Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.18576/amis/200117

Data Governance and Security Assurance in ISO27001 Programs: A Context Study on Quality and Compliance in Middle Eastern Organizations

S. A. Badawi[1,*], *M. Takruri*[2], *K. Salameh*[3], *D. Guessoum*[4], *I. ElBadawi*[5], *and Aws Al-Qaisi*[2]

[1] Department of Autonomous Systems, Faculty of Artificial Intelligence, Al-Balqa Applied University, Al-Salt 19117, Jordan
[2] College of Engineering and Technology, American University of The Middle East, Egaila 54200, Kuwait
[3] Advanced Technology and Artificial Intelligence Center (ATAIC), American University of Ras Al Khaimah, Ras Al Khaimah 72603, United Arab Emirates
[4] Electrical Engineering Department, École de Technologie Supérieure, Montreal, QC H3C 1K3, Canada
[5] Industrial Engineering Department, College of Engineering, University of Ha'il, Ha'il 81481, Saudi Arabia

Received: 06 Sep. 2025, Revised: 22 Nov. 2025, Accepted: 27 Dec. 2025
Published online: 1 Jan. 2026

Abstract: The rapid digital revolution in the Middle East has increased organizational awareness of information security; nonetheless, significant inconsistencies persist in the implementation and governance of ISO 27001 controls. This research assesses the quality and maturity of security programs within regional organizations by analyzing survey data from diverse industries and organizational sizes, while comparing the results to global benchmarks. The findings reveal a clear disparity: technological safeguards, encompassing password management, data center access, and network defense, are relatively sophisticated, while governance-focused measures, including records management, telework policies, and employee awareness training, are growing. Medium-sized organizations are the ones implementing controls, while educational institutions demonstrate excellence in terms of resources and governance. Still, the question is "are they following a systematic way to build and manage information security systems that ensure the effectiveness of their information security program?" Unfortunately, until now, different organizations have been approaching information security management in various ways. When they implement it, they don't have a clear idea about the quality of the implemented Information Security investment. In this paper, we have surveyed the quality of controls implemented in information security programs in the Middle East and analyzed the results to target optimization in their future information security investments.

Keywords: ISMS, information Security, ISO 27001, Risk Management, SABZA, Enterprise architecture, Maturity Model Assessment, NIST, Six Sigma, benefit analysis.

1 Introduction

Today's organizations want effective information security systems, especially in the wake of the recent financial crisis. That leads organizations to be industry-aware of targeting cost reduction, risk optimization, and optimal value management, and eventually leads the industry to review the quality of information security controls implemented critically. In this paper, we investigate whether organizations are following an optimal systematic approach to building and managing their information security investments, and whether they are aware of the quality of the controls implemented and are targeting improvements to enhance their effectiveness. Unfortunately, to date, organizations have not gone towards information security management in a consistent and optimized manner; in addition to the fact that when they implement it, they do not monitor its effectiveness after implementation. We have conducted a survey that targets measuring the quality of the implemented controls in the organizations in Middle East, the survey is based on ISO 27001 standard controls, after conducting the study we have analyzed the quality of the implemented controls, by doing analysis similar to previous study results targeting to be more effective in building their information security controls as well as to measure the

[*] Corresponding author e-mail: sufian.badawi@bau.edu.jo

quality of the implementation, in addition to targeting optimizing it in their future information security investments. We believe this study will help organizations gain insight into the quality and effectiveness of their security investments by reanalyzing their implemented programs and conducting a similar analysis to identify areas for improvement.
The rest of the paper is organized as follows: in Section 2 we have introduced in details literature and the related work about quality and adequate information security controls. In section 3 we have gone through the survey methodology, design, and participation analysis. While in Section 4 The results analysis is illustrated, the study is showing effect on the firm policy on the related control implementation, then the highest quality ten controls, the lowest quality team controls and the effect of organization size on the quality, the impact of industry type of organization on the quality of the implementation of Information security controls, then we have analyzed the quality of the implementation effect on the number of reported incidents, the paper is ended up by the conclusion section that is going through some further work to be done in this direction.

