Research article
UDC 34:004:34.05:004.056.5
EDN: https://elibrary.ru/xujvtm
DOI: https://doi.org/10.21202/jdtl.2025.6

Universal Information Security Governance System: Organizational and Legal Principles

Musadaq Ahmed Hadi ✉
University of Technology, Baghdad, Iraq

Mohammed Najm Abdulredha
University of Baghdad, Baghdad, Iraq

Keywords

cybersecurity,
digital technologies,
information protection,
information security governance,
information security,
information technologies,
law,
legal regulation,
legislation,
organizational structure

Abstract

Objective: to develop universal organizational and legal principles for building an information security governance system that will allow each organization to create its own effective information security governance system, taking into account its unique business goals and tasks.

Methods: the research integrates the key elements of information security governance, such as vision, strategy, goals, policies, standards, processes, and matrices. Vision and goals set the direction of an organization's development; policies and standards provide a conceptual framework for information protection; processes allow for systematic achievement of objectives; and matrices provide tools for evaluating and monitoring the entire structure. The proposed principles are consistent with international standards, regulatory requirements, and best practices in the field of information security.

Results: the research showed that the developed information security governance system allows for a clear distribution of roles and responsibilities among the employees, ensuring effective implementation of the governance system. The authors also analyzed the existing principles of information security, integrating them into a security strategy that meets the corporate goals. The proposed universal system complies with regulatory legal requirements and can be adapted for organizations of any scale and profile.

✉ Corresponding author

Scientific novelty: the paper represents a practical approach to the implementation of an information security governance system based on the authors' experience, international standards, control systems and legal acts. Unlike existing approaches, the proposed system is flexible and can be adapted to any organization, which makes it a universal tool for information security governance.

Practical significance: the research provides a structured approach to creating a universal information security governance system that can be used by organizations lacking knowledge and resources to implement such initiatives. The authors propose a general structure that can be adapted depending on the organization's assets, the employees' training and awareness of information security issues. This makes the paper a valuable resource for professionals seeking to increase information security in their organizations.

For citation

Hadi, M. A., & Abdulredha, M. N. (2025). Universal Information Security Governance System: Organizational and Legal Principles. *Journal of Digital Technologies and Law, 3*(1), 125–142. https://doi.org/10.21202/jdtl.2025.6

Contents

Introduction

Historically information security (infosec) was started when ancient Egyptians, Greeks and Romans were practicing techniques to secure their messages such as Cryptography. One of the first and most famous people to secure message communications was Julius Caesar. He was invented and used the Caesar cipher to secure his private communications for military purposes. After that, there were many contributions were made to confront this challenge and it became more necessary by agencies which a major portion of their duty is to guarantee infosec. Afterwards, many techniques were invented in the middle ages such as steganography which hides data throughout date as a part of security through obscurity (Rao & Nayak, 2014; Hadi et al., 2023; Wu et al., 2021).

In 1889, British government enacted the Official Secrets Act by created a framework and codified classification schemes to secure and control sensitive data. Moreover, Cyber schools and security Government Codes were established as mandatory need in 1919. These codes were then applied and put into implementation in World War I to secure sensitive data communications. By this time, a lot of securing methods and algorithms were invented such as classification algorithms, Cryptography algorithms code-breaking algorithms were (Ohki et al., 2009).

In World War II, one of the most important information security devices were designed and developed by German called Enigma Machine. It was electro-mechanical device that used for encryption and decryption messages coding warfare. After that, a mathematician and cryptanalyst Alan Turing who was working in British Government Code and Cipher School gained notoriety to solve the mystery of the German code and decipher it. In this era, many technological advancements in infosec, securing communication, encryption, and computer science were developed to made it easier to share an information and sensitive data (Rastogi & von Solms, 2005).

Between 1960 and 1990, infosec was significantly developed as digital electronic and information technology advanced. During this period, first mainframe computers was invented also, time-sharing systems became more important with more data protection mechanisms access development. Furthermore, ARPANET networked systems development with the design of Data Encryption Standard (DES) which was based on symmetric-key encryption standard. Afterwards, Local Area Networks (LANs) and Personal Computers (PCs) came to the scene and organizations started to implement Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS) and Firewalls to protect their information all over networks. By the end of the 1980s, infosec became an important aspect of computer and network operations which laid the groundwork to the era of Cybersecurity[1] (Bendovschi, 2015; Johnston & Hale, 2009).

From 1990 to 2024, infosec was rapidly advanced and due to the expansion of security concepts and security appliances. The main reasons behind that the invention of the internet in the 1990s that created real challenges in the world of infosec such as converting normal protocols into securing protocols (HTTP to HTTPS) by adding security protocols (SSL). Moreover, new technologies and other challenges were discovered such as IoT, blockchain, cloud-computing, quantum-computers and Artificial Intelligence these created many attack-vectors by involving cyberattacks which made infosec of an organization harder to be achieved. Eventually, the mandatory need to assign and design an ISG to every organization is essential to secure organization data (Corriss, 2010; Moulton & Coles, 2003; AlGhamdi et al., 2020).

