Journal of Information Systems Education

Volume 35
Issue 4
Fall 2024

Teaching Case

Combining Standards to Conduct Risk Assessment at SecureEnd Solutions

Muhammad Al-Abdullah, Alper Yayla, and Mohammed Salem Al-Atoum

Recommended Citation: Al-Abdullah, M., Yayla, A., & Al-Atoum, M. S. (2024). Teaching Case: Combining Standards to Conduct Risk Assessment at SecureEnd Solutions. *Journal of Information Systems Education*, 35(4), 461-466. https://doi.org/10.62273/SWQX4831

Article Link: https://jise.org/Volume35/n4/JISE2024v35n4pp461-466.html

Received: January 8, 2024
First Decision: April 16, 2024
Accepted: August 2, 2024
Published: December 15, 2024

ISSN: 2574-3872 (Online) 1055-3096 (Print)

Journal of Information Systems Education, 35(4), 461-466, Fall 2024
https://doi.org/10.62273/SWQX4831

Teaching Case
Combining Standards to Conduct Risk Assessment at SecureEnd Solutions

Muhammad Al-Abdullah
Alper Yayla
Sykes College of Business
University of Tampa
Tampa, FL 33606, USA
mal-abdullah@ut.edu, ayayla@ut.edu

Mohammed Salem Al-Atoum
Computer Science Department
University of Jordan
Amman, Jordan
m.atoum@ju.edu.jo

ABSTRACT

In today's cybersecurity landscape, organizations need frameworks that provide a holistic approach to risk assessment as part of the risk management process. This case introduces SecureEnd Solutions, a rapidly growing cybersecurity company, and its core team, including Alan Touring, Ada Lovecode, Bob Jobs, and Suzan, the head of development. The company must conduct a detailed risk assessment to obtain ISO/IEC 27001 certification using a combination of ISO/IEC 27005:2022 and NIST SP 800-30 guidelines. Students will engage with the characters and the company's technological ecosystem to apply risk assessment standards, enhancing their decision-making, analytical, and problem-solving skills in a real-world scenario.

Keywords: Risk assessment, Risk management, Teaching case, Security assessment, Security frameworks

1. CASE SUMMARY

Technology is inevitably integrated into our lives, but this integration brings to the surface the growing risks of cyberattacks. Therefore, managing risks is an essential part of successful cybersecurity. At the heart of risk management is risk assessment, which involves identifying, analyzing, evaluating, and prioritizing risks. Several standards and guidelines have been established to assist organizations in navigating the risk assessment process. Among them are the guidelines created by the National Institute of Standards and Technology (NIST) (Joint Task Force Transformation Initiative, 2012) and the International Organization for Standardization's guideline (International Organization for Standardization, 2022). The ISO/IEC 27005:2022 guideline is based on general risk management practices, leading practitioners to approach risk assessment more broadly. Accordingly, combining it with NIST SP 800-30 sharpens the risk assessment process (Al Fikri et al., 2019).

It is important for practitioners and students to conduct proper risk assessments, given the increasing demand for skilled personnel in cybersecurity risk management in recent years. The main limitation of the existing academic courses and practitioner training is that they heavily focus on theoretical understanding of risk assessment methods (Alzoubi, 2022; Rodríguez-Espíndola et al., 2022). While understanding the standard or guideline is crucial, it does not necessarily allow learners to implement these components effectively in real-world scenarios. Developing practical skills requires hands-on experience, which enables students and trainees to apply their knowledge effectively.

This case study seeks to bridge this gap by introducing students to the ISO/IEC 27005:2022 and NIST SP 800-30 risk assessment standards and training them with practical skills to 1) define risk assessment scope, 2) identify and classify company assets, 3) identify potential threats and their sources, 4) research the industry to gauge the severity of the threats, 5) investigate and rate vulnerabilities, and 6) rate risks based on their probability and impact.

The case concerns a fictitious successful startup, SecureEnd Solutions, founded by Alan Touring, Ada Lovecode, and Bob Jobs. The company offers cybersecurity services of device management, network monitoring and control, and data loss prevention. With the emerging focus on zero-trust architectures, SecureEnd Solutions decided to develop their endpoint detection and response (EDR) and extended detection and

response (XDR). At the same time, the company sought ISO 27001 certification to increase its competitive advantage. The company's CTO decided to utilize the NIST SP 800-30 r1 and ISO/IEC 27005:2022 guidelines jointly to increase the success of the risk assessment process.

