DOI: https://doi.org/10.48009/3_iis_2022_122

OSG practices in responsibility/accountability, awareness, compliance, and assessment: A qualitative analysis

Sushma Mishra, *Robert Morris University, mishra@rmu.edu*
Peter Draus, *Robert Morris University, draus@rmu.edu*
Natalya Bromall, *Robert Morris University, bromall@rmu.edu*
Kevin Slonka, *Saint Francis University, kslonka@francis.edu*

Abstract

Organizational security governance (OSG) practices require a holistic approach to addressing all security domains in an organization. Research identifies multiple OSG domains that are important for effective practices. This study looks at four domains of OSG: 1) Responsibility and accountability, 2) Awareness, 3) Assessment, and 4) Compliance. These domains have been identified in the extant literature as crucial for the success of the OSG program. This qualitative study explores the experiences of security professionals regarding security practices and initiatives in these four domains. Interview data were analyzed, and thematic analysis was performed. Results suggest all four domains are essential for organizations for effective security governance. Implications for research and practice are drawn, and future research directions are suggested.

Keywords: organizational security governance, responsibility, accountability, auditing, awareness, assessment, compliance, qualitative

Introduction

With the increased number of cybersecurity threats, many organizations require mandatory security training for all employees, involve top management in security policies, and enforce constant monitoring. However, all these measures are still often unable to provide an adequate defense. Organizations face threats so complex that few organizations follow effective and comprehensive defense strategies (Tagarev, Davis, & Cooke, 2022).

The theoretical framework of organizational security governance is well established in literature; many research studies recommend following its steps, such as establishing awareness and training, conducting assessments, and auditing, measurement, and reporting. The studies offer specific recommendations for designing and maintaining a successful security governance strategy. Unfortunately, there is a significant gap between the theory and the practical implementation. Developing an effective security governance strategy poses a significant challenge for numerous reasons: lack of administration and leadership inclusion, ineffective measurement and reporting, and complexity of the process, which leads to the employees' lack of awareness. Even with the increased involvement of the executive management, there are still data breaches, phishing attacks, and other security threats (Corris, 2010). In many cases, organizations either do not state specific security governance objectives or do not communicate them to involved parties, which results in a lack of understanding of these objectives (Mishra, 2015).

Connecting the theoretical framework and its implementation in practice would help researchers understand the specific challenges organizations face, identify the most common issues, and provide recommendations based on the successful experiences reported by security managers.

The theoretical framework of organizational security governance includes seven critical domains defined by AlGhamdi (2020): (1) Responsibility and accountability, (2) Awareness, (3) Compliance, (4) Assessment/auditing, (5) Measurement, (6) Reporting, and (7) Monitoring. The goal of this research is to explore the strategies that organizations follow in enforcing the first four of the seven domains, which will be achieved by answering the following four research questions:

RQ1: How does responsibility & accountability structure influence Organizational Security Governance (OSG) practices?
RQ2: How do awareness initiatives influence OSG practices?
RQ3: How do compliance measures influence organizations' OSG practices?
RQ4: How do assessment & auditing influence OSG practices?

Literature Review

Organizational Security Governance

Blum (2020) lists the main functions of OSG as "Charter or mandate the security program," "Manage, control, and report on risk," "Coordinate security projects and manage issues," "Manage security policy," and "Allocate security budgets and resources." It is essential to recognize that this is a governance activity, not simply a framework for IT security; it is part of the overall organizational governance. Schinagl & Shahim (2020) noted the expansion into the top board, strategic level, from the technical level when they wrote, "landscape has shifted "from the basement to the boardroom," that is, from a narrowly focused technical issue towards a strategic business issue and a top priority item for the board" (p. 283).

Another driving force behind the expansion into the boardroom is the increasing number of laws and regulations impacting data, privacy, and security. Khoo, Harris, & Hartman (2010) wrote, "Organizations must elevate the issue to a corporate governance priority to systematically strengthen information security at all levels of the organization" (p. 51). Some researchers have looked at the relationship between information security governance strategic alignment and information security governance and found "that effective information security governance strategic alignment greatly improves organizations' risk management, resource management, performance measurement, and delivers business value" (Yaokumah, & Brown, 2014, p.51).