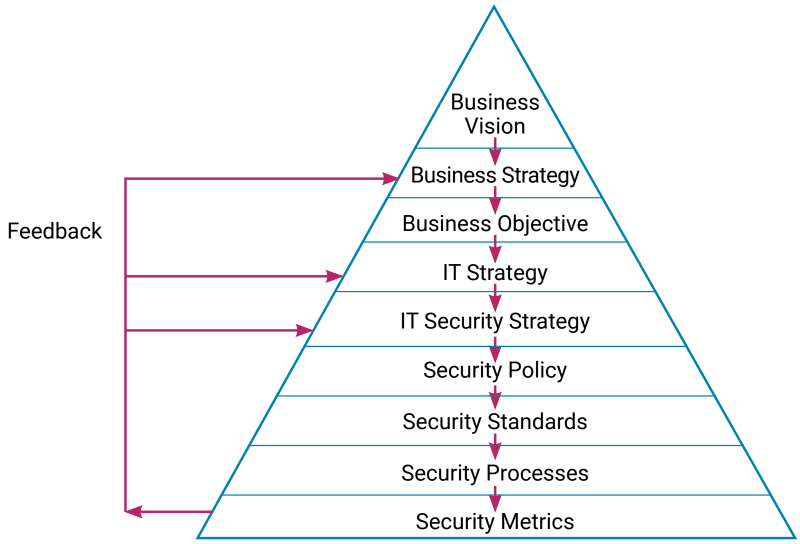
Nowadays, the activities that represent the main focus of the infosec is the management within all assets such as people, risk, incident, vulnerability and also business continuity plan. On the other hand, metrics and other instruments are are used to measure and evaluate in order to achieve an effective ISG program by monitoring

[1] Gregory, P. H. (2018). CISM®: Certified Information Security Manager Exam Guide. New York: McGraw Hill Education.

process and procedures od organization improvement. However, addressing infosec as a critical business challenge is necessary because the lack in securing data leads to serious issue in organizations which indicates the lack of commitment and knowledge of senior executives and boards of directors. Moreover, public and private organizations have challenges to handle infosec at board-level due to lack of knowledge or cybersecurity skills[2] (Carcary et al., 2016; Rocha Flores et al., 2014).

First of all, employees, seniors even board members should appreciate the importance of having ISG, otherwise it cannot be applied effectively. Second, a solid IT governance program must exist in order for ISG to be implemented successfully. A good ISG framework need to be supported by a good IT framework and they should be integrated together in order to achieve organization objectives and goals. Strategically, IT framework contributes to the overall performance of the organization by supporting operational efficiency. An organized method for overseeing IT processes and assets is offered by ISG architecture. Eventually, to put it simply, the cooperation between ISG and IT governance is necessary to guarantee that infosec of public and private organizations are not only put into its place but also align with their overall business aims (S. H. von Solms & R. von Solms, 2010).

In this paper, an efficient ISG (included Cybersecurity) is proposed for public and private organizations that helps them to secure and control their assets and IT. Since, infosec assigns the broader desire of protecting all forms of information, Cybersecurity is a branch of infosec that specified to secure digital information. Therefore, what is applied in the ISG framework includes necessarily Cybersecurity. Moreover, the proposed ISG framework should work under laws and regulations which makes it successively implemented (Fig.). Eventually, a cooperation between IT management and ISG should exist in order to make it easier and serve the organization needs.



An organization vision path from top to bottom

Source: (H., von S.S. & Solms, 2010).

[2] Gregory, P. H. (2022). CISM Certified Information Security manager all-in-one exam guide. New York: McGraw Hill.

The rest of this paper is structured as follows: In Section 1, a key question is asked about the aim and the reason beyond the ISG with details. In Section 2, roles and responsibilities are introduced with RACI chart and Organization elements. In Section 3, Some of top ISG frameworks are presented to consider them as example to design a customized ISG framework that inspired by them. In Section 4, the proposed ISG framework is presented with laws and regulations plus the actions that should be provided by the organization to ensure a good ISG framework is Implemented. the ISG framework is concluded at the end.

1. Why do organizations should have ISG framework? What is the aim of it?

In this section, the mandatory needs of organizations having its own ISG is presented. Generally, ISG becomes very necessary for Public and private organizations due to the rapid advancements in technologies and social media era as discussed earlier in the previous section. Consequently, many government organizations in different sectors are highly depend on their information and IT infrastructure. Therefore, this dependency could reach a level where organizations keep focusing on products/services that information-related to keep their business operations. Moreover, it is necessary for these organizations to secure their assets and data by recognizing their business priority and apply Confidentiality, Integrity, and Availability (CIA) concepts[3].

The aim of designing ISG framework is to work along with their business needs which should contain a strategy to secure/control infosec efficiently. Furthermore, formal security controls are established to explain and ensure activities and desired results. IT and security programs are structured and executed consistently in order to support business priorities. Meanwhile, formal controls and measurement of processes provides managing with clear insights into security governing of the organization. By aligning security management along with procedures that is used in corporate and IT governance ensures efficiency of ISG program. Security management should be integrated into IT and corporate governance processes. Eventually, through security management, strategic planning the proposed ISG program can ensure an overall governance in both public and private organization (Rebollo et al., 2015).

