Issues in Information Systems
Volume 24, Issue 3, pp. 116-131, 2023

DOI: https://doi.org/10.48009/3_iis_2023_111

Principles of organizational security governance

Sushma Mishra, *Robert Morris University, mishra@rmu.edu*

Abstract

This study aims to understand the interrelationships of organizational security governance (OSG) objectives and propose paths for accomplishing strategic security planning by using these objectives. Mishra (2015) proposed OSG objectives that are grounded in theory and empirically validated. However, no guidance is provided on "how" to use these objectives in a natural organizational setting for strategic security planning. This research conducts a case study to understand the relationships between OSG objectives. Interviews and secondary internal documents of the organization were used as data sources. The results suggest eight principles of organizational security governance that prescribe various paths to accomplishing strategic security planning. The theoretical implications lie in the unique contribution of these principles for furthering knowledge in security governance research. The contributions to practitioners are in prescribing paths of accomplishing better security preparedness by implementing the principles. Theoretical anomalies are identified, and suggestions for future research are presented.

Keywords: organizational security governance, strategic planning, principles, case study, interpretive, qualitative

Introduction

Organizational Security Governance (OSG) provides a set of responsibilities and practices typically used by the company's management to determine the direction to manage business risks and appropriate organizational resources (ISACA, 2012). Organizations need OSG objectives aligned with stakeholders' values for optimal results from security plans to ensure proactive security initiatives to control current and future risks. For an organization to strategically prepare for effective, comprehensive security activities, the planning needs to be rooted in Organization Security Governance (OSG) objectives. Mishra (2015) proposed a set of six fundamental and seventeen means OSG objectives grounded in value theory and empirically validated. These value-driven objectives contextualize the purpose and provide a sense of ownership to employees who are the developer and users of security initiatives. These OSG objectives offer clear guidance about "what" should be done for strategic security planning (see Mishra, 2015, for details). However, these objectives do not clarify "how" to use the objectives to develop security activities. There is no guidance about the interrelationships of these objectives and how the linkages between particular objectives help target specific areas in the overall security plan. Many studies in this domain propose similar domains of OSG activities. However, there is insufficient clarity about how these domains interact and strengthen a particular area of security planning.

This study explores the interrelationships of these OSG objectives in natural organizational settings. The goal is to provide specific principles of OSG that postulate how using the interplay of particular objectives allows for accomplishing specific strategic objectives for security planning. The study addresses the following research question: What are the interrelationships among OSG objectives to facilitate achieving strategic objectives in an organization? This study proposes eight principles of OSG to answer the above question. The following section briefly introduces the literature review in organizational security governance research and discusses the study's methodological approach. A section describing the principles of OSG follows with discussions and contributions of the study.

Literature Review

Organizational security governance (OSG) is a set of responsibilities and practices exercised by management to provide a strategic direction and set the tone for adequate security policies and procedures (Westby & Allen, 2007). Several studies identify good OSG objectives for comprehensive security programs in organizations, and Mishra (2015) used a value-focused approach to develop OSG objectives. This study proposed six fundamental and seventeen means objectives for OSG that are rooted in the values of stakeholders in an organization. AlGhamadi et al. (2020) critically reviewed literature in the OSG domain. They proposed a condensed list of seven domains and 27 key areas under this domain for a successful OSG program. These domains are 1) Responsibility and accountability, 2) Awareness, 3) Compliance, 4) Assessment/Auditing, 5) Measurement, 6) Reporting, and 7) Monitoring. These domains were used in two different studies, Mishra et al. (2022) and Slonka et al. (2023), to understand the importance of these domains in an actual organizational setting. The results suggest that all seven domains are regularly being used in organizations to cover the entire security landscape for comprehensive practices.

Regulatory compliance is considered a driving force for OG practices and policies. Khoo, Harris, & Hartman (2010) observe, "Organizations must elevate the issue to a corporate governance priority to systematically strengthen information security at all levels of the organization" (p. 51). Many studies 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). Another area of concern for OSG is the need for top management commitment. Abraham, Chatterjee, & Sims (2019) observe many regulations with specific compliance needs regarding security governance preparedness. Still, the lack of involvement on the part of senior management complicates the issue.

