the score will be assigned (0, 0.5, or 1).

Therefore, an organization that fully meets an evaluation criterion during the scoring phase will receive a score of 1, an organization that partially meets an evaluation criterion will receive a score of 0.5, and an organization that does not meet a criterion will receive a 0 for that assessment factor.

2. Assessment weights

The final step is to assign weights w_i to each assessment factor. These weights serve as scaling factors to specify the relative importance of each criterion. The Reference Comparison method is used to assign weights to each factor. Given a set of assessment factors, the most important and significant factor in the set is assign a value of 3 and used as reference criterion. Using this as a reference, the remaining factors are ranked as follows:

Table 10
Reference Comparison Weights on evaluation criteria template.

#	Assessment Factor	Weight	
1.0	Domain x	Before normalization	After normalization
1.1	Factor 1	2	0.25
1.2	Factor 2	3	0.375
1.3	Factor 3	1	0.125
1.4	Factor 4	2	0.25

3 if the factor is as important as the reference criterion
2 if the factor is slightly less important than the reference criterion
1 if the factor is much less important than the reference criterion.

After assigning weights the next step is to normalize these values so that they sum to one. Table 10 shows an example of the weights assigned to each factor belonging to a specific domain x using the Reference Comparison method for computing weights where factor 1, factor 2, factor 3, and factor 4 are assigned respectively a weight of 2, 3, 1, 2.

The sum of these weights is 8, so to normalize the values, we need to divide each one by 8. The resulting numbers sum to 1 and give the weights as presented in Table 10.

3. Calculation of the index

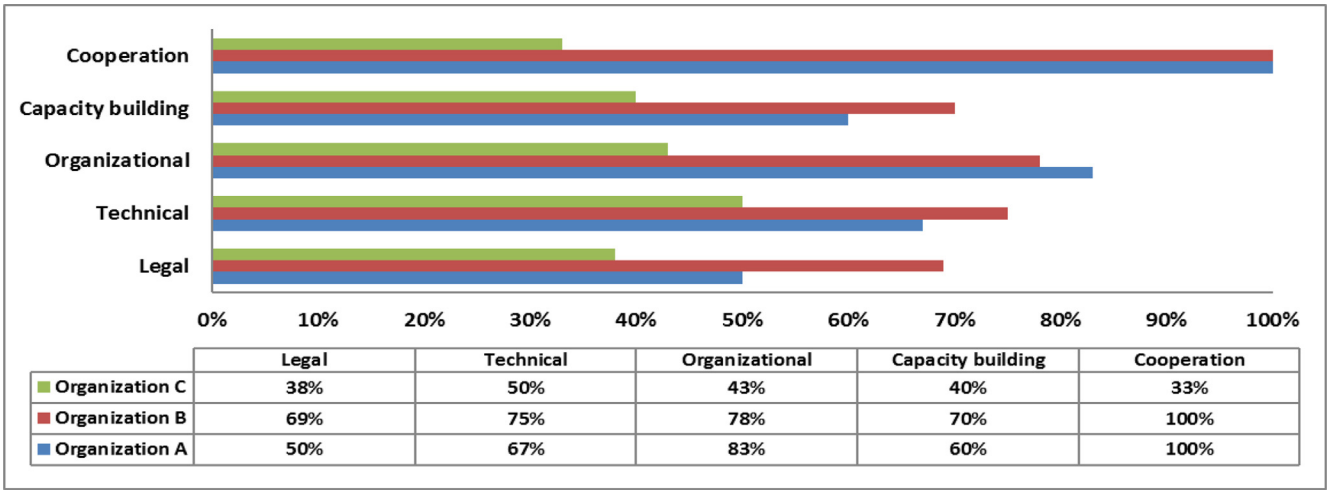
Fig. 17 illustrates the average *aeNCI* score for three anonymous organizations to illustrate the respective assessment factor. Organization B is the highest-ranking, scoring a perfect 100 in Cooperation and all other scores show positive across to all assessment factors. Organization A is the second highest ranked organization scoring 100 in Cooperation, plus the highest score in the Organizational factor. Organization C is ranked third, placing between 33rd and 65th percentiles for the five factors. On the other hand, Fig. 17 shows the organizations' scores by assessment factor. Some factors contributed the same score to different organizations, while others did with significant difference.

6.6. Recommendations

This initiative is a humble approach to introduce a pre-audit tool, which can be useful as a quick status check for any IT or non-IT management understanding an organization's preparedness and compliance towards ADSIC. As of now, there are not many tools available in compliance with Abu Dhabi information security standards. This tool is also intended to popularize the UAE's information security initiatives.