Frameworks

As the importance of the information and information infrastructure to the organization grew, the governance structures needed to evolve to keep up. An expanded structure was required to help manage this growing complexity. Multiple frameworks were developed to assist with this challenge; some were part of the general organizational governance structure, and some were specific to the information security realm. A partial list of these frameworks includes ISO/IEC 38500 and COSO, which are focused more on governance itself and have high levels of abstraction. In contrast, others are focused more on IT tactics and strategies such as ISO/IEC 17779 and ITIL. Of course, ISO/IEC 17779 is the more detailed and focused framework, making it more prevalent among technical managers; it is less of a framework for overall organizational governance (Von Solms, 2005). Other frameworks cover higher governance levels down to the tactical level and are in the middle of the abstraction layer, such as COBIT 4/5 (De Haes, Van

Grembergen, & Debreceny, 2013). Some researchers have looked at using COBIT 5 to improve security. One such researcher looked at accounting information systems and noted that the framework included governance and implementation processes (Al-Fatlawi, 2021).

Other researchers have found deficiencies in COBIT's use for information security even though it is a very successful and popular framework (Pratiwi, Indah, Jauhari, & Firdaus, 2020). In a literature review in this area, AlGhamadi (2020) found that when using frameworks for information security governance, there are seven critical success factors: 1) Responsibility and accountability, 2) Awareness, 3) Compliance, 4) Assessment/Auditing, 5) Measurement, 6) Reporting, and 7) Monitoring.

Problems with the current situation

Current problems with Information Security Governance include the lack of inclusion of top organization leaders. After reviewing security governance in the healthcare industry, some researchers concluded that the increasingly complex laws and regulatory environment exasperated the problems, writing, "the preponderance of healthcare-related laws, compliance regulations, and security guidance frameworks serve to complicate the cybersecurity challenge further and too often results in senior leadership assuming a state of blissful ignorance" (Abraham, Chatterjee, & Sims, 2019, p.539).

Others have noted the difficulty in measurement and reporting as an issue, as well as the breadth of the framework. Some researchers have worked on creating formulas to help the security auditors in their duties to try and help solve this problem. They found that the data was "deeply influenced by the expertise of the assessor and his/her sensitivity" (Angelini, Bonomi, Ciccotelli, & Palma, 2020, p. 1). The disconnect from the everyday work and the complexity of the entire process for most workers was also listed as an issue by Ridley, Young, & Carroll (2004). Sadok, Alter & Bednar (2020) concluded that "security practices remain an illusory activity in their real-world contexts" (p. 18). Phishing attacks are a security activity where this is often seen. Data gathering and employee testing in phishing are easy across many organizations. Some researchers have suggested gathering data by using scenario-based analysis instead of looking at sample phishing attacks on workers' emails. They hope to collect data on their understanding of different situations and the user's knowledge of phishing. The goal is to acquire a broader data set on the employee's knowledge of the issues and their knowledge of the possibility of data loss (Das, Nippert-Eng, & Camp, 2022).

Responsibility & Accountability and Awareness

Alghamdi, Win, & Vlahu-Gjorgievska (2020) have identified clarity in responsibility and accountability (R&A) in organizational structure as a critical determinant of efficient corporate security governance practices. In their meta-analysis of extant research literature in the security governance area, they list many vital factors under R&A that lead to the strategic and successful implementation of a security governance program. It is pertinent that organizational security governance objectives are aligned with the responsibility structure in the organization (Mishra, 2021).

Many studies have mentioned the importance of awareness for prompting OSG in organizations; awareness is an essential factor in the success of the OSG program. Awareness can contribute to enhancing knowledge of the organizational security practices to create trust between the organization and its employees and raise the realization of security risks that the organization can face (Alghamdi et al., 2020). Lack of security control awareness is a significant obstacle to effective security governance (Johnson, 2006). Mishra (2015) argues that controls training programs could illustrate the relevance of controls with work-related examples. Education can be provided through regular training sessions about the need and usage of the controls.