Slonka et al. (2023) studied the impact of measurement, reporting, and monitoring on OSG practices. The results suggest that all three domains are essential for OSG and have practical implications. Measurement is considered the doorway to the other two domains of reporting and monitoring. Without proper measurement, there can be no reporting or monitoring. This study suggests that measurement must be implemented at various organizational levels to be effective. Mishra (2020) studied the OSG objective proposed in the literature and its correlation with an organization's upper, middle, and lower management level managers. The results suggest that the perception of OSG practices is related to the role of a manager in the organization. The main characteristics of OSG are to "charter or mandate the security program" and coordinate security projects and management issues while managing security policies (Blum, 2020). Schinagl & Shahim (2020) note that the expansion of OSG into the top board, and strategic level, from the technical level, has brought OSG practices into the limelight.

In summary, research in this identifies many OSG objectives important for successful security governance practices. These objectives are related to critical success factors that improve organizations' overall security posture. However, there is a dearth of studies about the interrelationships of these OSG objectives. There is a need for a practical understanding of how these OSG domains interact and their interrelationships, leading to a more secure organization. This study addresses this gap by attempting to understand and postulate the relationship of OSG domains in practical principles. This study primarily focuses on the means and fundamental objectives proposed by Mishra (2015) to develop these principles. However, these objectives are similar to other objectives proposed in the literature.

Methodology and Analysis

2.1 Case Study

This study adopts an interpretive case study approach to understand the inter-relationships among multiple OSG objectives and how it works together in a natural organizational setting. A case-based approach is preferable when the descriptive intent is supported by meanings people assign to constructs under study (Orlikowski, 1991). In a natural environment, events unfold, and focusing on contemporary issues, a realistic picture of the relevance of the constructs under study emerges.

2.2. Organizational Context

The case study site was the information technology (IT) department of a major City Council (hereafter referred to as Omega) in southeast of the United States of America. Omega provided a good fit for this study as the organization was developing new OSG objectives. Omega is a state agency responsible for the administration of the information technology needs of the city. The organization strives to work with customers to align business and technology goals. The agency identified developing OSG objectives and managing proactive security measures as a strategic area of improvement. The parent agency uses an innovative technology planning process driven by the state's business needs and aligned with the city's business initiatives. The organization's CIO has a proactive approach to aligning the state's business and IT needs. The leadership wants to create a standard framework and processes using an enterprise-wide view to deliver IT services for each agency. An enterprise approach by the agency reduces maintenance costs and helps manage enterprise-level risks. Building standard services leverages the resources and establishes effective partnerships between Omega and other agencies. The CIO is the head of the agency, with five managers who directly report to him. The applications development manager is responsible for all the in-house development work. End-user services manager is in charge of operations and support facilities. The infrastructure services manager is responsible for enterprise systems and database administrators. The manager in charge of administration is responsible for training and administrative support functionalities. The newly added project management manager looks after the software development projects in the organization. Omega is responsible for keeping the data and services secure within the agency. As a state agency, Omega must keep the procedures getting audited so that public scrutiny is plausible. The organization, owning IT services, acts as a service provider to all the other agencies supported by the state.

2.3 Data Collection & Analysis

The primary source of data was the semi-structured interviews. Secondary sources include internal documents such as policies, the audit manual at Omega, and previous audit reports. The key stakeholders were identified for interviews and provided good insight into the organization's internal control structure in the context of OSG. Thirteen interviews were conducted with representation from IT, security, and audit personnel across the organization. The researcher established a point of contact at the organization and conducted all the interviews face-to-face. These interviews were recorded for transcription purposes. The additional documents reviewed for this study included the security policies of the organization and the last comprehensive audit report.

Huberman and Miles (1994) suggest three ways of data analysis for qualitative interview data: data reduction, data display, and conclusion drawing. In the data reduction process, the researchers identify portions of the data relevant to the theoretical construct under study. With the valuable data, the researcher categorized and structured the data so meaningful interpretations could be drawn. Finally, conclusion drawing is the interpretive process through which the researcher compares themes and patterns and then compares and contrasts to triangulate the data (Huberman & Miles, 1994). Based on the data triangulation, inter-relationships with means objectives were identified, and paths to fundamental objectives were proposed through OSG principles.

Results and Discussions

There are eight proposed principles of OSG in this study. For each principle, a table is provided with evidence from the case supporting each means objective, and prescriptive strategies are listed for organizations to implement these objectives. The data from the case allows for a deeper understanding of the principles proposed.