7. Conclusion and future work

The lack of national security standardization bodies can have adverse impacts on the adoption of recognized standards and best



	Legal	Technical	Organizational	Capacity building	Cooperation
Organization C	38%	50%	43%	40%	33%
Organization B	69%	75%	78%	70%	100%
Organization A	50%	67%	83%	60%	100%

Fig. 17. Factor scores by organization.

practices. In this paper, we have established an assessment framework and devised a national security index that will aid organizations when evaluating and assessing information security management systems to embark on its readiness for evolving risks and threats. We focused on the Institute of Applied Technology (IAT), a leading geographically dispersed educational institution in the UAE, as a case study.

The proposed framework focuses on ISO/IEC 27001 international security standards which have been mapped to local information security standards engineered by the Abu Dhabi Systems and Information Center (ADSIC) along with the information assurance standards driven by the UAE's National Electronic Security Authority (NESA). The framework formulates policies and controls that are compliant with both national and international information security standardization bodies to build more security resilience educational systems in the UAE and worldwide. In current format, the framework does not support life assessment, this can be further enhanced by embedding online life assessment methodology based on machine learning, where several parameters can be fetched in continuous manner, and then used in order to provide index evaluation that can be monitored against certain threshold. This can be used to highlight risks instantly. This concept is currently under investigation by the team.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

Authors would like to thank our colleague Munavwar Shaikh from AbuDhabi Polytechnic for his input on ISMS survey during initial time of wok on this paper. This work was internally supported by Abu Dhabi Polytechnic University and University of Dubai. The authors also value the initial discussions on the importance of this work with Dubai Electronic Security Center (DESC) back in 2018.

References

About ISO. ISO standards. [Online accessed: December 2016]. http://www.iso.org/iso/home/about.htm.

Abu Dhabi government Information Security Policy – version 2 [Online 2013 accessed: January 2020]. https://www.ecouncil.ae/PublicationsEn/information-security-policy-v2, property=pdf.pdf.

Abu Dhabi Systems and Information Center, Abu Dhabi Digital Authority. [Online accessed: June, 1 2020]. https://adsic.abudhabi.ae/.

Ali, Syed Mubashir, 2014. Integration of information security essential controls into information technology infrastructure library-A proposed framework. Int. J. Appl. 4 (1).

Anton, A.I., Earp, J.B., 2004. A requirements taxonomy for reducing web site privacy vulnerabilities. Requirem. Eng. 9 (3), 169–185.

Barafort, Béatrix, Mesquida, Antoni-Lluís, Mas, Antònia, 2017. How to Elicit Processes for an ISO-Based Integrated Risk Management Process Reference Model in IT Settings? In: European Conference on Software Process Improvement. Springer, Cham, pp. 43–57.

Beckers, Kristian, Heisel, Maritta, Solhaug, Bjørnar, Stølen, Ketil, 2014. ISMS-CORAS: A structured method for establishing an ISO 27001 compliant information security management system. In: Engineering Secure Future Internet Services and Systems. Springer International Publishing, pp. 315–344.

Cavusoglu, H., Cavusoglu, H., Son, J.-Y., Benbasat, I., Jun. 2015. Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources. Inf. Manage. 52 (4), 385–400.

Crespo, L., Wanner, B., Ghernaouti, S., 2018. Cybersecurity Capacity Building: A Swiss Approach. In: Bartsch, M., Frey, S. (Eds.), Cybersecurity Best Practices. Springer Vieweg, Wiesbaden.

Cybersecurity Index of Indices, 2015. Published by ABI Research. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Index_of_Indices_GCI.pdf.

Dubai Cyber Security Strategy DESC 2020 Dubai UAE. https://desc.dubai.ae/.

Dzombeta, S., Stantchev, V., Colomo-Palacios, R., Brandis, K., Haufe, K., Jul. 2014. Governance of Cloud Computing Services for the Life Sciences. IT Prof. 16 (4), 30–37.

Education in the UAE. Ministry of Education. [Online accessed: December 2016]. Retrieved from: http://www.moe.gov.ae/English/Pages/UAE/UaeEdu.aspx.

Elahi, G., 2009. Security requirements engineering: state of the art and practice and challenges. http://www.cs.utoronto.ca/~gelahi/Depth.

Erin, Olayinka Adedayo, Kolawole, Adebola Daniel, Noah, Abdurafiu Olaiya, 2020. Risk governance and cybercrime: the hierarchical regression approach. Fut. Bus. J. 6, 1–15.

Fabian, B., Gurses, S., Heisel, M., Santen, T., Schmidt, H., 2010. A comparison of security requirements engineering methods. Requirem. Eng. 15 (1), 7–40.