Compliance and Auditing

Compliance with security policies requires some form of testing and auditing. It is not just governance that can be improved by including the upper level of the organization. Steinbart et al. (2018) found that as the quality of the relationship between the auditors and upper management improved, the quality of security improved. Individual IT security audits for specific systems have been part of IT systems for a long time, and there are mature models available. However, auditing models for the complete security of an organization are still being developed. Sabillon (2018) has proposed the CyberSecurity Audit Model (CSAM), which comprises 18 domains that can be rated as Immature, Developing, Mature, or Advanced. Such a model is not connected to a particular framework, such as COBIT. Auditing acts as a catalyst for the management to accelerate its efforts for information systems security governance (Mishra, 2020).

The organization's security practices become more significant than just the security framework employed. The goal of measurement should be that all the data is evaluated as a whole, not just on individual metrics, to provide a better overview of the organization's security practices (Orehek & Petric, 2020). Tan, Ruighaver, & Ahmad (2010) noted that to improve organizational security levels, the security practices need to expand to the workers so that they are not only working to meet specific security metrics. A centralized entity for controls assessment would allow separate budget allocation for security governance functions and help establish a business case for security governance. A controls department would integrate controls into the business processes (Mishra, 2020).

Organizational security governance practices

We have noted that increasing the upper levels of management in the security governance improves security levels. Moreover, a sense of complacency has been reported by other researchers. Sadok, Alter, & Bednar (2020) interviewed 187 employees in 39 organizations concerning the security practices and found that the corporate policies were disconnected from the security activities of the workers. They also found that the employees don't prioritize security policies, concluding that "security practices remain an illusory activity in their real-world contexts" (p. 1). The OSG security practices include how the employees interact with the policies, process, and governance structure. In all organizations, what is policy and what is rewarded are two different things—a recent study surveyed over 300 workers concerning their activities in hypothetical scenarios. The findings indicate that their response was motivated less by any costs based on non-compliance and rather more by benefits (Khatib & Barki, 2021).

In any security culture, some employee interactions with the policies and procedures increase the security level, and some decrease the organization's security level (Da Veiga et al., 2020). By looking at the interplay between security practices and the overall culture of the organization and information security awareness, some researchers have moved beyond the security practices themselves. These researchers noticed a high correlation between the security practices and the overall culture. They suggested that training efforts on security practices alone could be a more efficient use of limited training budgets (Wiley, McCormac, & Calic, 2020). Security practices depend on a comprehensive security governance framework that covers from the boardroom down to the lowest level of workers. Veiga & Eloff (2007) reviewed security practices in academia and industry and made the key recommendation that "the first step in developing an information security culture and empowering the workforce to be aware of their responsibilities towards protecting information assets would be to implement a comprehensive Information Security Governance framework" (p. 370).

To fully understand an organization's OSG practices, we need to gather data about the structure and policies and conduct interviews concerning all aspects of the organization's security practices.

Methodology

Data collection and analysis

A set of interview questions was developed to collect the data about the organizations' perceptions of responsibility, accountability, compliance, and assessment tools. The interview included four question groups, each group matching one of the four domains. In addition, each question group had multiple talking points as a guide for an interviewer in case the respondent missed certain information. Table 1 shows a sample interview question with the sub-questions or talking points.

We conducted 10 interviews with security professionals managing OSG using the designed interview questions. Organization sizes ranged from 65 employees to 200k+ employees and spanned business sectors from healthcare, to financial, to defense. Each interview started with demographic questions, including (1) the type and size of their organization, (2) their title and role within the organization, and (3) the number of years of their relevant experience in cybersecurity. Following the demographic questions were probing questions pertaining to each research question (domain).

Table 1. Sample interview question structure

Question 1: How does the "responsibility and accountability" structure influence the Organizational security governance practices?
• How is security functionality/team organized in your organization?
• How does the reporting structure work? Who does the CISO report to?
• Do you have security committees? Who are the stakeholders involved?
• Is the reporting structure clear if there is a breach situation?
• Is there a sense of ownership for processes/controls etc.?
• How does risk management work? Who is involved in policy development?

Each interview was recorded as an audio file and as plain text with the help of a transcribing tool. The answers were categorized according to the four research domains and by respondents within each domain. Each response was thematically analyzed in two stages. During the first stage, we outlined all emerging themes. A theme was included in the list if it was emphasized by the respondent or mentioned multiple times by one or more respondents. The answers were matched to the themes and then analyzed during the second stage. The results of this analysis are presented in the following section.