After all, for effective ISG framework implementation, the C-level executives of organization should take the responsibility of data protection in their organizations, here are some activities that should be included in the organization ISG framework (Rebollo et al., 2015):

a) risk management: organization risks should me managed to mitigate exist and future risks of the organization. However, in some cases management should compromise and accept a certain level of risk to sustain the organization functionality.

[3] Gregory, P. H. (2020). CISA Certified Information Systems Auditor all-in-one exam guide. New York: McGraw-Hill.

b) compliance: organization should have restricted to laws and regulations applied in their country also, it should have their own policies and standards to protect their data and assets.

c) incident Response Management: organization executives should establish strategy to handle incidents in order to control sudden event, minimize its impact and support the organization's capability to mitigate the after effect.

d) business Continuity Plan (BCP): it ensures that the organization should stay functional during and after any incident or disaster. Also, this is essentially including a Disaster Recovery Plan (DRP) to maintain the operations in the organization.

e) Disaster Recovery Plan (DRP): it is a part of BCP which is focused on restoring the organization data, infrastructure, IT systems, after incident or the disaster. DRP should have emergency team which have done backups (mirrors), multiple sites (hot, cold) and documentation.

f) security Awareness: it is important to keep all members of the organization at a certain level of awareness in infosec and what ISG framework brings to the table by subjecting multiple training programs thought a year especially IT and management staffs.

Through these activities, C-level executives are played important roles in managing and directing the organization's information systems, ensuring resilience against potential threats and fostering a strategic approach to security governance.

2. Job titles, roles and responsibilities in organizations

The department of infosec in any organization is imaged of being the «department of no» and viewed as an obstacle to business activities. This image emerged from infosec managers who were occasionally overly cautious about risks, oversighting organizations in terms of expand, introduce innovative products and services. As a result, this reputation creates a hesitation among IT members and other business units to interact with security professionals without fearing that cooperation may impede their job. Moreover, a good implementation of ISG happens when organization members grasps their duties and restrict to roles and responsibilities. Also, organizations should establish formal roles and responsibilities that assigns every employee to instructions on how to preserve organization data and assets. Consequently. these roles should be tied to job titles by indicating an employee's place within the organization. Job titles are valued by the organizations in order to ensure that everyone should be rolled based on their titles. Generally, job titles are attached with employee's position which reflects their authority level, here are some job titles that are listed in order of seniority (Nicho, 2018):

a. Chairman, Board of Directors.

b. Member, Board of Directors.

c. Chief Executive Officer.

d. President.
e. Executive Vice President.
f. Senior Vice President.
g. Vice President.
h. Executive Director.
i. Senior Director.
j. Director.
k. Senior Manager.
l. Manager.
m. Supervisor.

The above list covered some of seniority ranks but in larger organizations there are other titles such as first (e.g. first vice president), general (e.g. general manager) and assistant (e.g. assistant director). Further, the responsibilities are much like roles defining the tasks expected from someone. In infosec, organizations assign specific roles and responsibilities to employees and team members in order to guarantee the organization's ISG strategy and goals.

2.1. Standard method of governing organizations

Many organizations used non-standard methods for governing infosec such as doing some security experience here and there. However, there is a standard method which used widely to define roles and responsibilities in organizations known as the Responsible-Accountable-Consulted-Informed (RACI) chart. It is designed to assign roles to employees and teams to perform tasks and activities. Moreover, the chart basically describes who to do what in that organization. For instance, assigns a manager for a project plus that manager should work as security analyst. Also, it gives responsibilities to each employee at any seniority level as follow (Bettwy et al., 2016):

i. Responsible: Any employee who is responsible of a task.
ii. Accountable: Any employee who is responsible of result of a task.
iii. Consulted: Any employee who has experience and can be consulted in a topic.
iv. Informed: Any employee who gets prior notice during or before an action.

Table 1 contains an example of assign roles and responsibilities in an organization. First, employees in organizations must have their own roles and belong to a team. Moreover, every employee should get a specific training course that give him a set of skills in order to accomplish their tasks. In addition, RACI chart urging employees in the organization to have their own tasks and this is called Separation of Duties (SoD). SoD means that no single employee has the full control of a critical process of activity that may affect the organization's functionality. For example, the provisioning of employee account, the provisioner, approver and requester must not be at the same department as a part of preventing the conflicts of interest (Von Solms et al., 2011).

Table 1. Assign roles and responsibilities in RACI chart

Activity	Responsible	Accountable	Consulted	Informed
Audit user account	IA	IAM	AO	IT SD, IT SM, EUM
Provision user account	IT SD	IT SM	AO	IT SD, EUM, ST
Approve user account	AO	COO	EUM, ST	EU, IA, IT SD
Request user account	EU	EUM	IT SD, EUM	AO, ST

* EU: End User, EUM: End User Manager, SD: Service Desk, EUM: End User Manager, AO: Asset Owner, ST: Security Team, IA: Internal Audit, SM: Service Manager, IAM: Internal Audit Manager.

