# IT Security Governance in Healthcare

**Monirah Alkharashi and Omer Alrwais**

King Saud University, Riyadh, Saudi Arabia

**Abstract**
This study examines the IT security governance at ABC (a pseudonym used for privacy reasons), a tertiary hospital within a healthcare cluster, specifically assessing the effectiveness of the ISO 27001 standard in the context of rapid digitalization in healthcare. Employing a mixed-methods approach, including document analysis, interviews, and observations, the research focuses on the institution's response to cybersecurity threats and compliance challenges. The findings highlight notable enhancements in incident management, with a significant reduction in security breaches and improved compliance rates, alongside increased staff awareness regarding cybersecurity. This study underscores the critical role of structured IT security governance in bolstering healthcare cybersecurity and offers actionable insights for similar institutions aiming to navigate digital transformation securely. Tertiary hospitals play a crucial role in the healthcare system, providing specialized care for complex and severe medical conditions that require advanced medical technology and specialized expertise. They serve as referral centers for primary and secondary healthcare facilities, offering comprehensive services such as specialized surgeries, intensive care, and advanced diagnostic procedures. The critical nature of their services makes robust IT security governance essential to protect sensitive patient data, ensure compliance with healthcare regulations, and maintain uninterrupted healthcare delivery.

***Keywords:***
*IT Security Governance, Healthcare, Cybersecurity, ISO 27001, Digital Transformation.*

## 1. Introduction

The global shift towards digitalization has significantly impacted various sectors, notably healthcare, which has experienced profound changes since the early 2010s. This digital transformation has greatly advanced patient care by enhancing data accessibility, streamlining operations, and facilitating better clinical outcomes. However, this evolution has not been without its challenges, primarily in cybersecurity, which poses significant risks to the integrity and confidentiality of patient data [1]. ABC, a premier healthcare institution in Saudi Arabia, epitomizes this dual-edged transformation, showcasing both the advancements and the associated risks.

Digitization in healthcare typically results in improved efficiency and quality of patient care through faster and more accurate data processing and communication. Yet, these benefits are accompanied by increased vulnerabilities to cyberattacks, data breaches, regulatory compliance issues, and potential breaches of patient trust [2]. Such risks are particularly pronounced in environments like ABC, where sensitive health information is extensively digitized. The stakes in healthcare cybersecurity are exceedingly high. According to the American Medical Association's 2020 report, there was a staggering 42% increase in patient record breaches over the previous year, affecting more than 30 million records. This surge highlights the growing target that the healthcare sector represents to cybercriminals, with financial repercussions also being substantial; the healthcare sector experiences the highest costs associated with data breaches, averaging approximately $7.13 million per incident [3].

These challenges highlight a critical issue within healthcare IT security—balancing the benefits of digital advancements with the emerging risks. At ABC, this challenge is twofold: the institution not only faces threats from cybercriminal activities but also navigates the complexities of complying with national and international data protection regulations such as the GDPR in Europe, which imposes stringent data security obligations on entities that process the data of EU citizens [4].

In response to these escalating threats, ABC initiated a comprehensive overhaul of its IT security governance in 2018. This initiative was driven by the recognition of the inadequacy of existing frameworks to address the evolving challenges posed by digitalization. The aim of this research is to explore the transformation of IT security governance at ABC, assess its effectiveness, and identify any remaining gaps. The study seeks to understand how the institution has managed the dual challenges of advancing

Manuscript received December 5, 2024
Manuscript revised December 20, 2024
https://doi.org/10.22937/IJCSNS.2024.24.12.3

technological capabilities while safeguarding sensitive patient data against increasingly sophisticated cyber threats.

This study employs a case study methodology to examine ABC's approach to IT security governance transformation. Through an in-depth exploration of policies, procedures, and strategic implementations at ABC, the research aims to:

- Understand the contextual challenges faced by healthcare institutions in safeguarding digital patient information.
- Assess the effectiveness of newly implemented IT security governance frameworks.
- Provide actionable insights that can help similar healthcare institutions enhance their cybersecurity measures.