Results

This section presents the results of our data analysis. The data is presented research question-wise.

Domain 1: Responsibility and accountability

Our data in this study for responsibility and accountability shows five emergent themes: 1) team structure, 2) reporting structure, 3) committees, 4) clarity in adverse situations, and 5) risk management (Table 2). Responsibility and accountability need to be clearly defined, communicated, and assessed at multiple levels in an organization for alignment with overall OSG objectives. The R&A domain requires that job descriptions be not changed abruptly, clear organizational responsibility for compliance should be defined, individuals should be made responsible for appropriate accesses, and transparency about accountability should be encouraged (Mishra, 2020).

Theme 1 suggests that clarity in team structure allows for transparency in R&A. Our data indicate that the organization's size is essential in organizing teams. Large organizations have large security teams and need clarity in assigning responsibilities. Organizations could structure team R&A through data needs, compliance needs, business needs, or different business functionality needs. A data-centric structure with all security services around the data in multiple layers shows more consciousness of data governance. Other multilayered security models are available based on the nature and scope of services provided. Some services are enterprise-wide, and some are targeted at business units. Depending on the type of organization, appropriate R&A practices should be designed.

Table 2: Responsibility and Accountability

Emerging themes	
Theme 1: Team structure	• Size of the organization is essential. Large organizations have large security teams. It could be aligned through data, compliance, business, or separate security functionality. • Data-centric structure with all services around the data in multiple layers -more conscious of data governance • Multilayered security models based on the nature and scope of services provided. Some services are enterprise-wide, and some are targeted at business units.
Theme 2: Reporting structure	• There is a variety of reporting structures available in organizations depending on the size and nature of the company. • Some standard reporting models involve CISO reporting to CIO or CEO or legal leadership. • Compliance typically is separate functionality that works closely with security.
Theme 3: Committees	• Committees are common involving multiple stakeholders. It could be a security board, privacy board, or council for security controls. • Cross-functional teams for governance at the enterprise, unit, and operational levels. • Different layers of committees focus on different types of needs.
Theme 4: Clarity in adverse situations	• Not much clarity for people who are not directly involved in IR or BCP • Awareness that there is a plan in place to deal with such a situation
Theme 5: Risk management and policy development	• Risk management is essential to understand where does the risk lie in data • Required by regulations • The policy is required to address risk

Theme two shows that there are various reporting structures available in organizations depending on the size and nature of the company. Some standard reporting models involve CISO reporting to CIO or CEO, or legal leadership. Data suggests that regulatory compliance typically is separate functionality that works closely with security.

Theme three is about committees that conduct governance responsibilities and accountability at multiple levels in an organization. Results suggest that committees commonly involve various stakeholders in a company. These committees could be called security boards, privacy boards, or council security controls boards, to name a few. These committees are cross-functional teams for governance at the enterprise, unit, and operational levels. Data suggests that different layers of committees focus on different types of needs for security governance and have to be aligned to overall OSG objectives.

Theme four is about clarity (or lack of it) in responsibility and accountability in an adverse situation such as an incident or disaster. Our data suggest an assigned person/team that one can call upon in an adverse case; however, there was no clarity on who or how to approach someone in this situation. There is an awareness that actions are predefined for individuals in such cases; however, our participants were not clear on these actions.

The last theme for this domain is risk management and policy in the context of responsibility and accountability. Risk management goes hand-in-hand with a clear responsibility structure in an organization. Our data suggest that risk management is essential to understand where the risk lies in data so that R&A can be created around it. Results indicate that most of the risk management is driven by regulations. Organizations form policies to address risk and embed accountability in job responsibilities. Risk management and policies are tools and directives of the organization in developing OSG foundations.

Domain 2: Awareness

Data in this domain suggests four emergent themes 1) awareness role, 2) training nature and frequency, 3) employee outlook and 4) benefits (see Table 3).