Source: (Von Solms et al., 2011)

2.2. Standards and security frameworks of organizations

A successive organization is the one that operates under well designed ISG framework which based on standards that works along with its vision and strategy. However, design a strategy is not easy which includes policies, standards, process and matrices that supports the overall vision of the organization. In this section, many standards are presented that applied in world-wide organizations such as Google, Meta[4], Amazon, …, etc. Moreover, if security professional along with C-level executives are decided to design ISG framework to an organization and selected a control framework alone, it is often considered as a mistake. Arguably, this ISG framework should exemplified and take advantage of some world-wide standards and security controls to avoid mistakes/ issues in order to provide a good start in governing the organization. Many standards and control frameworks are listed in Table 2 that can be useful as a start point to design ISG framework for public and private organizations (Tan et al., 2010; Fazlida & Said, 2015; Ula et al., 2017).

Table 2. Some standards and control frameworks

No.	Standards and frameworks	Explanation
1	National Institute of Standards and Technology (NIST)	NIST is used by U.S. Department of Commerce to standardize economic security, innovation, industry and technology comprehensive
2	International Organization for Standardization/ International Electrotechnical Commission (ISO/IEC)	ISO/IEC two main international standards that are used for infosec, technology, industry and business practices

[4] The organization is recognized as extremist, its functioning is prohibited in the territory of the Russian Federation.

End of Table 2

No.	Standards and frameworks	Explanation
3	Control Objectives for Information and Related Technologies (COBIT)	COBIT is a framework that is used to governing IT and managing enterprises by set some guidelines and best practices for IT organizations
4	Payment Card Industry Data Security Standard (PCI-DSS)	PCI-DSS is a combination of infosec standards that established to protect sensitive information of payment cards
5	Health Insurance Portability and Accountability Act (HIPAA)	HIPAA is an act in U.S. law that enacted to protect information of people's health privacy plus to secure medical data
6	Information Security Forum (ISF)	ISF is a combination of security controls and best practices that used to manage risks in infosec
7	Information Technology Infrastructure Library (ITIL)	ITIL is an IT service framework is designed to for management purposes that included managing IT infrastructure, environment, services and processes

Source: (Ula et al., 2017).

3. Top ISG/Cybersecurity frameworks

In this section, some of the top countries in ISG and cybersecurity field are presented. Meanwhile, there are some Arabic countries that are listed with the highly ranked and powerful countries such as United Arab Emirates and Saudi Aribia. These countries are highly recommended examples to be follow in such sensitive and valuable field. The following are the countries including their ISG frameworks, Laws and regulations to control Information (Shingarev & Kazakova, 2021; Creemers, 2023; Priyadarshini & Cotton, 2022; Carr & Tanczer, 2018; Singh & Alshammari, 2020; Al Neaimi et al., 2015):

Russia's ISG framework: it implies laws such as Federal Service for Technical and Export Control (FSTEC) which was enacted to secure products, Federal Law No. 149-FZ to protect data and the role of Federal Security Service (FSB) in Cybersecurity. Consequently, local laws of data urged that Russian citizens' information has to be stored in the country (Shingarev & Kazakova, 2021).

China's ISG framework: it includes ministries like Ministry of Public Security (MPS) which oversights infosec in China. In addition, the Chinese Cybersecurity Law enacted in 2017 with the National Security Law (NSL). Eventually, the law of Cyberspace Administration of China (CAC) that controls internet regulations (Creemers, 2023).

US's ISG framework: it involves laws such as Federal Information Security Management Act (FISMA) and Cybersecurity Enhancement Act (CEA) of 2014. Also, National Institute of Standards and Technology (NIST) which established standards. Cybersecurity and Infrastructure Security Agency (CISA) that coordinated agencies such as the National Security Agency (NSA) that handles Cybersecurity activities (Priyadarshini & Cotton, 2022).

UK's ISG framework: it contains acts and strategy National Cyber Security Strategy (NCSC) and Data Protection Act (DPA) 2018. Moreover, the Computer Misuse Act (CMA) in 1990 assigns cyber offenses. The UK government involves international cybersecurity cooperation (Carr & Tanczer, 2018).

Saudi Arabia's ISG framework: it involves laws such as the Saudi Arabia Cybersecurity Law (SACL) in 2019 that controlled by the Communications, Space and Technology Commission (CITC) and National Cybersecurity Authority (NCA). Saudi Central Bank (SAMA) oversight the financial transactions in the financial sector (Singh & Alshammari, 2020).

UAE's ISG framework: it includes laws like UAE Cybersecurity Law of 2019 and oversight by the National Electronic Security Authority (NESA) and Telecommunications and Digital Government Regulatory Authority (TRDA). Dubai English Speaking College (DESC) that oversights the cybersecurity in Dubai (Al Neaimi et al., 2015).

4. A proposed information security governance framework

Before proposing any new framework, or development an existing framework, it is imperative to explain two fundamental concepts: Governance and Corporate Governance. Governance pertains to protect the interests of owners by guiding, managing and supervising on their behalf, with the Board of Directors acting as their representatives. Corporate Governance is defined as response to the separation between management and ownership within private and public organizations. Moreover, it aims to maintain this separation by providing incentives to both the management and board to pursue aims which are in line with the interests of the company and its shareholders.