Principle 1

The data suggests that means objectives visible executive leadership, management commitment, and allocation of resources work together to accomplish the fundamental objective of defining a corporate controls strategy. The strategy for OSG establishes the business context in which information security will be managed and prioritizes the resource allocation for the objectives. OSG challenges could be in the form of new unwanted costs for the protection of assets, the diversion of resources for control purposes creating new vulnerabilities, or due to the temporary nature of solutions. A control strategy helps plan and coordinate in advance to meet these challenges. Research literature in security governance suggests that strategy, leadership, and management commitment are all required to deploy resources for overall security effectiveness.

The successful deployment of any IT plan requires management commitment, a structured decision-making process, and a strategy based on an understanding of the vision and architecture of the organization (Shupe & Bheling, 2006). Effective control strategies require efficient risk management processes, and management needs to be committed to implementing an effective risk assessment procedure where vulnerabilities and threats are identified. Any strategy would fail without the consistent support of the management (Wright, 2007). Security controls planning, and resource allocation needs strategic attention. The problem with the existing security guidelines, prescriptions, and best practices is that all of these take an operational view of risks (Msihra, 2019). The strategic management of security controls focuses on the competing demands for enterprise resources and their opportunity costs and seeks to identify security benefits that justify related costs (Anderson & Choobineh, 2008). At the strategic level of an organization, the benefits of information security (considerable reduction in damages and losses) must be balanced against security costs (Sklovos & Souros, 2006). Leadership and management commitment are crucial in achieving the control strategy (table 1). Also, resource allocation for security governance is a part of the strategy and cannot be optimized without the management's total commitment to the governance program. Based on the understanding of the interplay of the above means objectives, the first proposed principle of OSG:

P1: Security governance activities shall be planned, coordinated, and executed by developing a strategy for controls by the leadership to encourage management commitment to allocating resources

Table 1: Principle 1

Fundamental OSG Objective-Ensure Corporate Controls Strategy		
Means Objectives	**Interview data**	**Key recommendations**
Ensure Visible Executive Leadership	"There has to be strong leadership, reinforcement of a tie between what's being done and its value and risks. Also, practice what you preach. It helps to have IT personnel in visible positions with good commitment being shown from top executives."	Encourage the management to "walk the talk." Encourage top management to lead by example Ensure that key individuals enforce rules and remedial solutions
Maximize Management Commitment	"I would recommend going to the top and finding out what the management really wants and then working with those supervisors to find out what it takes to serve that operation daily. Make things available. You have to have the top on board with the work. Find out what you can do with these resources."	Provide rewards for conformity with policies Discourage imposing ad hoc new rules Establish positive reinforcement for doing the right thing Ensure the availability of the management
Maximize Resource Allocation for controls	"Security is a non–functional requirement. There is no place for non-functional requirements in system design. User groups do not talk about security, as this a so-called non-functional technical requirement. How do you manage it then? It becomes an issue of internal policies."	Ensure adequate resources allocation for the maintenance of controls Discourage individuals from feeling restrained due to resources

The management has to be committed to security governance initiatives, for the controls require resources in the form of finance, people, and technology, which are imperative to develop a dynamic control structure. It is the management's responsibility to articulate security risks so that resources are not compromised (Wright, 2007). Managers influence the top management about priorities for security governance, including the induction of adequate skilled and knowledgeable personnel or security specialists.

Principles 2 and 3

The data in this study and research literature support the relationship among OSG objectives audit efficacy, business process clarity, and punitive structure to meet regulatory compliance preparedness. In preparing for regulatory compliance, in-depth knowledge of business processes is required. Breauxa et al. (2008) argue that leading regulations describe specific requirements for various IT-related business processes, which require comprehensive documentation to demonstrate how personnel decisions implement standards and regulations. Transparent business processes help the auditing function search for anomalies in the systems. Frequent audits can help an organization maintain clarity in processes and the fear of non-compliance. The regular audit helps in increasing the probability of being caught in case of deviant behavior. Management needs to evaluate compliance with the regulations to estimate the effectiveness and possible shortcomings (Myler & Broadbent, 2006). Auditing can help determine improvement areas (Myler & Broadbent, 2006). An audit process is a powerful tool to contrast the policies versus practices of an organization. Based on the discourse above, the second principle of information security governance is proposed:

P2: Business process clarity should be encouraged through efficient audit processes and punitive structures to achieve compliance

Auditing deters the creation of process anomalies in organizations, and employees tend to behave if an audit is possible. The audit process's efficacy improves clarity in an organization's business processes. It is crucial to understand the workflow in an organization to integrate controls into the business processes in a manner integral to the system's functionality (table 2).