Table 3: Awareness

Emerging themes	
Theme 1: Awareness role	• Organizations have a significant emphasis on awareness and training activities. • Depending on the organization's size, formal positions for awareness officers are created. Ongoing awareness activities all year long are common.
Theme 2: Training-nature and frequency	• It is customized to the audience and targeted with a specific purpose. • Used in various ways, such as training on the ground, online, newsletters, talks, etc. • The nature of the training should be more fun so that message is disseminated at a broader level.
Theme 3: employee outlook	• Acceptance is more positive. Employees believe it helps them do their job better, even if it is more work. • It helps them contextualize the purpose of governance practices and the risk associated.
Theme 4: benefits	• It helps in gaining better accountability, coordination in teams, and staying on top of things that should or should not be performed in the organization • Internal and external constituencies appreciate the controls and initiatives due to better understanding.

Theme one suggests that organizations, in general, are invested in raising employee awareness about organizational security governance initiatives and practices. Large organizations with sensitive data have formal roles for awareness officers. These officers are in charge of developing ongoing activities to enhance employees' awareness of security governance activities.

Theme two suggests that various means are utilized to customize training for employees with specific purposes. Different modalities such as on-ground, online, synchronous, and asynchronous methods are used to reach, train, and educate users. Data suggests that training should be made more fun to disseminate the message at a broader level.

Theme three suggests that the employment outlook of these awareness campaigns is mainly positive and accepting. Employees believe it helps them do their job better, even if it is more work. These ongoing awareness activities help users contextualize the purpose of governance practices and the risk associated with non-compliance with associated policies.

Theme four suggests multiple benefits of awareness activities for internal and external constituencies. These activities help in gaining better accountability and coordination in teams. Employees feel more empowered to understand and decide what actions should or should not be performed in the organization. Internal and external constituencies appreciate the controls and initiatives due to better understanding.

Domain 3: Compliance

Domain 3 is about regulatory compliance. We identified three themes in this domain 1) Process, 2) Evaluation, and 3) third party involvement (Table 4). Theme one is about the process of regulatory compliance in organizations. Data suggests that organizations are cognizant of how it handles data. The data lifecycle needs to be mapped to security initiatives to coordinate IT security and compliance. This alignment requires process maturity. Compliance frameworks are highly regulated, and teams working on frameworks must have the right people be appropriately aligned with the business. Meeting regulatory compliance is a significant part of OSG practices, and the process requires guidance in terms of frameworks.

Theme two is about the evaluation of compliance activities and processes. Some compliance frameworks require yearly third-party audits, while others do not. Some organizations prefer using independent evaluators for evaluation purposes. Some businesses contract third-party auditors as part of their team to constantly evaluate the process. In the case of international organizations, working within non-US countries requires audits specific to those countries. Some businesses have to learn continuously about compliance needs and take specialized exams to be eligible. DoD-related organizations have mandated compliance needs and frameworks. Guidelines are provided for self-assessment and reporting the scores to agencies. The capability maturity models approach is used for assessing the compliance process maturity.

Theme three is third-party involvement in compliance activities. For organizations with an international presence, many a time, privacy is regulated by locale/country. NIST 800-171/CMMC dictates privacy (confidentiality) when working with the government. Third parties are involved in getting a fair outlook of the process. A neutral perspective helps in understanding issues. Resources are required to do everything in-house, and contracting third-party services are favorable. There are some challenges in using a third party for compliance purposes. Data ownership and territory need to be clearly defined to reduce the risk involved. There is a contractual or non-disclosure limit as some risk of exposure is always present in using a third party. One of the ways to address this risk is to only have people certified in those providers on the project when utilizing external providers.

Table 4: Compliance

Emerging themes	
Theme 1: Process	• Compliance frameworks are highly regulated • Compliance teams must have the right people and be properly aligned with the business • IT security coordinates with compliance. It's a process that needs alignment and maturity • Cognizant of how we handle our data
Theme 2: Evaluation	• Some compliance frameworks require yearly third-party audits; others do not • Some businesses utilize third parties as part of their team • Working within non-US countries requires audits specific to those countries • Some businesses have to be in continuous learning mode about compliance needs and take specialized exams to be eligible • Capability maturity models used for assessing the compliance process
Theme 3: Third-Party involvement	• When not dealing with compliance frameworks, privacy is regulated by locale/country • When working with the government, NIST 800-171/CMMC dictates privacy (confidentiality) • A neutral perspective helps in understanding issues. Resources are required to do everything in-house • Data ownership needs to be precise. Who owns the data, and is territory clearly defined? Reduced third-party risks • There is a contractual or non-disclosure limit. Some risk of exposure is always present in using the third party • When utilizing external providers, only have people certified in those providers on the project

Domain 4: Assessment

Domain 4 is about the assessment of governance initiatives. We identified four themes in this domain 1) Alignment with controls and operations, 2) policy evaluation, 3) architecture evaluation, and 4) BCP evaluation (Table 5).