In this case, students will step into the role of a consultant hired by SecureEnd Solutions to help conduct this risk assessment. They will define the scope, identify and classify assets within the defined scope, recognize potential threats and vulnerabilities, and evaluate risks based on established standards. Upon completing the exercise, students practice analytical, decision-making, and research skills, as well as critical thinking and problem-solving skills, all essential in risk management.

2. CASE TEXT

In 2017, three friends (Alan Touring, Ada Lovecode, and Bob Jobs) set out to strengthen the digital realm against lurking cyber threats. Their startup SecureEnd Solutions was founded in San Carlos, CA, to "*create advanced endpoint security software, including polymorphic anti-malware and simple threat detection mechanisms for clients' devices*." The mission of their company was "*to provide cutting-edge, reliable, and comprehensive security solutions that empower businesses to operate securely in an interconnected world."*

SecureEnd grew quickly and successfully received $2M in funding in 2019. As a result, the core team expanded. The company started to offer new services and products: 1) device management services (to make sure all clients' devices are updated, patched, and configured securely), 2) network access control services, and 3) data loss prevention (monitoring and controlling data transfer across the client's endpoints). The company rented an office floor in downtown San Jose, CA, with the structure presented in Table 1. The initial software technology stack the company used is listed in Table 2.

On May 12, 2021, President Joe Biden signed an executive order on cybersecurity. The order mandates agencies to implement a zero-trust architecture. This approach operates on the principle of continuous verification and authentication. Zero trust requires minimizing access to the assets necessary to reduce potential insider threats. This model also assumes that breaches are inevitable; therefore, continuous monitoring, risk-based controls, and automated security measures are critical (The White House, 2021).

On September 7, 2021, the Office of Management and Budget (OMB) released a draft of the zero-trust strategy. The strategy requires agencies to make progress in the following (The White House, 2022):

1. Identity: Agencies are required to review their access control practices and implement Multi-Factor Authentication (MFA).
2. Devices: Agencies should have an updated devices list of devices and detect, prevent, and respond to incidents on those devices.
3. Networks: Agencies must encrypt their HTTP and DNS packets and create isolated perimeters.
4. Applications and Workload: Agencies will test their applications thoroughly and rigorously.
5. Data: Agencies must implement data categorization and maintain data and information sharing logs.

Character	Role
Alan Touring	Co-founder and CTO: responsible for the visionary behind the technology
Ada Lovecode	Co-founder and CEO: responsible for driving the company's strategy
Bob Jobs	Co-founder and COO: responsible for overseeing operations
John Doe	Marketing Director: responsible for promoting the company's services. John manages two marketing employees
Dawn Jackson	Sales Director: responsible for managing client relations. Dawn is managing two sales employees
Implementation Team	Five technical employees responsible for deploying end point security solutions at clients' locations
Customer Support Team	Four technical support employees responsible for providing ongoing support, updates, and maintenance for the clients
Accounting Team	A controller and two account managers

Table 1. SecureEnd Solutions Preliminary Hierarchical Structure

In addition to the zero-trust architecture requirement, agencies were mandated to proactively deploy endpoint detection and response tools to hunt malicious and risky activities using EDR platforms. Such EDR *tools monitor endpoints in real time, collect data, and respond on time to malicious and suspicious activities* (The White House, 2022). XDR *solutions are an extension of EDR and offer a more comprehensive approach to security management beyond the endpoint. They provide security across networks, cloud workloads, and servers*. By integrating security across the network, XDR tools provide the context to detect complex and distributed attacks.

SecureEnd Solutions recognized a significant market opportunity in the need for robust cybersecurity solutions. Rather than relying on third-party software to secure clients' devices, the company decided to develop and sell its own XDR and EDR solutions. Despite being a small company, SecureEnd Solutions is adaptable to the dynamic cybersecurity market and has chosen to create its own EDR and XDR tools using in-house artificial intelligence models. The company plans to offer these tools to clients for a one-time installation fee and a monthly subscription.

To do so, SecureEnd Solutions needs to expand its team by hiring two groups of professionals. The first group is a team of researchers specialized in artificial intelligence and cybersecurity. They will be responsible for designing an AI-based tool. This team will comprise *eight researchers* with expertise in artificial intelligence (specifically deep learning and neural networks) and cybersecurity (networks, protocols, encryptions, and malicious software). The second group is a team of developers who will program the tools. Suzan, the head of development, will lead the development team, consisting of five frontend and backend developers, five QA testers, a team lead, four UI/UX designers, two database administrators, and two DevOps engineers.