2 Related Work

Technology is changing rapidly, and managing information security with this rapid change is a great challenge, especially when information is growing tremendously. This increases the challenge of managing the risks associated with information security in organizations if they do not focus on the quality and effectiveness of its implementation. Nowadays, information security management has emerged in various forms, including standards, frameworks, and methodologies such as ISO 27001:2013, COBIT 5, SABSA, and NIST SP 800-30. Despite the multiple frameworks for managing information security, there is still a need for further studies that focus on the quality of implementation rather than on whether controls exist. In the [1] study, ISO 27001 is adopted, but it faces many organizational adaptation and implementation challenges. It shows that even though the standard provides a well-defined structure, many users don't get the full benefits. [2] 's initial research on information governance remains highly pertinent today, as he argues that governance must be addressed at the upper echelons and that the absence of an organizational framework delineating data ownership is critical to its implementation. [3] highlighted that information security governance (ISG) should be viewed as a comprehensive, strategic discipline encompassing corporate governance, stakeholder engagement, and process improvement, rather than solely as technical compliance. While Bena confirmed that legacy governance frameworks are inherently inefficient for real-time, unstructured, and continuously streaming data from sources such as IoT sensor networks, social media feeds, and automated business processes [4]. They have addressed the difficulties arising from the inherent characteristics of data produced by intelligent systems and concluded that governance must be reconsidered as an integrated component within the data pipeline. To solve these issues, new frameworks are proposed. A study by [5] confirms that effective BDG must be flexible, scalable, and adhere to specific legal standards across industries. The lack of unified BDG standards makes it hard for different stakeholders within the same organization to work consistently. Wade H. Baker and Linda Wallace conducted a survey study that quantitatively shows the relationship between the quality of implemented controls and factors such as the strength of management policy, organization size, industry type, and their effects on reported security incidents. They stated that organizations may adopt their model to measure the quality of their implemented controls at minimal cost, and that researchers can use it to identify a balance among management, operational, and technical controls to achieve a holistic approach [6]. A case study conducted in Turkey [7]. Introduced a collaborative risk management method where a proactive risk assessment is a key approach that enables organizations to implement an information security management system effectively. By focusing on the scope and determining and modeling the process, the proposed method does not emphasize technical items such as servers and software; rather, it accents IT processes. This proposed method is ideal for use in the Middle East context because of the similarities between the Region and Turkey in terms of legislation and cultural environment. This method is suitable for an environment that lacks sufficient security-related legislation, top management support, or sufficient information security professionals. Traditionally, a great deal of attention is focused on efforts to address risks affecting business information from an IT infrastructure perspective. Currently, there is a consensus on Big Data Governance (BDG) that conventional data management frameworks are insufficient to accommodate the scale of contemporary data ecosystems. Recent literature has focused on the technical architecture for governance, highlighting the need for embedded controls that operate on streaming data [8], [9] and [10]. Big Data Governance encounters three main challenges: (1) a lack of standardized but flexible implementation frameworks,(2) deep organizational and cultural barriers, and (3) a lack of standardized but flexible implementation frameworks [2] and [5]. These challenges are addressed in recent studies, such as those by [4] and [5], which suggest practical solutions. In 2007, a survey conducted on 28 enterprises from different industries in Korea that acquired ISMS certification between 2002 and 2005 resulted in a suggested reference model for conducting self-assessment and measuring the maturity level of the ISMS implemented controls by referring to a lesson learned database that includes the defects an organization may fall on during implementation. The reference model for the self-assessment of the ISMS completeness is based on the items vs. frequency of defects [11]. A good point in this study is that it measures the defects to void rather than prescribing best practices to follow, which is similar to the way of Hudhaifa Ibn ul Yaman, who used to ask the Prophet Muhammad, PBUH, about the evil deeds to avoid. At the same time, people used to ask about the good deeds to follow [12], although this study is suitable for implementation in the Middle East. Still, it is measuring completeness rather than the quality of the ISMS implementation. T. Delimani et al conducted surveys in the industry. Regarding ISMS implementation, they reviewed related publications, compared and analyzed the results, and developed a comprehensive view of the current information security landscape. In addition to listing a set of critical information security issues that were still not addressed and another set that were being overlooked, they recommended additional efforts to analyze the gap between the regulatory issues and the technical implementation [13]. J. Chaulaa et al proposed an Information Security Assurance framework for evaluating ISMS that is based on the standard criteria (CC), which is an established method for security functions identification, assurance levels classification, and development of Protection Profiles. The proposed framework helps create the balance required for a comprehensive approach view. It considers factors related to non-technical assurance, the use of Protection Profiles, and the use of security metrics in the information assurance process [14]. In [15], the adoption of ISO 27001 in the Middle East is analyzed in depth. The authors found that legal and cultural obstacles prevent its implementation, and the aforementioned ISO 27001 governance system does not fully cover control assurance throughout the data lifecycle, as required by recent approaches that are more focused on data in big data governance scenarios rather than on infrastructure or terminals. Furthermore, [16]. Study the impact of fragmenting the global data governance frameworks and the challenges faced by organizations when they adhere to multiple governance standards. This research promotes the data-centric models, in which governance and security policies are linked with the data throughout its lifecycle. Other research addresses the socio-technical challenges, in which the success of any governance initiative depends on strong organizational structures, clear data ownership models, and a culture that prioritizes data quality and ethical use [17] and [18]. Despite advancements in data governance systems research, there remain many opportunities for future research and for validating the proposed frameworks in large-scale, real-world contexts through empirical case studies. Future research shall focus on the creation and evaluation of implementation roadmaps and maturity models for these frameworks [17]. There is also a need for new governance tools that can automatically verify the compliance of AI and machine learning models—ensuring fairness and accountability [19] and [20].

Table 1: Questions classification in the survey

NIST Security Control Domains	Count Of Controls
Antivirus Software	2
Business Continuity/Incident Response	2
BYOD	5
Compliance	6
Employee training and awareness	1
Help desk/IT support training	1
Management Policy -org. of IS	6
Monitoring and logging	4
Network Security Management	6
Password and access control	8
Physical security	7
Remote access security	1
Risk Management	5
Sensitive Data Handling and Protection	4
Staff hiring and termination	1
System-Level Security	1
Technical documentation	1
Testing and review	6
Total	67

Finally, the growing interest in decentralized data architectures opens up a new area for BDG. This means that new ways must be found to manage and govern data that is spread out over an extensive network of devices and is not stored in one place.

3 Methodology

This work emphases on big data governance level of implementation in the Middle Eastern firms. The study is survey based refereed to ISO27001 standard controls to design the survey. Followed by analysing the impact of the strong policy on the related implemented control, then the highest and the lowest ten controls implemented in the organizations, and finally studying the impact of the industry type of organization, and the quality of the implementation effect on the number of reported incidents.

To assess the quality level of ISMS implementation in Middle East organizations, we have designed a survey. The survey is prepared in accordance with ISO 27001:2011 and NIST 800-53 publications, and the controls are classified into technical, operational, and management categories. The total number of controls is 67, covering the NIST domains below.

We have prepared the survey online, and the survey link has been sent to participants via email. We requested their participation and encouraged them by informing them that responses would be anonymous and used solely for academic purposes. The survey remains online for 1 month, with several follow-ups and reminders to encourage participation. A set of interviews was