Theme one points to aligning controls and operations with OSG objectives using continuous auditing and evaluation mechanisms. Data suggests that internal and third-party teams are involved in preparing assessments and auditing. Risk assessment, control assessment, and internal auditing align with overall OSG objectives. Some organizations have instituted independent control towers to evaluate centralized enterprise-wide control effectiveness and remediation. Centralized control functionality allows constant assessment of control effectiveness and alignment with the risk profile. Data suggests that business and security teams meet regularly to align goals. It helps them perform gap analyses and address the issues based on the framework being used by the organization. Different maturity levels are assigned based on the assessment performed by these teams.

Theme two is about policy evaluation. Our data suggest that policies and procedures are written around the particular frameworks, and various committees make this work possible. Constant evaluation of policies requires the proper structure to collect and evaluate data around policy effectiveness. Continuous steering committee meetings for evaluating key metrics are performed in this regard.

Theme three is architecture evaluation for the assessment of OSG activities. Control domain authorities represented by auditors sit in regular meetings and evaluate controls, objectives, and performance. These form the second line of defense as an advisory group to the rest of the security functionality. The constant evaluation of security blueprints by advisory groups is performed by advisory groups. Specific sub-domains are identified for review and assessment by advisory services. Third-line audit services perform regular audits in a coordinated approach. Smaller and targeted areas for review are selected in an ongoing manner. For DoD-related organizations, guidance is provided for federal agencies for self-attestation and creating a score.

Table 5: Assessment and Auditing

Emerging themes	
Theme 1: Alignment with controls/operations	• Internal and 3rd party teams are involved in preparing and auditing • Risk assessment, control assessment, and internal auditing is done and aligned • Independent control tower to evaluate centralized enterprise-wide control effectiveness and remediation • Business and security meet regularly to align goals • Perform gap analysis and address the issues based on the framework being used. Different levels of maturity are assigned based on the assessment
Theme 2: Policy evaluation	• Policies and procedures are written around the particular frameworks • Various committees make this work possible • Continuous steering committee meetings for evaluating key metrics
Theme 3: Architecture evaluation	• Control domain authorities represented by auditors sit in regular meetings and evaluate controls, objectives, and performance. These are the second-line advisory group. • Specific sub-domains are identified for review and assessment by advisory services • Third-line audit services perform regular audits. Smaller and targeted areas for review. • The guidance provided for federal agencies for self-attestation and to create a score. Controls the evaluation process internally.
Theme 4: BCP evaluation	• BCP is regularly tested and updated • With no physical network, BCP focuses more on operations than physical infrastructure • Mandated by regulations

Theme four is business continuity evaluation. BCP is regularly tested and updated in organizations since it is highly regulated and mandated by law. With no physical network, BCP focuses more on operations than the physical infrastructure part of the planning. Organizations do regular mocks drills and documentation to show compliance.

Discussion

Each of the four domains in this study has implications for practice. The first domain, Responsibility and Accountability centers around the core theme of structure within an organization. While a current fad may be the flat organizational structure, this research suggests that a role-based structure is necessary for the proper alignment of R&A at multiple levels of an organization (Lee, 2021). From the bottom "team" level up to the strategic "committee" level, a clear understanding of one's place within the organization is required for the organization to function operationally, strategically plan for the future, and, possibly most importantly, mitigate risks to the organization and have a clear plan of action for when those mitigations fail. Research in this area has emphasized the importance of reporting structure for sound OSG practices.