Table 2: Principle 2

Fundamental Objective: Maximize Regulatory Compliance		
Means Objectives	**Support from Omega**	**Key recommendations**
Maximize Clarity in Business Processes	"The application should not be a black box; we should understand the business processes. What is it that it is doing? How does it convert the input into output? Whether the whole processing it is doing is correct or not should be clear."	Establish clarity in end-to-end business processes Understand the business processes flow Increase awareness of business activities and processes
Ensure the Efficacy of Audit Processes	"We do not create controls; we only test them. We consult about them, and we tell them [auditee] here is the type of control you will need to have, and you will have to create it because that's your job. If you need help in creating those controls, we can provide some guidelines and come back and see how well you have done it."	Develop audit practices for changing contexts of governance task Develop an audit process to integrate the information rules Develop cross-checking mechanisms for the audit function
Ensure Punitive Structures	"You have to make the consequences of the action very clear. Most of the times, companies do not make it clear. They warn them, saying, "if you do that, criminal action will be taken." But what is criminal action? People are held responsible for breaches, but it is not clear that if breaches happen, what action would be taken?"	Ensure disciplinary action against non-compliant behavior Ensure protection against disgruntled employees Establish clear consequences for not complying with laws

Auditors examine business processes to study the workflow and suggest ways to enhance the integrity of the process. Management ensures that there are established acceptance criteria for the performance of systems, which helps the auditors to check the actual performance of the systems versus the expectations from the system. Assessing the system's actual versus expected performance helps test the accuracy of the data provided to the organization's customers. Verifying anomalies in the business process requires external intervention in the form of auditing. Another path to achieving the fundamental objective of regulatory compliance is proposed in principle 3. OSG objectives such as standardization of controls, clarity in controls, and enhancing trust mechanisms interplay to help achieve regulatory compliance in an organization. OSG requires an end-to-end view of the operations in an organization which can be achieved through clarity in the business process. The vulnerabilities in business processes can lead to systems compromise, intentionally or otherwise. In such cases, preventive security mechanisms and active deterrence measures protect the organization. D'Arcy et al. (2009) argue that combined proactive and preventive security approaches deter users from IS misuse. Auditing helps achieve good security governance, providing traceability of user action and a chain of evidence that can be reconstructed to understand when and how the system broke down (Swanson & Guttman, 1996). One of the most critical usages of audits is to help the organization meet regulatory compliance (Goel et al., 2006). Security countermeasures include deterrent administrative procedures (such as frequent audits) and preventive security software, leading to lower computer abuse (Straub & Welke, 1998). The study suggests that regulatory compliance requires standardization of controls so that the organization's stakeholders can trust the management with critical information. Clarity of control development is essential for standardizing controls and establishing trust within and outside the organization. Regulations are intended to protect the interest of external stakeholders, such as investors and business partners. Standardization of the controls is one of the best strategies to proactively establish respect for the organization's security program (May 2005). Loss of trust and confidence, which results from an organization's inability to meet users' expectations and protect their identity and privacy, would compromise business objectives (Abu-Musa, 2010). The third principle of OSG:

P3: Standardization and clarity in controls should be developed to enhance trust within and outside the organizations and to achieve regulatory compliance

Regulatory compliance helps organizations do things in a manner that is consistent, transparent, and open for review. The clarity in the controls development process assures a normal behavior pattern, which enhances intra-organizational trust for security measures (Mishra & Dhillon, 2006). Trust indicates a series of direct relationships with people and not with a set of organizational entities or policies (Fleming, 2007). If there is a lack of trust in the organization, regulatory compliance would be compromised and not entirely in the spirit of the legislation (table 3).