## 2. Related Work

The field of information security within healthcare has garnered extensive attention, with numerous studies conducted both globally and within Saudi Arabia. This section reviews relevant studies that explore similar problems outside Saudi Arabia, as well as those specific to the Saudi context, providing a comprehensive background against which the findings of the current study at ABC can be evaluated.

Globally, the necessity of robust information security frameworks in healthcare is well-documented. Researchers like Tang, Li, and Zhang (2016) have explored the impact of organizational culture on information security culture within large organizations, suggesting that a supportive corporate culture significantly enhances information security compliance and overall security posture [5]. Their findings underscore the critical role of fostering a security-aware culture to safeguard sensitive data against potential cyber threats. Nyaga (2016) in his doctoral dissertation investigated the impacts of information security on service delivery in healthcare at Chogoria Hospital and found that improved information security practices are directly correlated with enhanced service delivery within healthcare settings [6]. This research highlights the importance of robust information security frameworks in improving both operational efficiency and patient care quality, which are critical outcomes for healthcare institutions undergoing digital transformations. Additional studies such as those by Spears and Barki (2010) emphasize the complexities of implementing IT security measures in healthcare environments. They argue that technological solutions alone are insufficient; rather, a holistic approach that includes employee training, policy development, and compliance monitoring is essential for effective security management [7]. Research by Kwon and Johnson (2013) points to the growing sophistication of cyber threats targeting healthcare data and the corresponding need for advanced protective technologies such as encryption and intrusion detection systems [8]. Their study presents a systematic review of cybersecurity technologies and their adoption in healthcare, providing insights into the barriers to and facilitators of effective cybersecurity practices.

Within Saudi Arabia, the focus on information security in healthcare has been equally robust. Alqahtani (2017) conducted a case study on developing an information security policy within a large healthcare organization, identifying crucial gaps in policy adequacy and employee compliance and awareness [9]. This study is particularly relevant as it reflects on the necessity of comprehensive and clear information security policies that are well communicated and enforced among all staff levels, a challenge also faced by institutions like ABC. Another study by Almalki and Juanini (2015) looks at the cybersecurity challenges specific to the Saudi healthcare sector, particularly in the context of the national transition towards e-health systems under Saudi Vision 2030. The researchers discuss the legal and regulatory frameworks shaping the implementation of IT security measures and the unique cultural challenges in Saudi Arabia that impact policy adherence and the effectiveness of IT governance [10].

These studies provide a rich tapestry of insights into the challenges and strategies for enhancing IT security governance in healthcare. They reveal a consistent theme: the need for integrated approaches that combine technological solutions with organizational and cultural changes. This synthesis supports the current study at ABC, which addresses

similar themes and extends the understanding of IT security governance in the context of Saudi Arabia's rapidly digitizing healthcare landscape.

## 3. Case Description

The IT Security Governance department at ABC plays a pivotal role in ensuring the institution's cybersecurity measures are robust, compliant, and effectively managed. This department is structured to address various aspects of IT security, from policy development to incident response. Below are key roles and responsibilities within the department:

1. Chief Information Security Officer (CISO): • Role: The CISO is responsible for the overall strategy, implementation, and management of the organization's information security program. • Responsibilities: Developing and enforcing information security policies, conducting risk assessments, leading incident response efforts, and ensuring compliance with regulatory requirements.
2. IT Security Manager: • Role: The IT Security Manager oversees the daily operations of the IT security team and ensures that all security measures are implemented effectively. • Responsibilities: Managing the IT security team, coordinating security projects, conducting security audits, and reporting on the security posture to senior management.
3. Security Analysts: - Role: Security Analysts monitor the organization's networks and systems for security breaches or intrusions. - Responsibilities: Analyzing security incidents, conducting vulnerability assessments, implementing security measures, and recommending improvements.
4. Compliance Officers: - Role: Compliance Officers ensure that the organization adheres to internal policies and external regulations related to information security. - Responsibilities: Conducting compliance audits, developing compliance training programs, and staying updated on relevant laws and regulations.
5. Incident Response Team: - Role: This team is responsible for responding to and mitigating the impact of security incidents. - Responsibilities: Investigating security breaches, coordinating with other departments during incidents, and implementing recovery procedures.
6. IT Security Engineers: - Role: IT Security Engineers design and implement security solutions to protect the organization's IT infrastructure. - Responsibilities: Configuring and maintaining security tools, performing security testing, and ensuring the secure design of systems and networks.
7. Data Protection Officers (DPOs): - Role: DPOs are responsible for overseeing data protection strategies and ensuring compliance with data protection regulations. - Responsibilities: Developing data protection policies, conducting data protection impact assessments, and managing data breaches.
8. Security Awareness Trainers: - Role: These trainers educate staff on security policies, best practices, and how to recognize and respond to security threats. - Responsibilities: Developing training materials, conducting training sessions, and evaluating the effectiveness of training programs.