The proposed framework for ISG should include some elements to ensure an effective protection and management of an organization's information assets, achieving both discipline between owners and management plus granting owners the authority to oversee the organization. Additionally, by establishing a secure environment for sharing and storing information, organizations can not only enhance productivity, consumer benefits and business efficiency but also support security measures. Conversely, any insecure work environment presents significant risks, potentially resulting in substantial harm to corporations and governments, with possible adverse effects on citizens and consumers. This is particularly critical for businesses operating in crucial organizations such as finance, electricity generation, banking, or healthcare, where the stakes are exceptionally high. Table 3 includes the key questions essential for establishing effective ISG.

Table 3. Some important questions/actions for effective ISG

Actors/Actions	Corporate Executives	Business Unit Head	Senior Manager	CIO/CISO
Governance/Business Drivers	What am I required to do? What am I afraid not to do?			
Roles and Responsibilities	How do I accomplish my objectives?			
Metrics/Audit	How effectively do I achieve my objectives? What adjustments do I need to make?			

The ISG framework serves as a tool to implement the strategy and vision of the C-level executives to achieve high performance of business operations and decision-making in organizations. It falls under their purview to manage as part of their oversighting the organization and protect its data and assets by guaranteeing the efficient integration of infosec throughout their organization.

To design an effective ISG framework that can be globally affirmed and accepted, there are some global laws and regulations that should be taken into consideration. Consequently, these laws and regulations can be a great advantage due to their structures and well-designed by use it as a law experiences of other countries to legislate and enact our Laws and Regulations. Table 4 shows some key laws and regulations that has been used over the globe in governing infosec.

Table 4. Global laws and regulations examples[5]

No.	Laws and Regulations	Explanation
1	General Data Protection Regulation (GDPR)	It mandates organizations to protect the personal data of individuals within the European Union (EU) and imposes strict requirements for data privacy and security.
2	California Consumer Privacy Act (CCPA)	It applies to businesses that collect personal information of California residents and requires them to implement measures to protect the privacy and security of such information.
3	Sarbanes-Oxley Act (SOX)	It requires companies to establish and maintain internal controls over financial reporting, which includes measures to protect the integrity and confidentiality of financial data.
4	Federal Information Security Management Act (FISMA)	It is a US federal law that establishes security requirements for federal information systems and provides a framework for managing cybersecurity risks in federal agencies.
5	Cybersecurity Maturity Model Certification (CMMC)	It developed by the U.S. Department of Defense (DoD) to assess and enhance the cybersecurity posture of defense contractors and subcontractors.
6	Data Protection Laws (DPL)	Various countries have enacted their own data protection laws, such as the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada and the Personal Data Protection Act (PDPA) in Singapore.

Conclusions

In this work, a new ISG (includes cybersecurity) framework is proposed to protect information and assets of public and private organizations by taking advantage of some laws and regulations. This framework can be compared to the existed frameworks that have been implemented in the world-wide organizations. In addition, it focuses on cooperation between continuous improvement and risk management which aligns with the business model of the organization that includes regulations and laws requirements.

[5] Manning, W. (2010). CISM Certified Information Security Manager certification exam preparation course in a book for passing the CISM: The how to pass on your first try certification study guide. Brisbane, Australia: Emereo Pty Ltd.

Meanwhile, any organization should have its own ISG framework and a committee (BoD) to implement it. For successive ISG in a country, the committees in all organizations should be connected to each other by a higher committee of ISG or Cybersecurity that can implement the overall governance. Furthermore, this ISG framework acts as a weapon to implement governance of infosec plus ensures that the overall process works along with the business goals and objectives effectively. Finally, this ISG framework offers a real security program which can be applied by the authors to any private and public organization.

References

Al Neaimi, A., Ranginya, T., & Lutaaya, P. (2015). A framework for effectiveness of cyber security defenses, a case of the United Arab Emirates (UAE). *International Journal of Cyber-Security and Digital Forensics*, *4*(1), 290–301. https://doi.org/10.17781/p001502

AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2020). Information security governance challenges AND CRITICAL SUCCESS FACTORS: Systematic review. *Computers & Security*, *99*, 102030. https://doi.org/10.1016/j.cose.2020.102030

Bendovschi, A. (2015). Cyber-attacks – trends, patterns and security countermeasures. *Procedia Economics and Finance*, *28*, 24–31. https://doi.org/10.1016/s2212-5671(15)01077-1

Bettwy, G., Beevers, M., & Williams, M. (2016). *CISM Review Manual Certified Information Security manager*. Rolling Meadows, Ill: ISACA.

Carcary, M., Renaud, K., McLaughlin, S., & O'Brien, C. (2016). A framework for Information Security Governance and Management. *IT Professiona*l, *18*(2), 22–30. https://doi.org/10.1109/mitp.2016.27

Carr, M., & Tanczer, L. M. (2018). UK cybersecurity industrial policy: An analysis of drivers, market failures and interventions. *Journal of Cyber Policy*, *3*(3), 430–444. https://doi.org/10.1080/23738871.2018.1550523

Corriss, L. (2010). Information security governance. *Proceedings of the 2010 Workshop on Governance of Technology, Information and Policies* (pp. 35–41). https://doi.org/10.1145/1920320.1920326

Creemers, R. (2023). Cybersecurity law and regulation in China: Securing the smart state. *China Law and Society Review*, *6*(2), 111–145. https://doi.org/10.1163/25427466-06020001