Gadyatskaya, O., Harpes, C., Mauw, S., Muller, C., Muller, S., 2016. June). Bridging two worlds: reconciling practical risk assessment methodologies with theory of attack trees. In: International Workshop on Graphical Models for Security. Springer, Cham, pp. 80–93.

Global Cybersecurity Agenda (GCA). A Framework for International Cooperation in Cybersecurity [Online]. Available: https://www.intgovforum.org/Substantive_2nd_IGF/ITU_GCA_E.pdf [accessed: June. 1, 2020].

Haufe, Knut, Colomo-Palacios, Ricardo, Dzombeta, Srdan, Brandis, Knud, Stantchev, Vladimir, 2016. Security management standards: a mapping. Procedia Comput. Sci. 100, 755–761.

Hohmann, M., Pirang, A., Benner, T., 2017. Advancing Cybersecurity Capacity Building: Implementing a Principle-Based Approach. Global Public Policy Institute. http://www.gppi.net/publications/data-technology-politics/article/advancing-cybersecurity-capacity-building-implementing-a-principle-based-approach/2017.

Humphreys, E., 2016. Implementing the ISO/IEC 27001: ISMS Standard. A book published by Artech House.

Improving Critical Infrastructure Cybersecurity, Executive Order 13636. Preliminary Cybersecurity Framework. NIST, available at: https://www.nist.gov/system/files/documents/itl/preliminary-cybersecurity-framework.pdf.

International Organization for Standardisation and International Electrotechnical Commission, ISO/IEC 27002:2013. Geneva, 2013.

ISO/IEC 27002:2013(E): Information technology Security techniques — Code of practice of information security controls, 2013. Second ed. Switzerland.

ISO/IEC 27001:2013(E): Information technology Security techniques — Information security management systems — Requirements, 2013. Second ed. Switzerland.

ISO/IEC 27001 – Information Security Management. ISO standards [Online accessed Retrieved from: December 2016.

Jazri, H., Zakaria, O., Chikohora, E., "Measuring Cybersecurity Wellness Index of Critical Organisations, 2018. IST-Africa Week Conference (IST-Africa). Gaborone 2018, 1–8.

Jennex, Murray Eugene, Durcikova, Alexandra, 2020. Knowledge Systems and Risk Management: Towards a Risk and Threat Assessment Framework. In: Current Issues and Trends in Knowledge Management, Discovery, and Transfer. IGI Global, pp. 367–385.

Layton, Timothy P., 2016. Information Security: Design, implementation, measurement, and compliance. CRC Press.

Mirtsch, Mona, Kinne, Jan, Blind, Knut, 2020. Exploring the Adoption of the International Information Security Management System Standard ISO/IEC 27001: A Web Mining-Based Analysis. IEEE Trans. Eng. Manage.

Peltier, Thomas R., 2016. Information Security Policies, Procedures, and Standards: guidelines for effective information security management. CRC Press.

Real security in a variety world, 2015. NESA UAE Information Assurance Standards. [Online accessed: January 2020]. Retrieved from: https://www.dionach.com/blog/nesa-uae-information-assurance-standards.

Schmid, M., Pape, S., 2019, June. A Structured Comparison of the Corporate Information Security Maturity Level. In: IFIP International Conference on ICT Systems Security and Privacy Protection. Springer, Cham, pp. 223–237.

Schmitz, C., Pape, S., 2020. LiSRA: lightweight security risk assessment for decision support in information security. Comput. Security 90, 101656.

Shah, M., 2014. Impact of management information systems (MIS) on school administration: What the literature says. Procedia-Soc. Behav. Sci. 116, 2799–2804.

Souag, A., Salinesi, C., Mazo, R., Comyn-Wattiau, I., 2015. A security ontology for security requirements elicitation. In: International symposium on engineering secure software and systems, March 4–6.

Souag, Amina, Mazo, Raúl, Salinesi, Camille, Comyn-Wattiau, Isabelle, 2016. Reusable knowledge in security requirements engineering: a systematic mapping study. Requirem. Eng. 21 (2), 251–283.

Dubai Electronic Security Strategy. Dubai Electronic Security Center, Version 2.0, 2017. All rights reserved. http://csc.dubai.ae/res/wp-content/uploads/DCSS-EN.pdf.

Watkins, L.A., Hurley, J.S., 2015. Cyber maturity as measured by scientific-based risk metrics. J. Inform. Warfare 14 (3), 57–65.

Williams, Susan P., Hardy, Catherine A., Holgate, Janine A., 2013. Information security governance practices in critical infrastructure organizations: A socio-technical and institutional logic perspective. Electron. Mark. 23 (4), 341–354.