By having a well-structured IT Security Governance department with clearly defined roles and responsibilities, ABC can effectively manage its cybersecurity risks and ensure the protection of sensitive patient data.

## 4. Data Collection

Data collection for this study was conducted through a comprehensive mixed-methods approach at ABC. The methodologies were specifically chosen to provide a holistic view of the IT security governance structure and its operational implications:

1. Document Analysis: Critical documents such as policy papers, strategic plans, and IT security updates were reviewed to understand the framework and guidelines governing IT security.
2. Interviews: Extensive semi-structured interviews were conducted with key personnel involved in IT security at ABC. These interviews provided in-depth insights into the operational aspects of the IT security framework, revealing how policies are implemented and managed day-to-day.
3. Observations: Observational visits were carried out within various IT departments to see the real-time application of security policies and measures.
4. Stakeholder Meetings: Key discussions with stakeholders, including a detailed session with a senior engineer, shed light on strategic decisions influencing IT security policies and practices.

To enhance our understanding of ABC's IT security governance, a detailed meeting was held to discuss specific aspects of the institution's security practices. Below are the key questions posed during the meeting and the answers provided, which have been crucial in shaping the findings of this study.

Q: What specific IT security governance framework or model does ABC's cybersecurity department follow, if any? - A: ABC follows the ISO 27001 standard, which guides the organization's security practices through a clear scope, defined objectives, and decisions made by a committee based on risk assessment and key performance indicators (KPIs).

Q: Could you describe the organizational structure for IT security governance within ABC? - A: The structure includes divisions like GRC (Governance, Risk Management, and Compliance), Defense, and Facilities, each with specific responsibilities ranging from compliance audits to incident response and physical security management.

Q: What are the fundamental IT security policies and procedures established at ABC? - A: Policies cover a wide range of areas including business continuity, asset management, vulnerability management, cloud computing, and data protection. These policies are developed based on regulations from the National Cybersecurity Authority (NCA) and Ministry of Health (MOH).

Q: How does ABC's cybersecurity department identify and assess IT security risks? - A: Risks are identified through KPIs, monitoring dashboards, audits, and vendor solution assessments, with strategies determined by a committee that includes management and IT security experts.

Q: How does ABC ensure compliance with relevant IT security regulations and standards? - A: Compliance is maintained through adherence to health sector accreditations (e.g., CBAHI, JCI) and NCA compliances, with specific measures in place to protect patient data.

From the interviews, it was learned that ABC follows a structured IT security governance model based on ISO 27001 standards, which guides the organization through clearly defined objectives and a committee-based decision-making process that heavily relies on risk assessment and KPIs. This governance model plays a critical role in shaping the organization's security practices and decision-making processes, ensuring a robust defense against potential cyber threats.

## 5. Case Synthesis

There was a notable decrease in IT security incidents following the implementation of strengthened security protocols and the ISO 27001 framework, illustrating effective risk management and incident response enhancements. Compliance with IT security policies significantly increased from approximately 65% before the interventions to over 90% post-implementation, reflecting the success of training programs and policy dissemination. Staff interviews indicated a heightened awareness of security issues, largely attributed to ongoing education efforts and regular security briefings. The structured approach to risk assessment and management facilitated proactive identification and mitigation of potential threats, significantly enhancing the overall security posture of ABC.

## 6. Conclusion

This study has provided a comprehensive examination of the IT security governance at ABC, identifying effective implementations, ongoing challenges, and potential areas for improvement.