In summary, SecureEnd Solutions hired two teams: the development team led by Suzan and the research team, to build their own XDR and EDR solutions.

3. THE SOFTWARE DEVELOPMENT PROCESS

In relation to the development of EDR and XDR, Suzan has exclusive access to the researchers' private communication channel on Slack and the shared research folder on the company's server. Suzan's access is granted due to her role in translating research findings and designs into stories and backlogs. Under the supervision of Alan Touring, the CTO, Suzan translates research findings into technical requirements, makes architectural decisions, and assigns tasks to the development team members. Suzan creates the backlogs (tasks) on GitLab to communicate the requirements to the development team. Once the backlogs are created, the UI/UX designers will create wireframes and design the EDR and XDR software pages. After the design is finalized, the database engineers will design and architect the database.

After the designs and database architecture are approved, Suzan sets up the project repository, and the developers clone the project to set up their environment. This involves choosing the database (NoSQL), setting up the backend programming language (C++) using software (CLION), setting up the frontend programming language (JavaScript) using the software WebStorm, and setting up the environment using Docker. The developers will then work on development according to their assigned tasks in separate branches.

Asset Name	Purpose	User	Location	Risk
VMware Workspace One	Software for clients to manage users' access to the organization's resources from the devices they use to increase their productivity	Implementation Team, Support Team	Cloud	Moderate
Microsoft Windows Server 2019	Software to manage in house endpoints and clients	All Teams	On premise	High
McAfee Total Protection	Software for Data Loss Prevention that SecureEnd sells to its clients	Implementation Team, Support Team		
Cisco Identity Services Engine (ISE)	Software for ensuring only compliant and secure devices can access the network	Implementation Team, Support Team		
SolarWinds Remote Monitoring & Management	Software for monitoring, managing, and maintaining client endpoint devices and networks	Implementation Team, Support Team		
Cisco AnyConnect VPN	Software for remote connection to EndPoint Secure Server	Support Team		
Slack	Team communication and collaboration software	All Teams including Developers and Research Team		
Jira	Project management software used by the development team	Developers Team		
Asana	Task management software	Developers Team, Research Team		
HubSpot	Customer relationship management (CRM) software	Sales and Marketing Team		
Freshdesk	Support ticketing and customer support software used by the support team	Support Team		
Gusto	Human resources management relations. Things related to payroll, and benefits software	Human resources management, payroll, and benefits software		
QuickBooks	Accounting and invoicing software	Accounting department		
GitLab	Software for version control and code hosting on private repositories	Developers		

Note: This table is to be completed by the students in Q2 for the assets that are within the scope.

Table 2. The Technology Stack Used in SecureEnd Solutions

After developers complete their tasks, they combine their individual codes for the initial testing phase, which includes automated unit testing using Git hooks (a tool integrated into GitLab). If no issues are detected, the branches are pushed into a secondary repository for manual testing by the QA testers. Automated testing is also conducted using a Python-coded program. If no issues are found, the code undergoes a peer review for quality, libraries, and dependencies. Finally, the secondary repository branches are merged into the master branch.

Then, the CI/CD team automates the code deployment via GitLab actions. Suzan pushes the code and its documentation for production versions. The technical team required software beyond what SecureEnd Solutions already has, as listed in Table 2. These additional software tools are assigned to the Developer Teams and listed next:

- Docker,
- Kubernetes,
- NoSQL
- CLion and WebStorm IDEs by JetBrains.

A copy of the source codes is stored on the company's server in case of interruption on GitLab. The developers' scrum process is supported by Jira, in which the team members' tasks are planned, and continuous integration and continuous deployment are implemented. Figure 1 shows the steps in the software development process. In 2022, the marketing team forwarded a lead to the sales team from CreativeOil, an international firm operating in the oil industry. Dawn Jackson and her sales team collaborated with CreativeOil to understand their needs and tailor products and services to safeguard their network and end devices. As a result, SecureEnd Solutions successfully closed a deal with an installation fee of $3 million and an annual subscription of $1 million in July 2022. During the 2022 campaign, from which SecureEnd Solutions secured the contract with CreativeOil, John Doe and his marketing team realized that being ISO/IEC 27001 certified would improve their chances of attracting new clients and sharpening their competitive edge. It makes perfect sense for a cybersecurity company to demonstrate that they have been certified by a reputable international agency like the International Organization for Standardization!