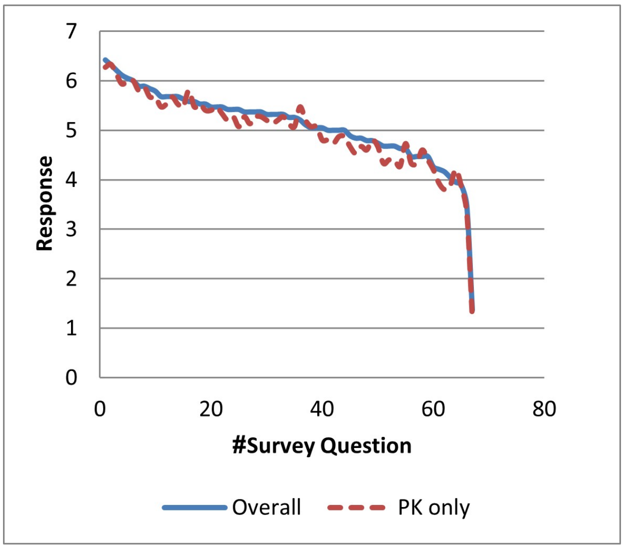


Fig. 1: Middle East Organization Responses vs. Overall Responses

conducted, the survey was completed manually for 5 participants, and the results were entered into the online survey. The respondents included a CISO, a CIO, an IT governance consultant, a security specialist, IT operations members, and a process engineer. Of 27 responses, 21 were from the Middle East, one from the USA, one from Saudi Arabia, and two from the UAE. As our targets are Middle East organizations, we have discarded the six responses from outside the Middle East and excluded partially filled surveys, resulting in 15 Middle East responses. Middle East responses have been isolated from those outside the Region, and the trend in overall responses closely matches that in the Middle East. This is because the sample of outside participants is tiny compared to the reactions from the Middle East. As the trend remains the same, the analysis below considers all 19 responses, including 15 Middle East companies and four from outside, forming a uniform sample. Figure 1 shows that there were 27 responses in all. Twenty-one of them came from the Middle East. The research focused only on organizations in the Middle East; therefore, responses from outside the Region were not included. We removed the partially completed questions, leaving us with 15 genuine replies from the Middle East. The patterns in the complete response set were surprisingly similar to those in the Middle East replies alone. We included 19 responses in the study since the sample size from outside the Middle East was small and the response patterns were similar. Of these, 15 were from Middle Eastern organizations and four were from outside the region, resulting in a relatively homogeneous sample. A significant 83% of the participants were employed in the telecommunications, IT, and government sectors in the Middle East. The breakdown is as follows: IT (47.06%), government (11.76%), telecommunications (29.41%), services (5.68%), and other (5.88%). This indicates that our study comprised 50% of the Middle East's telecom from Middle Eastern enterprises (red dashed line) and the total number of replies (blue solid line) for 67 surveyed security measures. Both response sets are shown on a scale from 0 to 7, with higher scores indicating the controls listed from least to most implemented according to the ISO 27001 standard. The visual link between Middle Eastern replies and overall responses shows that organizations in the area usually follow global norms. The blue global trend aligns with the red dashed line across most survey questions. This suggests that Middle Eastern businesses don't fare significantly better or worse than the global average. This demonstrates that more and more areas are adopting international standards such as ISO 27001. Globalization, compliance standards, and the work of regional regulators are all to blame. There are some modest variances in the middle half of the survey (items 20–45), but the overall alignment is solid. In this context, Middle Eastern organizations are not as strong as the global average in several areas, including employee education, policy enforcement, and third-party contract safety. These areas were already highlighted as regional weaknesses in past evaluations. On the other hand, there have been occasional gains in controls related to technological safeguards, such as password management, antivirus software, and access security. In these areas, companies in the Middle East appear to be on level with or somewhat better than their worldwide counterparts. It is noticed that 83% of the participants are from Telecom, IT, and government sectors in the Middle East. The breakdown of participants is: IT 47.06%, government 11.76%, telecommunication 29.41%, services 5.88%, and others 5.88%. This shows that the participating telecom organizations account for 50% of the telecom organizations in the Middle East. The percentages of participating organizations in the survey according to industry type is illustrated in Figure 2. The pie chart shows that 70% of them are either from the telecommunication or the IT industry organizations.

The scale used for the survey is 1=Not implemented, 2=poorly implemented, 3=Unsure, 4=below average, 5=average, 6=above average, 7=advanced

4 Results

Targeting the quality of the implemented information security controls always yields more precise facts. For example, using the above responses' weights, we can calculate the average rating of the control quality using equations (1) and (2):

$$ControlQualityRate = \sum_{k=1}^{n} \frac{\sum_{i=1}^{N} Count(Pitickeda_k)}{N} \quad (1)$$

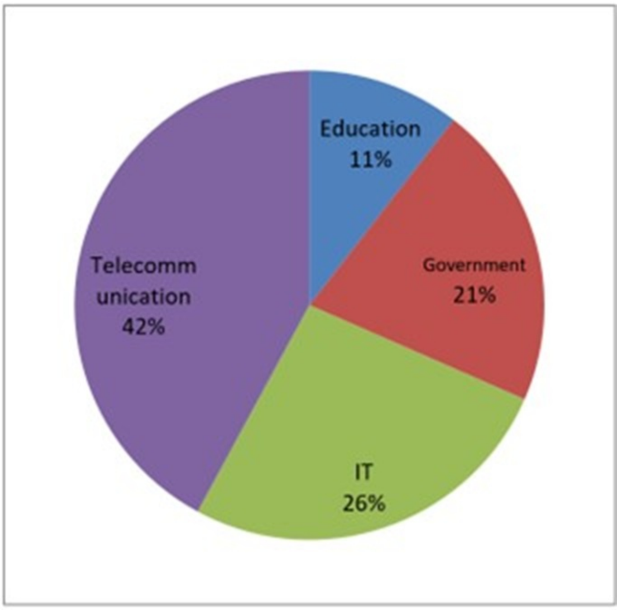


Fig. 2: Industry Types of Participant's Orgs.

Where:
n Number of multiple choices in the control question.
N Number of survey responses.
Count(Pi ticked a_k) = Response frequency.
a_k=is a constant of weight given to each response, where: (1=Not implemented,
2=poorly implemented,
3=Unsure, 4=below average,
5=average
, 6=above average,
7=advanced).

$$ControlQualityIndex = (ControlQualityRate)/100 \quad (2)$$

4.1 Controls with the Highest Quality implementation

The survey results show the following top 10 high-quality implementation controls sorted from highest to lowest, as illustrated in Figure 3, while the lowest ten high-quality implementation controls, are illustrated in Figure 4:

Figure 3 is showing clearly 10 implemented controls are related to controls related to password management, authentication and access control and that is showing a harmony of exemplary quality implementation of information security management policy at top management level then the existence of access control and authorization policy and then set of operational and technical controls and mechanisms that are implementing a good quality level and this emphases the notion of the holistic approach is highly effecting the quality of the implemented controls and creates a strong balance in having successful implementation of the controls,

Figure 5 shows that as whole the holistic view of access control management the survey findings from different angles are showing that whenever we have strong controls at management, operational and technical level then we expect to have a higher quality in the implemented controls and those controls empower each other in the implementation and create a higher quality level with the balance that is made between the three types of controls.

4.2 The Role of Policy in Quality

"Successful Password Management Program" in Figures 6 and 7 is the highest implementation quality control. The main reason could be of the existence of a supporting password management policy is a famous practice across organizations, in addition to the fact that it is normally supported by management. The existence of approved information security management policy and the survey figures show that the quality level of the implementation of the technical controls and operational controls are normally increased when it is related to policies that are exist and are supported by the top management's information security management policy.

The above facts show a strong correlation with other factors, that 9 of the top 10 quality controls are related to access control and authentication, which makes the password management

control the highest quality in implementation, and a strange finding that those organizations that record those quality results have another strong control, which is "Existence of strong Password Policy". As a whole, the survey findings from different angles show that whenever we have strong controls at the management, operational, and technical levels, we expect higher-quality controls to be implemented. Those controls empower each other during implementation and create a higher quality level through the balance among the three types of controls.