Fazlida, M. R., & Said, J. (2015). Information security: Risk, governance and implementation setback. *Procedia Economics and Finance*, *28*, 243–248. https://doi.org/10.1016/s2212-5671(15)01106-5

Hadi, M. A., Abdulredha, M. N., & Hasan, E. (2023). Introduction to ChatGPT: A new revolution of artificial intelligence with machine learning algorithms and cybersecurity. *Science Archives*, *04*(04), 276–285. https://doi.org/10.47587/sa.2023.4406

Johnston, A. C., & Hale, R. (2009). Improved security through information security governance. *Communications of the ACM*, *52*(1), 126–129. https://doi.org/10.1145/1435417.1435446

Moulton, R., & Coles, R. S. (2003). Applying information security governance. *Computers & Security*, *22*(7), 580–584. https://doi.org/10.1016/s0167-4048(03)00705-3

Nicho, M. (2018). A process model for implementing Information Systems Security governance. *Information & Computer Security*, *26*(1), 10–38. https://doi.org/10.1108/ics-07-2016-0061

Ohki, E., Harada, Y., Kawaguchi, Sh., Shiozaki, T., & Kagaya, T. (2009). Information security governance framework. *Proceedings of the first ACM workshop on Information security governance* (pp. 1–6). https://doi.org/10.1145/1655168.1655170

Priyadarshini, I., & Cotton, C. (2022). Cyber laws in the United States. *Cybersecurity* (pp. 157–237). https://doi.org/10.1201/9781003187127-6

Rao, U. H., & Nayak, U. (2014). History of computer security. *The InfoSec Handbook* (pp. 13–25). https://doi.org/10.1007/978-1-4302-6383-8_2

Rastogi, R., & von Solms, R. (2005). Information security governance – a re-definition. *Security Management, Integrity, and Internal Control in Information Systems* (pp. 223–236). https://doi.org/10.1007/0-387-31167-x_14

Rebollo, O., Mellado, D., Fernández-Medina, E., & Mouratidis, H. (2015). Empirical evaluation of a cloud computing information security governance framework. *Information and Software Technology*, *58*, 44–57. https://doi.org/10.1016/j.infsof.2014.10.003

Rocha Flores, W., Antonsen, E., & Ekstedt, M. (2014). Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers & Security*, *43*, 90–110. https://doi.org/10.1016/j.cose.2014.03.004

Shingarev, A., & Kazakova, A. (2021). The Russian Federation's approach to Cybersecurity. *The Oxford Handbook of Cyber Security* (pp. 672–684). https://doi.org/10.1093/oxfordhb/9780198800682.013.44

Singh, H. P., & Alshammari, T. S. (2020). An institutional theory perspective on developing a cyber security legal framework: A case of Saudi Arabia. *Beijing Law Review*, *11*(03), 637–650. https://doi.org/10.4236/blr.2020.113039

Tan, T. C., Ruighaver, A. B., & Ahmad, A. (2010). Information security governance: When compliance becomes more important than security. *Security and Privacy – Silver Linings in the Cloud* (pp. 55–67). https://doi.org/10.1007/978-3-642-15257-3_6

Ula, M., Ula, M., & Fuadi, W. (2017). A method for Evaluating Information Security Governance (ISG) components in banking environment. *Journal of Physics: Conference Series*, *812*, 012031. https://doi.org/10.1088/1742-6596/812/1/012031

Von Solms, S. H., & von Solms, R. (2010). *Information security governance*. New York, United States: Springer.

Von Solms, R., Thomson, K.-L., & Maninjwa, P. M. (2011). Information security governance control through comprehensive policy architectures. *Information Security for South Africa* (pp. 1–6). https://doi.org/10.1109/issa.2011.6027522

Wu, M., Aranovich, R., & Filkov, V. (2021). Evolution and differentiation of the cybersecurity communities in three social question and answer sites: A mixed-methods analysis. PLOS ONE, 16(12). https://doi.org/10.1371/journal.pone.0261954

Authors information

Musadaq Ahmed Hadi – MSc. (Control Engineer), Control and Systems Engineering Department, University of Technology
Address: Al-Wehda, Baghdad, Iraq
E-mail: musadaq.ahmed@alshaab.edu.iq
ORCID ID: https://orcid.org/0000-0002-3884-495X
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57117413800
WoS Researcher ID: https://www.webofscience.com/wos/author/record/JZT-4113-2024
Google Scholar ID: https://scholar.google.com/citations?user=wcrA7n8AAAAJ

Mohammed Najm Abdulredha – MSc. (Computer Science), Department of Computer Science, University of Baghdad
Address: Al-Jadriya, Baghdad, Iraq
E-mail: mohammed.najm.422@gmail.com
ORCID ID: https://orcid.org/0009-0007-8441-3505
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57226709471
WoS Researcher ID: https://www.webofscience.com/wos/author/record/KIJ-3538-2024
Google Scholar ID: https://scholar.google.ru/citations?user=-oXQXKEAAAAJ

Authors' contributions

The authors have contributed equally into the concept and methodology elaboration, validation, formal analysis, research, selection of sources, text writing and editing, project guidance and management.