Alan Touring, the CTO, has led the initiative to get the company ISO cybersecurity certified. To fulfill this requirement, Alan decided to adopt the information security risk assessment guideline ISO/IEC 27005:2005. ISO/IEC 27005:2022 is a widely used guideline for risk assessment. It places emphasis on alignment with organizational context and adherence to broad risk management principles. Alan also decided to integrate this guideline with NIST SP 800-30 to ensure an effective cybersecurity risk assessment process.

4. CASE STUDY QUESTIONS

Alan decided to start the risk assessment process by establishing the context of risk management. This step involves identifying the risk evaluation criteria, impact criteria, and risk acceptance criteria. To achieve this, Alan needs a team of experts with strong understanding of the technologies used by SecureEnd and the current cybersecurity landscape to identify related threats and achieve the company's business goals. Looking through the slim list of employees in the startup, Alan decides that he needs outside expertise. He immediately recalls your name as one of the rising stars in risk management to accomplish this task. He calls you in for an early meeting.

You are excited and slightly nervous to meet the legendary Alan Touring. This is the first time you have been hired as a consultant by one of the leaders of the industry. During the meeting, you take notes and start strategizing. It is apparent that the first step is to combine ISO/IEC 27005:2022 and NIST SP 800-30 for the risk assessment approach. Alan asks you to use the evaluation criteria based on the tables listed in NIST SP 800-30, which include D-3: Characteristics of Adversary Capabilities; D4, D5, D6, D7, E-4: Relevance of Threat Events; F-2: Vulnerability Severity; G-2: Likelihood of Threat Event Initiation; G-3: Likelihood of Threat Event Occurrence; G-4: Likelihood of Threat Event Resulting in Adverse Impacts; G-5: Overall Likelihood; H-3: Impact of Threat Events; I-2: Level of Risk; I-3: Level of Risk.

At the end of the meeting, Alan emphasized that, unfortunately, cybersecurity is not a priority for most startups. However, he wants you to understand that for SecureEnd, it is an integral part of the business and essential for its survival. He finally closes his laptop and, right before he leaves the boardroom, says, "We have a responsibility for our clients to secure their systems, and I trust you, as our consultant, to help us achieve this goal."

You are finally back in your office. A moment later, your phone alerts you to a new email. It is from Alan, thanking you for the meeting and wishing you good luck. He has also attached a document that provides details and background information about SecureEnd. After analyzing the situation outlined in the document (this case study), you put together an initial plan to address SecureEnd's needs.

1. As a consultant hired by SecureEnd Solutions, you must prepare a recommendation for the scope of the risk assessment? *The focus of the scope should be on the business processes necessary for SecureEnd Solutions to achieve its mission and goals*.
2. After defining the scope, create a list of the company's assets within this scope. Categorize each asset based on ISO/IEC 27005:2022 asset criteria. Assign an owner to each asset and identify its location. Consider the possibility that not all company assets need to be part of the assessment.
3. Identify the threat sources that can initiate threat events on the identified assets.
4. List all the threat events that affect the identified assets. For each threat event, identify which source is related to the threat from the threat sources identified above in Step 3. Rate each threat event's relevance based on NIST SP 800-30 Table E-4. This question requires researching the industry and the common vulnerabilities and exposure databases to identify a rational relevance.
5. Identify the existing controls at SecureEnd Solutions. If a control is not explicitly mentioned, it is missing.