Organizations must also have good security awareness campaigns to ensure that all employees at all levels of the company are continuously updated on the tactics, techniques, and procedures (TTP) of adversaries within their operating domain. If these campaigns are developed in a manner that not only ensures adequate education but also keeps employees stimulated and interested via entertaining and compelling presentation methods (Wu, Tien, Hsu, & Wen, 2021), they will not only be well-received but also yield greater benefits across the organization (Thangavelu, Krishnaswamy, & Sharma, 2021). Responsibility for security awareness should be dedicated to a discrete role/team within the organization to ensure its proper execution.

Domains three (compliance) and four (assessment) are often collaborative efforts in organizations. Understanding the regulations to which a company is held is of the utmost importance, especially when multiple regulating bodies are involved and when foreign governments impose regulations. Many organizations find that this work cannot be completed by a single employee over the course of a few weeks but is a highly collaborative effort between many different teams within the organization. These teams focus on the evaluation of policy, system architecture, and business continuity, and the more granular focus on individual security practices dictated by the regulations (Antunes, Maximiano, & Gomes, 2022; Goel, Kumar, & Haddow, 2020). Some larger organizations have specialized third parties contracted as part of their internal teams to ensure unbiased assessments (Razavi, Collins, Wilson, & Okereke, 2021), and, depending on the regulation, third-party involvement may be mandatory to achieve regulatory certification ("Cybersecurity Maturity", 2020).

Ultimately, the degree to which an organization separates these activities is a function of its size. This study, however, recommends that organizations have separate teams for these security and governance roles instead of the common practice of employees being assigned multiple roles (e.g., the CEO also being the IT manager or the most senior developer also being in charge of security). The utilization of third parties is also recommended, minimally, for unbiased assessments of an organization's security posture in preparation for regulatory audits.

Participants in this study were also keen to address the need for agility in the consistently changing threat landscape to prevent breaches, insider threat incidents, and the harmful effects of third-party compromises. This agility (and the resulting expertise requirement) is essential when the organization operates in multiple sectors, which leads to multiple regulatory obligations (NIST 800-171/CMMC in federal contracting, HIPAA in healthcare, etc.).

Conclusion

This qualitative analysis of security professionals' experiences of OSG practices in responsibility and accountability, awareness, compliance measures, and assessment/auditing uncovered key aspects that are crucial to organizational success. The results validated the existence and usefulness of the four OSG domains that were studied and offered insights from which other organizations can learn. Future research is necessary to understand the remaining three OSG domains from the seminal study and offer similar insights.

References

Abraham, C., Chatterjee, D., & Sims, R. R. (2019). Muddling through cybersecurity: insights from the US healthcare industry. *Business Horizons, 62*(4), 539-548.

Al-Fatlawi, Q. A., Al Farttoosi, D. S., & Almagtome, A. H. (2021). Accounting information security and its governance under COBIT 5 framework: a case study. *Webology, 18* (Special Issue on Information Retrieval and Web Search), 294-310.

AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2020). Information security governance challenges and critical success factors: systematic review. *Computers & Security, 99*, 1-39.

Angelini, M., Bonomi, S., Ciccotelli, C., & Palma, A. (2020). *Toward a context-aware methodology for information security governance assessment validation*. International Workshop on Cyber-Physical Security for Critical Infrastructures Protection, Springer, 171-187.

Antunes, M., Maximiano, M., & Gomes, R. (2022). A client-centered information security and cybersecurity auditing framework. *Applied Sciences, 12*, 1-15.

Corriss, L. (2010). *Information security governance: integrating security into the organizational culture.* Proceedings of the 2010 Workshop on Governance of Technology, Information and Policies, 35-41.

Cybersecurity Maturity Model Certification Requirements, DFARS 252.204-7021 (2020). Retrieved from https://www.acquisition.gov/dfars/252.204-7021-cybersecurity-maturity-model-certification-requirements

Das, S., Nippert-Eng, C., & Camp, L. J. (2022). Evaluating user susceptibility to phishing attacks. *Information & Computer Security, 30*(1), 1-18.

Da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organizational information security culture—Perspectives from academia and industry. *Computers & Security, 92*, 1-23.

De Haes, S., Van Grembergen, W., & Debreceny, R. S. (2013). COBIT 5 and enterprise governance of information technology: building blocks and research opportunities. *Journal of Information Systems, 27*(1), 307-324.

Goel, R., Kumar, A., & Haddow, J. (2020). PRISM: a strategic decision framework for cybersecurity risk assessment. *Information & Computer Security, 28*(4), 591-625.