Then the survey results show the lowest 10 qualities implemented controls sorted from highest to lowest, as illustrated in Figure 3 The lowest ten controls composed of eight management controls, two of them are operational controls 9, and one of them is a technical control and this shows that there is still a need in Middle East organizations information management setup those ten lowest controls are indicators that there should be an information security officer and there should be an information security policies (to manage digital identity or to have an Information security record management and to have the security requirement in any IT tender and to manage separate testing function from development function, to have a media sensation policy and to be linked with local security groups and manage PYOD devices and telework) the quality of implementation all

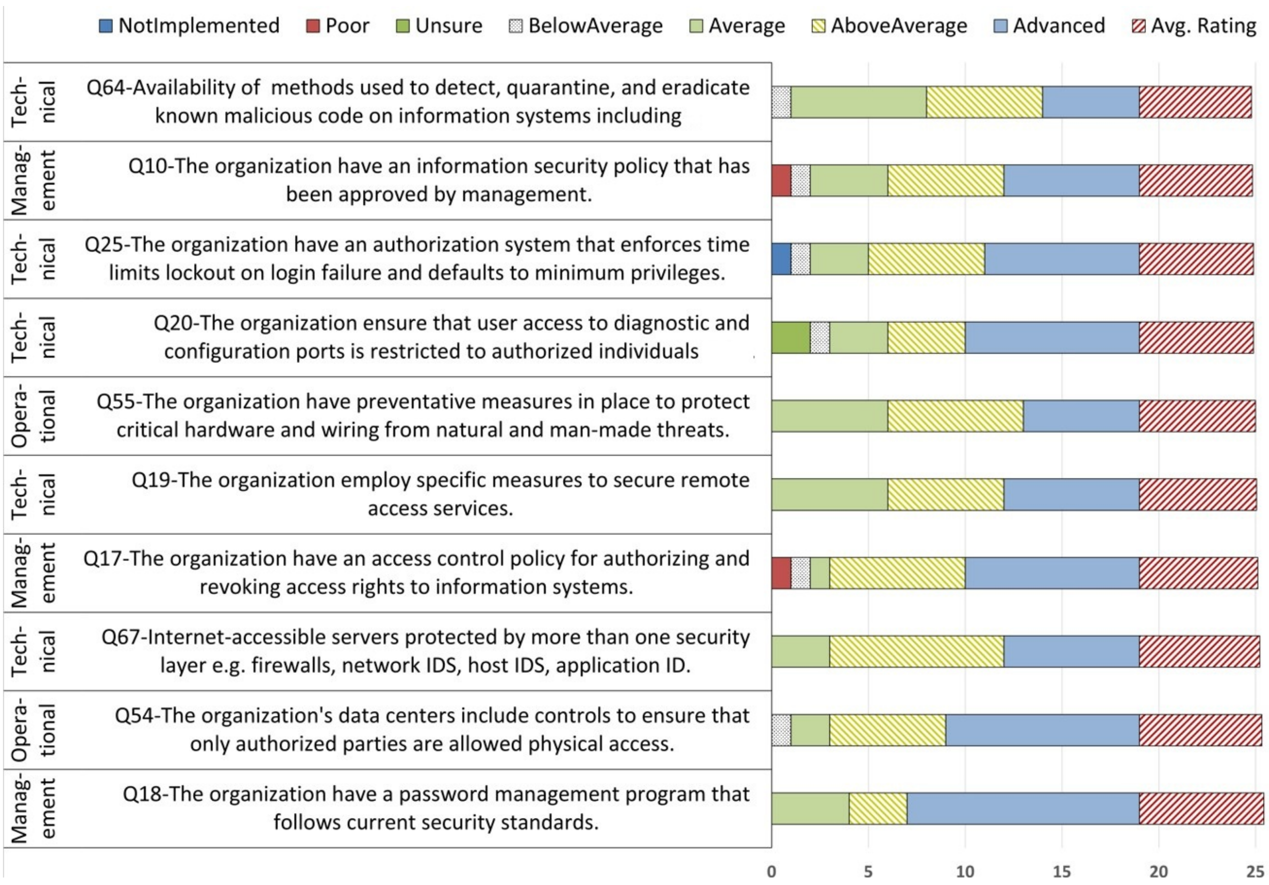


Fig. 3: Controls of highest Implementation Quality Rating.

on those controls is needing a focus to be improved in Middle East organizations.

4.2.1 The Role of Organization Size in Quality

The result of analyzing the effect of the organization size on the quality of the implemented controls shows that the organization size affects the quality of the implemented controls, as it is clear from participated organizations in Figure 8 vs the organization size impact on the implemented controls, Figure 9 shows that the best implementation for each control is in the medium size organizations:

Although in the Previous studies it was showing that: “The quality of the implementation is higher in the bigger organizations” with 25% deviation than this rule in 2007 survey study [6], in this survey results here the findings are the medium size organizations in Middle East have higher quality implemented information systems controls than large or small organizations for 69% of the controls while 31% the larger the organization is, the higher is the quality of the implementation. Table 2 and Figure 9 is showing the phenomena, These differences match previous research findings when the balance and maturity is there in implemented controls while apparently medium size organizations in Middle East has managed to create this balance between information systems management policy, domain specific policies and the needed operational or technical controls to achieve better quality implementation, and another factor is playing an important role here and that is in large organizations the cultural shift in the management, operational and technical practices is higher in large organizations that lead to medium size organizations to achieve this cultural shift easily compared to the big size organizations,

The major domains are, most importantly, IS risk management policy, business continuity/incident response, BYOD, compliance, employees’ awareness, network security management, and physical security. Another emphasis we want to point out is that the square footage of the network’s physical locations and the network’s complexity are higher with larger organization size. We’d expect large firms to put more effort into streamlining a higher-quality implementation across the three levels (management controls, operational controls, and technical controls).