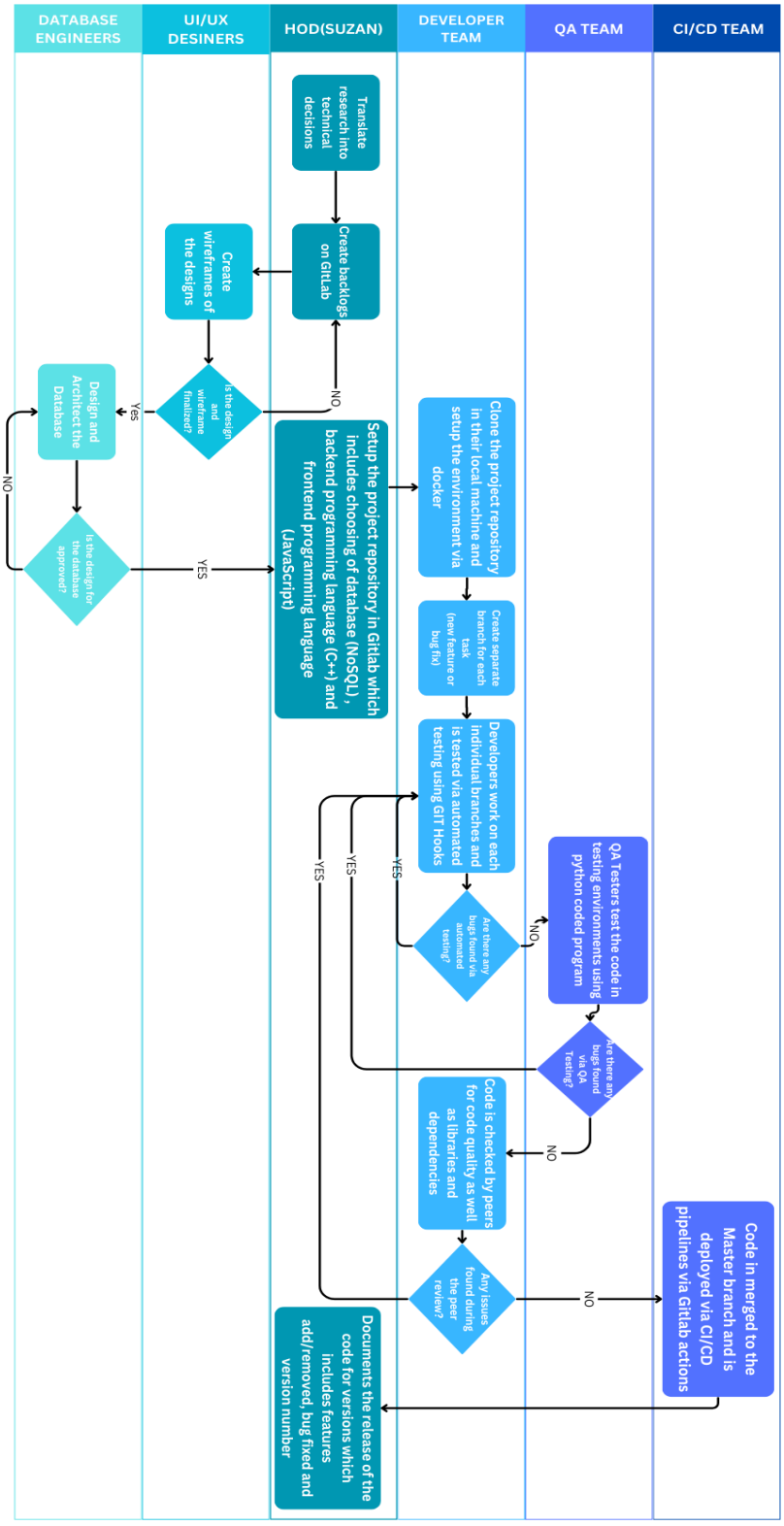


Figure 1. The Software Development Business Process Model

6. Identify the vulnerabilities of each asset. For each identified vulnerability, rate the severity of the vulnerability based on NIST SP 800-30 Table F-2: "vulnerability severity." According to definitions of vulnerability, it can result from the threat source having capabilities higher than the controls currently in place. To help measure a reasonable vulnerability severity, it is recommended to identify the controls that exist for the assets.
7. Create the risk analysis table. Use the NIST SP 800-30's tables below:
   a. Table G-2: the likelihood of threat initiation
   b. Table G-3: the likelihood of threat occurrence
   c. Table G-4: the likelihood of the threat event resulting in adverse impacts
   d. Table G-5: Overall likelihood
   e. Table H-3: Impact of threat events.
   f. Table I-2: the level of risk (combination of likelihood and impact)
   g. Table I-3: the level of risk

Finally, create a risk priority matrix, a matrix of assets and threats that highlights the risk of each threat event on each asset. This matrix is used to prioritize risks.

4. CONCLUSION

Conducting a comprehensive risk assessment is crucial for SecureEnd Solutions to achieve ISO/IEC 27001 certification, enhancing its market position and client trust. This case study aims to simulate a real-world scenario where students must apply their knowledge and skills to solve practical problems. By addressing the risk assessment needs, students help SecureEnd Solutions safeguard its operations and continue providing cutting-edge cybersecurity services. The deliverables produced by the students will be instrumental in supporting the company's mission and goals, highlighting the importance of their work.

5. REFERENCES

Al Fikri, M., Putra, F. A., Suryanto, Y., & Ramli, K. (2019). Risk Assessment Using NIST SP 800-30 Revision 1 and ISO 27005 Combination Technique in Profit-Based Organization: Case Study of ZZZ Information System Application in ABC Agency. *Procedia Computer Science*, 161, 1206-1215. https://doi.org/10.1016/j.procs.2019.11.234

Alzoubi, H. M. (2022). BIM as a Tool to Optimize and Manage Project Risk Management. *International Journal of Mechanical Engineering*, 7(1), 6307-6323.