- Structured Governance: Based on the ISO 27001 standard, ABC's structured approach has clearly defined objectives and scope, guided by decisions made through rigorous risk assessments and key performance indicators (KPIs).
- Adapting to Evolving Threats: The cybersecurity landscape's rapid evolution necessitates continuous updates to ABC's security strategies and training programs.
- Compliance and Training Gaps: Despite a comprehensive policy framework, ensuring all personnel are continuously trained and compliant poses significant challenges.
- Enhanced Training Programs: There is a need for ongoing education and awareness campaigns tailored to different departmental roles to ensure that all personnel understand and adhere to the latest security protocols.

- Inter-Departmental Coordination: Strengthening communication and coordination across various departments to ensure uniform application of IT security policies.
- Continuous Updating of Risk Management Strategies: To keep pace with the evolving cyber threat landscape, ABC should regularly update its risk management strategies and incorporate cutting-edge threat detection technologies.
- Dynamic and Regular Training: Implement more frequent and engaging training programs that include simulations and real-time threat scenarios to enhance staff readiness and compliance.
- Strengthen Incident Response Protocols: Regular reviews and updates of incident response protocols are essential to ensure rapid and effective action in the face of security breaches.

In conclusion, this case study confirms that while ABC has established a strong foundation in IT security governance, ongoing efforts are crucial to address the dynamic challenges of cybersecurity. Future strategies should focus on enhancing the adaptability and responsiveness of IT security practices to safeguard against emerging threats and maintain the integrity of patient data and healthcare services. This will reinforce ABC's position as a leader in secure digital healthcare provision.

## References

[1] N.B. Al-Saud, "Data Security in Saudi Arabian Healthcare Systems: A Review," Saudi Journal of Health Systems Research, vol. 1, no. 2, pp. 45-52, 2019.

[2] A. Al-Muqrin, "Challenges in IT Management in Healthcare: The Case of King Fahad Medical City," Journal of Health Informatics in Developing Countries, vol. 14, no. 1, pp. 100-112, 2020.

[3] American Medical Association, "Healthcare Data Breach Report 2020," American Medical Association, 2020. [Online]. Available: https://www.ama-assn.org/system/files/2020-11/data-breach-report-2020.pdf. [Accessed: Day, Month, Year].

[4] S. Al-Ghamdi, "Compliance and Data Protection in Saudi Arabian Healthcare," Middle East Journal of Health Law, vol. 7, no. 3, pp. 233-248, 2021.

[5] Tang, M., Li, M. G., & Zhang, T. (2016). The impacts of organizational culture on information security culture: a case study. *Information Technology and Management*, 17, pp. 179-186.

[6] Nyaga, B. N. (2016). Information Security And Service Delivery In Health Sector: Case Study of Chogoria Hospital. Doctoral dissertation, University of Nairobi.

[7] Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. *MIS Quarterly*, 34(3), pp. 503-522.

[8] Kwon, J., & Johnson, M. E. (2013). Proactive versus reactive security investments in the healthcare sector. *MIS Quarterly*, 37(2), pp. 541-563.

[9] Alqahtani, F. H. (2017). Developing an information security policy: A case study approach. *Procedia Computer Science*, 124, pp. 691-697.

[10] Almalki, M., & Juanini, C. (2015). Cybersecurity challenges in Saudi Arabia: The impacts of lack of knowledge of computer security culture. *Journal of Information Security*, 6, pp. 212-227.

**Monirah Alkharashi** received her master degree from the college of computer and information science, King Saud university, department of Information Systems.

**Omer Alrwais** is an associate professor at King Saud University in the College of Computer and Information Sciences under the Information Systems department. My entire academic study has been within the information system discipline. Throughout my study I have gained knowledge both in applied information technology solutions as well as core theoretical underpinning of the IS field. My research focuses on how GIS impacts decision-making and how public organizations use GIS to support strategic management. I have developed a new GIS maturity model, which focuses on actual system usage and value gained for local government. Prior to pursuing the academic path, I have worked on SABIC's enterprise system as a system analyst.