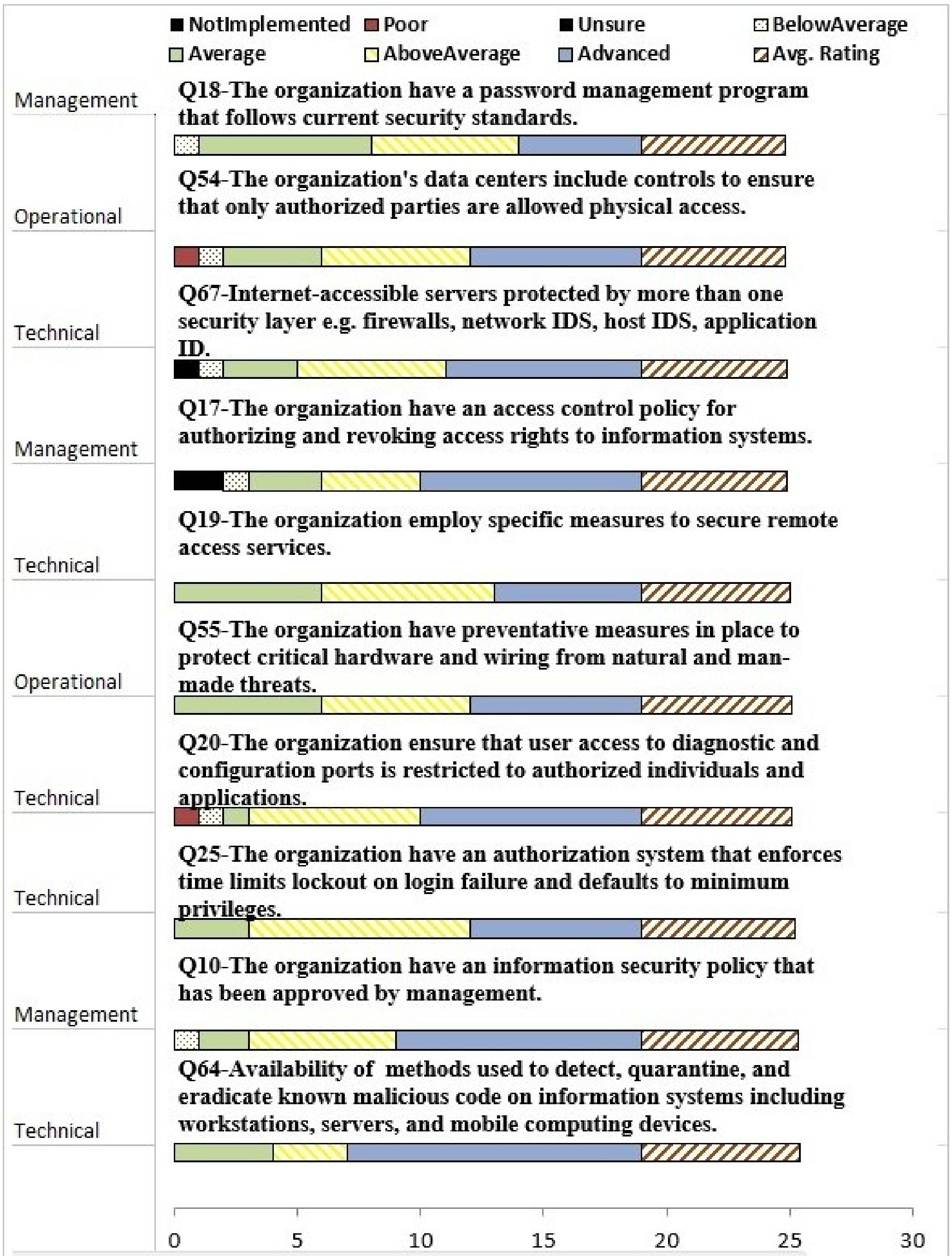


Fig. 4: Controls of lowest Implementation Quality Rating.

Large organizations' Quality is higher than medium organizations' for 31% of the controls, while Medium organizations have a higher quality level than the large ones for 69% of the controls.

Large organizations' Quality is higher than medium organizations' for 31% of the controls Count Of Controls Medium organizations have a higher quality level than the large ones for 69% of the controls. Antivirus Software 2 2 Business Continuity/Incident Response 5 BYOD 6 Compliance 1 Employee training and awareness Help desk/IT support training 1 6 Management Policy -org. of IS Monitoring and logging 4 Network Security Management 6 Password and access control 8 7 Physical security 1 Remote access security 5 Risk Management 4

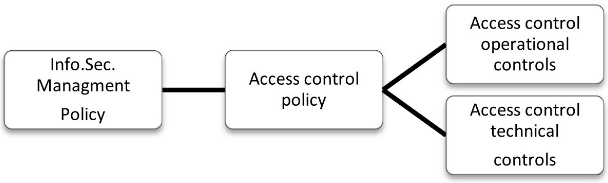

Info.Sec. Managment Policy
Access control policy
Access control operational controls
Access control technical controls

Fig. 5: Achieving high-quality results holistically.

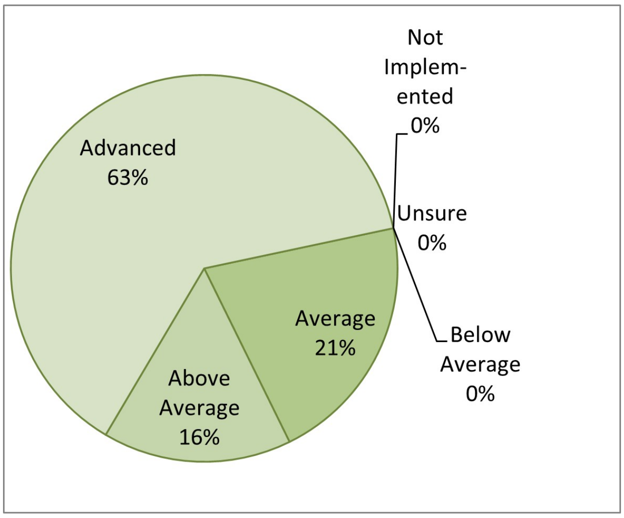


Fig. 6: Highest Quality implemented control "(91%) Successful Password Management Program".

Sensitive Data Handling and Protection 1 Staff hiring and termination 1 System-Level Security 1 Technical documentation 6 Testing and review 31% 67 69%

4.3 The Role of the Organization Industry in Quality

The result of analyzing the effect of the organization industry on the quality of the implemented controls shows that the size affects the quality of the implemented control, as it is clear from Figure 10.

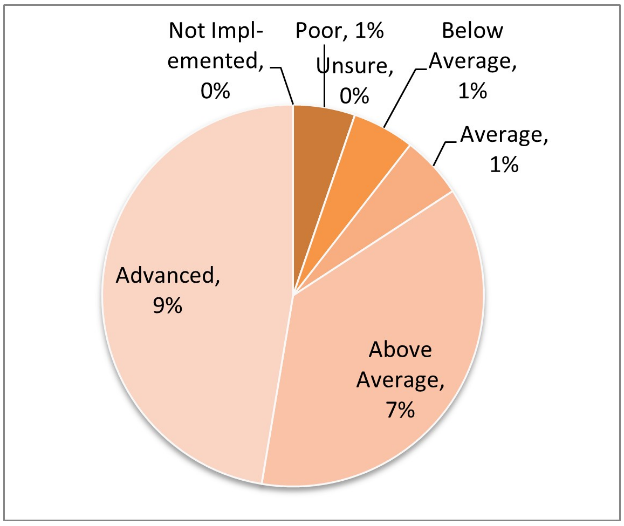


Fig. 7: Existence of Strong password Policy Control Caused Password Management Controls Stronger.

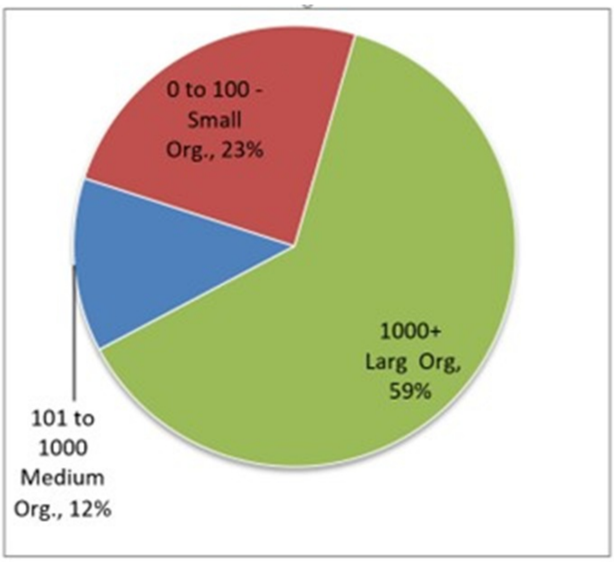


Fig. 8: Participated Organization Size by number of IT Systems.