International Organization for Standardization (2022). *Information Security, Cybersecurity and Privacy Protection — Guidance on Managing Information Security Risks* (ISO/IEC 27005:2022). https://www.iso.org/standard/80585.html

Joint Task Force Transformation Initiative (2012). *Guide for Conducting Risk Assessments* (National Institute of Standards and Technology Special Publication 800-30). https://doi.org/10.6028/NIST.SP.800-30r1

Rodríguez-Espíndola, O., Chowdhury, S., Dey, P. K., Albores, P., & Emrouznejad, A. (2022). Analysis of the Adoption of Emergent Technologies for Risk Management in the Era of Digital Manufacturing. *Technological Forecasting and Social Change*, 178, 121562. https://doi.org/10.1016/j.techfore.2022.121562

The White House (2021, May 12). Executive Order on Improving the Nation's Cybersecurity. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

The White House (2022, January 26). Office of Management and Budget Releases Federal Strategy to Move the U.S. Government Towards a Zero Trust Architecture. https://www.whitehouse.gov/omb/briefing-room/2022/01/26/office-of-management-and-budget-releases-federal-strategy-to-move-the-u-s-government-towards-a-zero-trust-architecture/

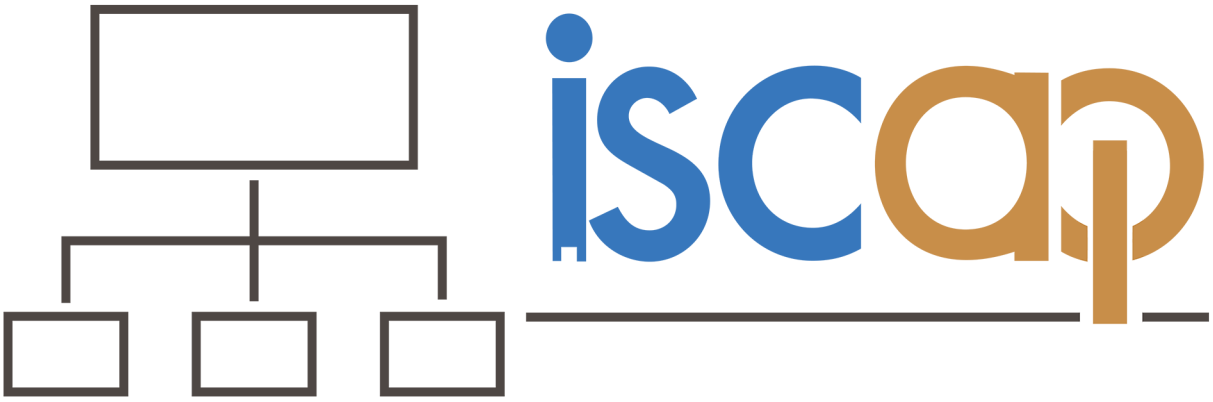
AUTHOR BIOGRAPHIES

Muhammad Al-Abdullah is an assistant professor of cybersecurity at the John H. Sykes College of Business at the University of Tampa. He earned his PhD from Virginia Commonwealth University. His research focuses on cybersecurity, blockchain, anti-money laundering, machine learning, and large language models. He has authored multiple journal articles, book chapters, and conference papers, with recent publications in journals such as the *International Journal of E-Business and the Journal of Digital Policy*.

Alper Yayla is an associate professor of cybersecurity and the director of cybersecurity programs at the John H. Sykes College of Business at The University of Tampa. He earned his Ph.D. degree in Management Information Systems from Florida Atlantic University. His research focuses on information security governance and training, information technology leadership, and strategic alignment. He has authored multiple articles in journals, including *Decision Sciences*, *European Journal of Information Systems*, *Journal of Information Technology*, and *Journal of Strategic Information Systems*.

Mohammed Salem Atoum is an assistant professor in the University of Jordan. He earned his Ph.D. from Universiti Tenologi Malaysia (UTM). His research interests include Information Security, Blockchain, and Risk Management.

INFORMATION SYSTEMS & COMPUTING ACADEMIC PROFESSIONALS



STATEMENT OF PEER REVIEW INTEGRITY

All papers published in the ***Journal of Information Systems Education*** have undergone rigorous peer review. This includes an initial editor screening and double-blind refereeing by three or more expert referees.

ISSN: 2574-3872 (Online) 1055-3096 (Print)