Conflict of interest

The authors declare no conflict of interest.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – April 16, 2025
Date of approval – May 4, 2025
Date of acceptance – March 25, 2025
Date of online placement – March 30, 2025

Научная статья
УДК 34:004:34.05:004.056.5
EDN: https://elibrary.ru/xujvtm
DOI: https://doi.org/10.21202/jdtl.2025.6

Универсальная система управления информационной безопасностью: организационно-правовые принципы

Мусадак Ахмед Хади ✉
Технологический университет, Багдад, Ирак

Мохаммед Наджм Абдулредха
Багдадский университет, Багдад, Ирак

Ключевые слова

законодательство,
защита информации,
информационная безопасность,
информационные технологии,
кибербезопасность,
организационная структура,
право,
правовое регулирование,
управление информационной безопасностью,
цифровые технологии

Аннотация

Цель: разработка универсальных организационно-правовых принципов построения системы управления информационной безопасностью, которые позволят каждой организации создать собственную эффективную систему управления информационной безопасностью с учетом ее уникальных бизнес-целей и задач.

Методы: основаны на интеграции ключевых элементов управления информационной безопасностью, таких как видение, стратегия, цели, политики, стандарты, процессы и матрицы. Видение и цели задают направление развития организации, политики и стандарты обеспечивают концептуальную основу для защиты информации, процессы позволяют систематически достигать поставленных задач, а матрицы предоставляют инструменты для оценки и контроля всей структуры. Предложенные принципы согласуются с международными стандартами, нормативными требованиями и лучшими практиками в области информационной безопасности.

Результаты: разработанная система управления информационной безопасностью позволяет четко распределить роли и обязанности среди сотрудников организации, обеспечивая эффективное внедрение системы управления. Авторы также анализируют существующие принципы безопасности информационных технологий, интегрируя их в стратегию безопасности, которая соответствует целям организации. Предложенная универсальная система соответствует нормативным правовым требованиям и может быть адаптирована для использования в организациях любого масштаба и профиля.

✉ Контактное лицо

Научная новизна: заключается в представлении практического подхода к внедрению системы управления информационной безопасностью, основанного на опыте авторов, а также на мировых стандартах, системах контроля и правовых актах. В отличие от существующих подходов предлагаемая система является гибкой и может быть адаптирована под специфику любой организации, что делает ее универсальным инструментом для управления информационной безопасностью.

Практическая значимость: состоит в предоставлении структурированного подхода к созданию универсальной системы управления информационной безопасностью, который может быть использован организациями, испытывающими недостаток знаний и ресурсов для реализации подобных инициатив. Авторы предлагают общую структуру, которая может быть адаптирована в зависимости от активов организации, уровня подготовки сотрудников и их осведомленности в вопросах информационной безопасности. Это делает настоящую работу ценным ресурсом для специалистов, стремящихся повысить уровень защиты информации в своих организациях.

Для цитирования

Хади, М. А., Абдулредха, М. Н. (2025). Универсальная система управления информационной безопасностью: организационно-правовые принципы. *Journal of Digital Technologies and Law*, *3*(1), 125–142. https://doi.org/10.21202/jdtl.2025.6

Список литературы

Al Neaimi, A., Ranginya, T., & Lutaaya, P. (2015). A framework for effectiveness of cyber security defenses, a case of the United Arab Emirates (UAE). *International Journal of Cyber-Security and Digital Forensics*, *4*(1), 290–301. https://doi.org/10.17781/p001502

AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2020). Information security governance challenges AND CRITICAL SUCCESS FACTORS: Systematic review. *Computers & Security*, *99*, 102030. https://doi.org/10.1016/j.cose.2020.102030

Bendovschi, A. (2015). Cyber-attacks – trends, patterns and security countermeasures. *Procedia Economics and Finance*, *28*, 24–31. https://doi.org/10.1016/s2212-5671(15)01077-1

Bettwy, G., Beevers, M., & Williams, M. (2016). *CISM Review Manual Certified Information Security manager*. Rolling Meadows, Ill: ISACA.

Carcary, M., Renaud, K., McLaughlin, S., & O'Brien, C. (2016). A framework for Information Security Governance and Management. *IT Professiona*l, *18*(2), 22–30. https://doi.org/10.1109/mitp.2016.27

Carr, M., & Tanczer, L. M. (2018). UK cybersecurity industrial policy: An analysis of drivers, market failures and interventions. *Journal of Cyber Policy*, *3*(3), 430–444. https://doi.org/10.1080/23738871.2018.1550523

Corriss, L. (2010). Information security governance. *Proceedings of the 2010 Workshop on Governance of Technology, Information and Policies* (pp. 35–41). https://doi.org/10.1145/1920320.1920326

Creemers, R. (2023). Cybersecurity law and regulation in China: Securing the smart state. *China Law and Society Review*, *6*(2), 111–145. https://doi.org/10.1163/25427466-06020001

Fazlida, M. R., & Said, J. (2015). Information security: Risk, governance and implementation setback. *Procedia Economics and Finance*, *28*, 243–248. https://doi.org/10.1016/s2212-5671(15)01106-5

Hadi, M. A., Abdulredha, M. N., & Hasan, E. (2023). Introduction to ChatGPT: A new revolution of artificial intelligence with machine learning algorithms and cybersecurity. *Science Archives*, *04*(04), 276–285. https://doi.org/10.47587/sa.2023.4406