Figure 10 shows that government organizations in Middle East has higher quality implemented controls for all categories except for risk management and testing and review categories compared to education, telecom or IT, the reason could be government organizations participated in the survey are sensitive ones that information security is of high value to them, that's why they score high mark, another obvious result that the lowest implementations quality are in the education industry due to low allocated budgeting to this sector in Middle East, and education industry needs a comprehensive program to protect the confidentiality of their data from being breached by outsiders and effect the intuition rights or individual rights, IT industry in Middle East are better than government industry in risk management and testing and review and this is obvious as IT projects delivered after testing and review for the offered products and has better awareness about risk management.

Surprisingly, the telecom field is the second-lowest IS quality industry and still needs improvement in the quality of implemented security programs, as technology

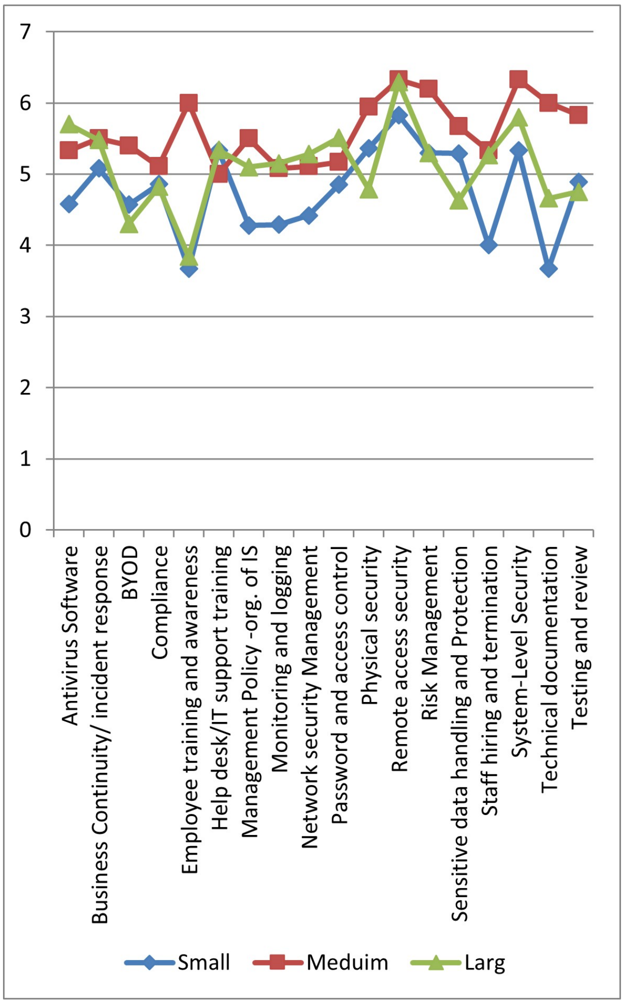


Fig. 9: Organization size effect on the quality of the control implementation.

Table 2: Organization Size vs. quality of the implemented controls

Large organizations implemented controls	Count	Medium organizations implemented controls
Antivirus Software	2	
	2	Business Continuity/Incident Response
	5	BYOD
	6	Compliance
	1	Employee training and awareness
Help desk/IT support training	1	
	6	Management Policy - org. of IS
Monitoring and logging	4	
Network Security Management	6	
Password and access control	8	
	7	Physical security
	1	Remote access security
	5	Risk Management
	4	Sensitive Data Handling and Protection
	1	Staff hiring and termination
	1	System-Level Security
	1	Technical documentation
	6	Testing and review
31%	67	69%

is emerging rapidly, and the need to protect new ICT investments is exceptionally high.

By looking at the IT industry in the Middle East participants have shown a good quality level of implementation in this sector in the Middle East.

5 Discussion

The survey results are showing that organizations in the Middle East are improving in targeting the quality of the ISMS implementations, and compared to similar previous studies, Middle East implemented ISMS programs are advanced in considering password management, authentication, and management policy alignment with the implemented controls; however, there is still a need for efforts to create balance in the implementation between management, operational, and technical controls to achieve a more holistic implementation approach, resulting in higher-quality information security practices.

The survey has shown the importance of having a holistic view balance in managing the information security in Middle East organization, and whenever there is a weakness in this balance it effects the quality of the implemented control and this shows that the security is the responsibility of all levels in the organization, from the top management commitment and support represented to middle management to operations and technical implementations and this spread in the quality of each control there should be operational/technical controls, technical control policy and supported by the information security policy, in Middle East environment there are areas of extra investigation that needs to be analyzed whether the big organizations need

more time to achieve the optimal level of quality of implementation than medium organizations as extra awareness, culture change and cost efforts are required in order to create the balance of the holistic view of the implemented information security controls compared to

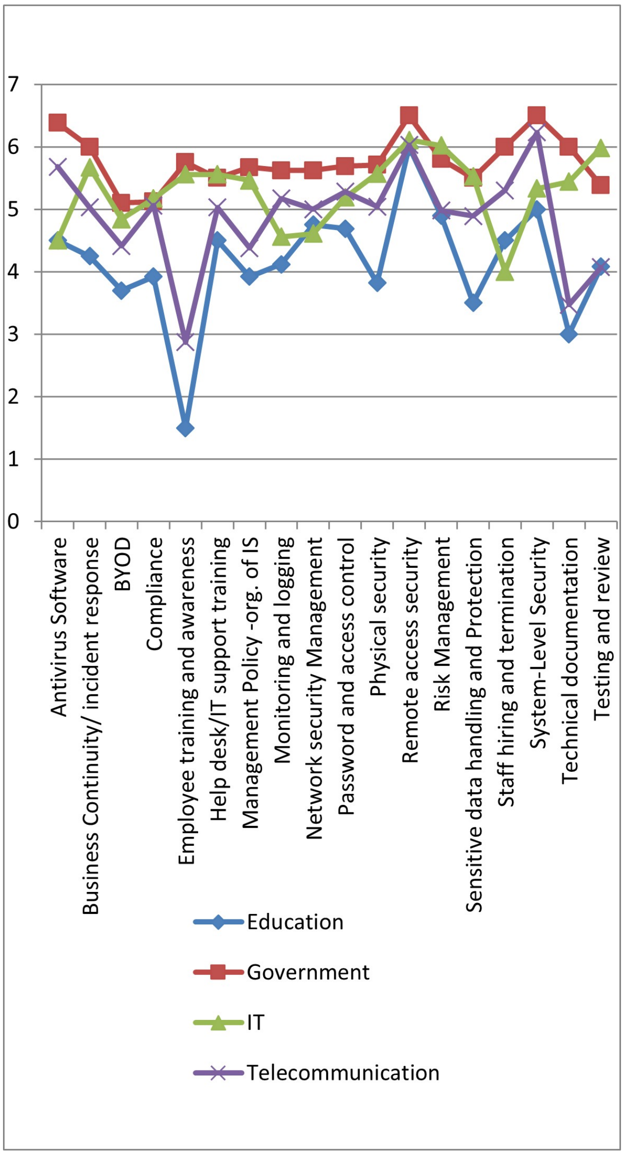


Fig. 10: Organization Industry Effect on the Quality of the Control Implementation.