Johnson, E.C. (2006). Security awareness: switch to a better programme. *Network Security, 2006*(2), 15-18.

Khatib, R., & Barki, H. (2021). How different rewards tend to influence employee non-compliance with information security policies. *Information & Computer Security, 30*(1), 97-116.

Khoo, B., Harris, P., & Hartman, S. (2010). Information security governance of enterprise information systems: An approach to legislative compliant. *International Journal of Management & Information Systems (IJMIS), 14*(3).

Lee, S. (2021). The myth of the flat start-up: reconsidering the organizational structure of start-ups. *Strategic Management Journal, 43*(1), 58-92.

Mishra, S. (2015). Organizational objectives for information security governance: a value focused assessment. *Information & Computer Security, 23*(2), 122-144.

Mishra, S. (2020). Examining organizational security governance (OSG) objectives: how strategic planning for security is undertaken at ABC corporation? *Journal of Information Systems Applied Research, 13*(2), 13-24.

Mishra, S. (2021). Interpreting organizational security governance objectives for strategic security planning. *Journal of Information Systems Applied Research, 14*(3), 30-43.

Nicho, M. (2018). A process model for implementing information systems security governance. *Information & Computer Security, 26*(1), 10-38.

Orehek, Š., & Petrič, G. (2020). A systematic review of scales for measuring information security culture. *Information & Computer Security, 29*(1), 133-158.

Pratiwi, A., Indah, D. R., Jauhari, J., & Firdaus, M. A. (May 2020). *Security capability assessment on network monitoring information system using COBIT 5 for information security*. In Sriwijaya International Conference on Information Technology and Its Applications (SICONIAN 2019), 167-171.

Razavi, A., Collins, S., Wilson, A., & Okereke, E. (2021). Evaluating implementation of International Health Regulations core capacities: using the Electronic States Parties Self-Assessment Annual Reporting Tool (e-SPAR) to monitor progress with Joint External Evaluation indicators. *Globalization and Health, 17*, 1-7.

Ridley, G., Young, J., & Carroll, P. (January 2004). *COBIT and its utilization: a framework from the literature*. Proceedings of the 37th Annual Hawaii International Conference on System Sciences Proceedings, 1-8.

Sabillon, R. (2018). A practical model to perform comprehensive cybersecurity audits. *Enfoque UTE, 9*(1), 127-137.

Sadok, M., Alter, S., & Bednar, P. (2020). It is not my job: exploring the disconnect between corporate security policies and actual security practices in SMEs. *Information & Computer Security, 28*(3), 467-483.

Schinagl, S., & Shahim, A. (2020). What do we know about information security governance? From the basement to the boardroom: towards digital security governance. *Information & Computer Security, 28*(2), 261-292.

Tagarev, T., Davis, B.Á. and Cooke, M., (2022). Business, organizational and governance modalities of collaborative cybersecurity networks. *Multimedia Tools and Applications, 81*, 9431–9443.

Thangavelu, M., Krishnaswamy, V., & Sharma, M. (2021). Impact of comprehensive information security awareness and cognitive characteristics on security incident management – an empirical study. *Computers & Security, 109*, 1-24.

Von Solms, B. (2005). Information Security governance: COBIT or ISO 17799 or both? *Computers & Security, 24*(2), 99-104.

Veiga, A. D., & Eloff, J. H. (2007). An information security governance framework. *Information Systems Management, 24*(4), 361-372.

Wiley, A., McCormac, A., & Calic, D. (2020). More than the individual: examining the relationship between culture and information security awareness. *Computers & Security, 88*, 1-8.

Wu, T., Tien, K., Hsu, W., & Wen, F. (2021). Assessing the effects of gamification on enhancing information security awareness knowledge. *Applied Sciences, 11*(19), 1-16.

Yaokumah, W., & Brown, S. (2014). An empirical examination of the relationship between information security/business strategic alignment and information security governance domain areas. *Journal of Law and Governance, 9*(2), 50-65.

Zaini, M. K., Masrek, M. N., & Sani, M. K. J. A. (2020). The impact of information security management practices on organizational agility. *Information & Computer Security, 28*(5), 681-700.