Johnston, A. C., & Hale, R. (2009). Improved security through information security governance. *Communications of the ACM*, *52*(1), 126–129. https://doi.org/10.1145/1435417.1435446

Moulton, R., & Coles, R. S. (2003). Applying information security governance. *Computers & Security*, *22*(7), 580–584. https://doi.org/10.1016/s0167-4048(03)00705-3

Nicho, M. (2018). A process model for implementing Information Systems Security governance. *Information & Computer Security*, *26*(1), 10–38. https://doi.org/10.1108/ics-07-2016-0061

Ohki, E., Harada, Y., Kawaguchi, Sh., Shiozaki, T., & Kagaya, T. (2009). Information security governance framework. *Proceedings of the first ACM workshop on Information security governance* (pp. 1–6). https://doi.org/10.1145/1655168.1655170

Priyadarshini, I., & Cotton, C. (2022). Cyber laws in the United States. *Cybersecurity (*pp. 157–237). https://doi.org/10.1201/9781003187127-6

Rao, U. H., & Nayak, U. (2014). History of computer security. *The InfoSec Handbook* (pp. 13–25). https://doi.org/10.1007/978-1-4302-6383-8_2

Rastogi, R., & von Solms, R. (2005). Information security governance – a re-definition. *Security Management, Integrity, and Internal Control in Information Systems* (pp. 223–236). https://doi.org/10.1007/0-387-31167-x_14

Rebollo, O., Mellado, D., Fernández-Medina, E., & Mouratidis, H. (2015). Empirical evaluation of a cloud computing information security governance framework. *Information and Software Technology*, *58*, 44–57. https://doi.org/10.1016/j.infsof.2014.10.003

Rocha Flores, W., Antonsen, E., & Ekstedt, M. (2014). Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers & Security*, *43*, 90–110. https://doi.org/10.1016/j.cose.2014.03.004

Shingarev, A., & Kazakova, A. (2021). The Russian Federation's approach to Cybersecurity. *The Oxford Handbook of Cyber Security* (pp. 672–684). https://doi.org/10.1093/oxfordhb/9780198800682.013.44

Singh, H. P., & Alshammari, T. S. (2020). An institutional theory perspective on developing a cyber security legal framework: A case of Saudi Arabia. *Beijing Law Review*, *11*(03), 637–650. https://doi.org/10.4236/blr.2020.113039

Tan, T. C., Ruighaver, A. B., & Ahmad, A. (2010). Information security governance: When compliance becomes more important than security. *Security and Privacy – Silver Linings in the Cloud* (pp. 55–67). https://doi.org/10.1007/978-3-642-15257-3_6

Ula, M., Ula, M., & Fuadi, W. (2017). A method for Evaluating Information Security Governance (ISG) components in banking environment. *Journal of Physics: Conference Series*, *812*, 012031. https://doi.org/10.1088/1742-6596/812/1/012031

Von Solms, S. H., & von Solms, R. (2010). *Information security governance*. New York, United States: Springer.

Von Solms, R., Thomson, K.-L., & Maninjwa, P. M. (2011). Information security governance control through comprehensive policy architectures. *Information Security for South Africa* (pp. 1–6). https://doi.org/10.1109/issa.2011.6027522

Wu, M., Aranovich, R., & Filkov, V. (2021). Evolution and differentiation of the cybersecurity communities in three social question and answer sites: A mixed-methods analysis. PLOS ONE, 16(12). https://doi.org/10.1371/journal.pone.0261954

Сведения об авторах

Хади Мусадак Ахмед – магистр наук (инженер систем управления), кафедра управления и системной инженерии, Технологический университет
Адрес: Аль-Вейда, г. Багдад, Ирак
E-mail: musadaq.ahmed@alshaab.edu.iq
ORCID ID: https://orcid.org/0000-0002-3884-495X
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57117413800
WoS Researcher ID: https://www.webofscience.com/wos/author/record/JZT-4113-2024
Google Scholar ID: https://scholar.google.com/citations?user=wcrA7n8AAAAJ

Абдулредха Мохаммед Наджм – магистр компьютерных наук, кафедра компьютерных наук, Багдадский университет
Адрес: Аль-Джадрийя, г. Багдад, Ирак
E-mail: mohammed.najm.422@gmail.com
ORCID ID: https://orcid.org/0009-0007-8441-3505
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57226709471
WoS Researcher ID: https://www.webofscience.com/wos/author/record/KIJ-3538-2024
Google Scholar ID: https://scholar.google.ru/citations?user=-oXQXKEAAAAJ

Вклад авторов

Авторы внесли равный вклад в разработку концепции, методологии, валидацию, формальный анализ, проведение исследования, подбор источников, написание и редактирование текста, руководство и управление проектом.

Конфликт интересов

Авторы сообщают об отсутствии конфликта интересов.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.19.61 / Правовое регулирование информационной безопасности
Специальность ВАК: 5.1.2 / Публично-правовые (государственно-правовые) науки

История статьи

Дата поступления – 16 апреля 2024 г.
Дата одобрения после рецензирования – 4 мая 2024 г.
Дата принятия к опубликованию – 25 марта 2025 г.
Дата онлайн-размещения – 30 марта 2025 г.