the medium organizations, and why Telecom field is still needs extra efforts compared to the IT industry, those are some areas of further investigation are still there to find a clear answer in Middle East information security implementations.

6 Conclusion

This study critically assessed ISO 27001 information security procedures in Middle Eastern enterprises, juxtaposing them with worldwide norms and big data governance frameworks. The analysis findings showed significant improvement, but there are still some issues that need to be addressed. This is because of quality control checks, the size of the company, industry requirements, and demographic studies. It seems like a lot of people use technology to keep networks safe, manage passwords, and access data centers, and it works well for all of these. Companies want KPIs that are genuine, easy to understand, and easy to compare against the ISO 27001 certification standards. This tendency is supported by the fact that most firms have rigorous password policies. The inquiry also revealed issues with overall governance, cultural acceptability, and data tracking over time. There were never enough laws to preserve records, train people, control third-party risk, and ensure telework was safe. These findings indicate the presence of global issues, particularly in regions where governance frameworks and organizational cultures are still under development. The difference between technology maturity and governance integration shows that many companies view ISO 27001 primarily as a means to meet requirements rather than as a comprehensive management system. Comparative assessments based on organizational size and sector further support these results. Medium-sized businesses are better at implementing ISO 27001 controls because they can strike a balance between flexibility and sufficient resources. The finest institutions are government ones because regulators keep an eye on them. IT and telecommunications are the greatest at protecting technology, but they aren't as effective at following cultural and compliance rules. The government isn't functioning well, and education isn't going well because it doesn't have enough money. This makes it a dangerous profession that requires expert help. According to a global assessment, organizations in the Middle East are still in line with the worldwide average. This signifies that the region is neither ahead nor behind. But the fact that governance and training aren't functioning properly provides regional governments and organizations with many opportunities to improve. These findings demonstrate that companies in the Middle East need to shift their security posture from fragmented, technology-focused to integrated, controlled. As digital ecosystems become more complex, implementing ISO 27001, combined with big data governance principles such as continuous monitoring, stakeholder involvement, and lifecycle stewardship, can ensure you remain compliant and strong. Further research may investigate regional cross-national discrepancies, legislative modifications, and the amalgamation of ISO 27001 with nascent ethical frameworks for data governance and artificial intelligence. In the digital age, information security measures must be strengthened to protect the integrity, privacy, and availability of data. This involves more technical help, greater alignment of strategies, changes in culture, and new methods of doing things.

Data Availability

Not Applicable.

Acknowledgments

The authors express their gratitude to the anonymous reviewers for their valuable suggestions. The authors also extend their sincere thanks and appreciation to both the American University of Ras Al Khaimah and the Shaikh Muhammad Bin Rashid Smart Learning Program Establishment, as well as Al-Balqa Applied University for their ultimate support to the research in artificial intelligence, robotics and big data.

Funding

This research was funded by the Muhammad bin Rashid Smart Learning Program. We gratefully acknowledge their financial support, which has been instrumental in the successful completion of this study. Their contributions have enabled us to conduct thorough research and prepare this article. We extend our sincere thanks for their unwavering support and commitment to advancing smart learning initiatives.

Disclosure of interest

None of the authors have any conflicts of interest to declare.

Author Contributions

Must include all authors, identified by initials, for example: "S. B., M. T., K. S., M. A., N. M., I. E., N. A.; methodology, S. B., M. T., K. S., M. A., N. M., I. E., N. A.; software, S. B., I. E.; validation, S. B., M. T., K. S., M. A., N. M., I. E., N. A.; formal analysis, S. B., M. T., K. S., M. A., N. M., I. E., N. A.; investigation, S. B., M. T., K. S., M. A., N. M., I. E., N. A.; resources, S. B., M. T., K. S., M. A., N. M., I. E.; data curation, S. B., M. T., K. S., M. A., N. M., I. E., N. A.; writing—original draft preparation, S. B., M. T., K. S., M. A., N. M., I. E., N. A.; writing—review and editing, S. B., M. T., K. S., M. A., N. M., I. E., N. A.; visualization, S. B., M. T., K. S., M. A., N. M., I. E., N. A.; supervision, S. B., M. T., K. S., M. A., N. M., I. E., N. A.; project administration, S. B., M. T., K. S., M. A., N. M., I. E."

Statement on Ethical Considerations and Human Participants

This article does not involve human participants, personal identifying data, or any form of data collection that requires ethics committee approval.

Acknowledgement

This research was funded by the Muhammad bin Rashid Smart Learning Program. We gratefully acknowledge their financial support, which has been instrumental in the successful completion of this study. Their contributions have enabled us to conduct thorough research and prepare of this article. We express our sincere thanks for their unwavering support and commitment to advancing smart learning initiatives.
The authors are grateful to the anonymous referee for a careful checking of the details and for helpful comments that improved this paper.

References

[1] Culot, G., Nassimbeni, G., Orzes, G., & Sartor, M. The ISO IEC 27001 information security management standard: Literature review and theory-based research agenda. International Journal of Information Management, **57**, 102276, (2021).

[2] Posthumus, S. R. A framework for the governance of information. Computers & Security, **23**, 638–646, 2004.

[3] AlGhamdi, S. (2020). Information security governance: A systematic literature review and an agenda for future research. Computers & Security, **95**, 101873.

[4] Bena, Yunusa Adamu, Roliana Ibrahim, Jamilah Mahmood, Arafat Al-Dhaqm, Ahmad Alshammari, Muhammed Nura Yusuf, Maged Nasser, and Matthew O. Ayemowa. Significant data governance challenges arising from data generated by intelligent systems technologies: A systematic literature review. IEEE Access, **13**, 2025.

[5] Chukwurah, Naomi, Adebimpe Bolatito Ige, Victor Ibukun Adebayo, and Osemeike Gloria Eyieyien. Frameworks for effective data governance: best practices, challenges, and implementation strategies across industries. Computer Science & IT Research Journal, **5(7)**, 1666–1679, 2024.

[6] Baker, W. H.; Wallace, L. Is Information Security Under Control?: Investigating Quality in Information Security Management. Security & Privacy. IEEE, **5(1)**, January–February 2007.

[7] Ozkan, B. K. Sevgi. Collaborative risk method for information security management practices: A case context within Turkey. International Journal of Information Management, **30(6)**, December 2010.

[8] Ullah, Faheem, and Muhammad Ali Babar. An architecture-driven adaptation approach for big data cybersecurity analytics. 2019 IEEE International Conference on Software Architecture (ICSA), IEEE, 2019

[9] Abouelmehdi, K., Beni-Hssane, A., Khaloufi, H., & Saadi, M. (2017). Big data security and privacy in healthcare: A review. Procedia Computer Science,**113**, 73–80. 8

[10] Ullah, I., Babar, M. A. (2018). Architectural tactics for big data cybersecurity analytics systems: A review. arXiv preprint arXiv:1802.03178.

[11] Kwon, S. Sungho. Common defects in the information security management system of Korean companies. Journal of Systems and Software, 80(10), October 2007.

[12] El-Masri, F. Sahih alBukhari The Myth vs. Reality (Translation). Reality December, 2024, Available at SSRN: https://ssrn.com/abstract=5128655 or http://dx.doi.org/10.2139/ssrn.5128655

[13] Dlamini, J. H. P. E. M. M. E. M. T. Information security: The moving target. Computers & Security, **28(3– 4)**, May–June 2009.

[14] Kowalski, J. A. C. a. L. Y. a. S. A Framework for Evaluation of Information Systems Security. Unpublished Work, 2005.

[15] Talib, A. (2012). Adoption of information security management standards in the Middle East: The case of ISO/IEC 27001. Issues in Informing Science and Information Technology, **9**, 331–349.

[16] Marcucci, D., Zingales, N., & Gasser, U. (2023). Global data governance frameworks: Fragmentation, challenges, and opportunities. arXiv preprint arXiv:2302.13731.

[17] El Aissi, M. E. M., Benhra, S., Chaoui, H., & Ramdani, M. A scalable smart farming big data platform for real-time and batch processing based on lambda architecture. Journal of System and Management Sciences, **13(2)**, 17–30, 2023.

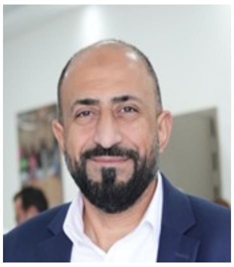
[18] Data-Centric Security. (2025). Data-centric security. Wikipedia. Retrieved from https://en.wikipedia.org/wiki/Data-centric security

[19] Ullah, Faheem, and Muhammad Ali Babar. An architecture-driven adaptation approach for big data cybersecurity analytics. 2019 IEEE International Conference on Software Architecture (ICSA), IEEE, 2019

[20] Ullah, F., Babar, M. A. (2019). Architectural tactics for big data cybersecurity analytics systems: A review. Journal of Systems and Software, **151**,81-118

Sufian A. Badawi Hac completed his Ph.D. from the National University of Sciences and Technology (NUST). currently, he is a Full-time lecturer / assistant professor at Al-Balqa Applied University. Before that, he was an assistant professor at Applied Science Private University in Jordan. He worked as a Post-Doctoral researcher at the American University of Ras Al-Khailmah (AURAK). His research interests include Artificial Intelligence and machine learning, data science, AIOT autonomous vehicles, smart cities, smart grid fraud detection, time series analysis, computer vision, diagnostic retinal image analysis, and innovative AI-based smart learning education. From 2001 till now, he managed to deliver innovative revenue-generating solutions and services in multiple organizations and firms across countries.mathematical journals.

Khouloud Salameh is an Associate Professor in the Department of Computer Science and Engineering at the American University of Ras Al Khaimah, United Arab Emirates. She earned her Ph.D. in Computer Science and Control Engineering, Automation, and Robotics from the University of the Basque Country, Spain, in 2013. Before joining AURAK, she served as a postdoctoral researcher in computer science at the University of Pau and Pays de l'Adour, France. Her teaching interests encompass software design and engineering, algorithm analysis and design, and human-computer interaction. Her research focuses on data representation and modeling, digital ecosystem optimization, and ontologies.



Maen Takruri received his Ph.D. in Electrical Engineering from the University of Technology, Sydney (UTS), Australia, in 2010. During his time at UTS, he was an active member of the Centre for Real-Time Information Networks (CRIN). In 2008, he served as a Visiting Researcher in the Department of Electrical and Electronic Eng. at the Uni. of Melbourne, Australia. Prof. Takruri has held several significant positions, including Chairman of the Department of Electrical, Electronics, and Communications Engineering and Director of the Advanced Technology and Artificial Intelligence Center (ATAIC) at the American University of Ras Al Khaimah (AURAK), UAE. He is currently a full professor with the Department of Electrical Engineering at the American University of the Middle East (AUM), Kuwait. His research interests span a broad range of areas, including signal processing and data fusion, estimation theory and target tracking, biomedical systems, machine learning, image processing, and the Internet of Things.

Djamel Guessoum is a Senior Electrical Engineer at Abu Dhabi National Oil Company in the United Arab Emirates. Worked as Pst Doctoral researcher at the American University of Ras Al-Khaimah (AURAK) in the United Arab Emirates. He earned a BSc. from the University of Batna in Algeria, an MS/Ph.D degrees from the Ecole de Technologie Superieure In Montreal, Canada. His research interests include Artificial Intelligence and machine learning, pervasive/Ubiquituous computing, and renewable energies.

.

Isam El-Badawi Professor El-Badawi is the chairman of Industrial Engineering department at University of Hail in KSA. He obtained his M.S. and Ph.D. from Purdue University of West Lafayette, Indiana USA. His research interests include digital and virtual manufacturing ,systems engineering, manufacturing process improvements, lean manufacturing, lean six sigma, , computer aided manufacturing, and innovative engineering education . Professor El-Badawi is the director of graduate executive master programs of Quality Engineering Management and Occupational Safety and Health.

Aws Al-Qaisi AWS AL-QAISI, he is a professor at the Electrical Engineering Department, College of Engineering and Technology, American University of the Middle East, Kuwait. Prof. Al-Qaisi received his PhD and MSc in communication and signal processing from Newcastle University in 2006 and 2010, respectively. He is a member of the IEEE executive committee in Jordan, responsible for the industrial section. His research interests include feature extraction, artificial intelligence algorithms and transformations, and digital communication. He has served as a reviewer in many international journals, where he has published more than 25 scientific papers in the field of communication and signal processing.