Table 3: Principle 3

Fundamental Objective: Maximize Regulatory Compliance		
Means Objectives	**Support from Omega**	**Key recommendations**
Encourage Standardization of Controls	"Somebody needs to do this; make sure that those objectives are being met by the systems. Those things [governance frameworks] have come into existence by looking at the experiences of several people who have suffered breaches. So, it's kind of learning from someone else's experience. It is critical to look at the frameworks."	Benchmark security governance investments against industry standards Benchmark security governance practices with industry standards Compare the state of controls with standards across the industry Create systemization in the control development process
Ensure Clarity in Control Development Process	"Creating the policy and the procedure needs to be clear because if nobody knows about the controls and procedures or understands it, they are not going to follow it."	Develop controls as a part of the change initiative Develop controls for all the levels in the organization Develop simple and easy-to-use controls Discourage complex controls Ensure that control usage is simple.
Maximize trust-building mechanisms	"They [employees] must learn to trust. When you say, you are doing something, [make sure] you are doing it. When you say you will get back to them, you get back to them. You got to have that consistency."	Encourage trust-building mechanisms for controls Enhance an environment of trust in the organization

Standardization of controls helps in trust building both within and outside the organization. The management should encourage standard protocols for control development as it makes finding deviations in the systems more accessible and helps cover any vulnerabilities. Standardized controls help in ensuring that expectations on the stakeholders' part are being met. In case of non-compliance with agreed procedures, the structure of the standardized control also communicates the need to be compliant and the consequences of non-compliance. The primary purpose of having standards is to ensure sufficient trust with stakeholders.

Principles 4 and 5

The results of this study suggest an ongoing dependency on frequent communications, regular monitoring and feedback, and training and education to accomplish the fundamental objective of continuous control improvement. Business needs are dynamic and change with time, and the changes need to reflect in controls designed to protect this information and processes. The monitoring and review of reviewing post-implementation is a critical phase for the success of the overall controls program (Slonka et al., 2023). End users should be able to understand the changes in controls to use the systems correctly. Policies and procedures can be transparent through developing open communication policies where discourse about controls is encouraged. The employees should be willing to comply with the use of the controls. A monitoring technique can be effective only if the employees understand and are eager to use the controls and provide feedback (Booker & Kitchesn, 2006). Straub and Welke (1998) suggest feedback loops develop better communication channels through departmental meetings and informal chatting. The understanding of the dynamics of the above means objectives leads to our fourth principle of OSG: ***P4: Frequent communication should be encouraged through regular monitoring and extensive training for the iterative development of controls***

Monitoring and feedback channels in the organization add to the effectiveness of communications about controls (table 4). Management needs to revisit the controls based on feedback from the employees continually. The input needs to be communicated in a way that it is incorporated in the next iteration.

Table 4: Principle 4

Fundamental objective: Ensure Continuous Improvements in controls		
Means Objectives	**Support from Omega**	**Key recommendations**
Ensure Communication about Controls	"Communication, discussion, and debate on controls topics are encouraged. Such exchanges are conducted in visible, open, participative forums, both formal and informal, as appropriate. The security actions and their contribution to mitigating enterprise risk are well known throughout the organization."	Communicate the importance/purpose of controls; Communicate the nature and scope of controls Communicate the consequences of internal controls breaches Encourage communication amongst employees about control issues
Maximize Monitoring and Feedback Channels	"The system in which I am right now, I am in a place where I am able to find out what they have done whatever needs to be done, seeing the audit trail. If they haven't done their work, we find that pretty quickly."	Ensure an adequate review of the governance program [Ensure continuous monitoring of controls; Institute corrective measures for continuous monitoring; Encourage informal feedback from people about controls
Maximize Training and Education	"You can put control, such as discussing the policies. But in my opinion, controls are not going to do anything unless you educate your end user. Understand that controls don't do anything for you unless you educate end users."	Define training programs to reflect details of internal controls, Discuss the relevance of controls adequately; Encourage education about internal controls; Illustrate with specific work-related examples; Ensure learning about internal control issues

Training and education improve communications about controls. Training, specifically about controls, emphasizes using knowledge about the relevance of controls in daily practice. The end users should be adequately trained and educated about the usage of controls. The knowledge thus imparted leads to more enquires and frequent communications about the controls.

The means objective of clarity in control development, resource allocation, and formal control assessment functionality have interrelationships to help achieve the fundamental objective of continuous control improvement, as reflected in the following principle. Effective communication channels about controls facilitate and open discussions and debates on important issues about controls. Resources are required to institute changes in the governance structure. Accepting the changed and improved controls would be enhanced when the control development process is open and transparent. The clarity in the controls development process facilitates quicker adoption of the changes introduced in the governance program. The centralized functionality ensures a cost-benefit estimate of the controls for long-term benefits. The interaction of these means objectives leads to our fifth principle of OSG:

P5: Controls development shall be clear, transparent, and easily understandable to the organizational members' and adequate resources must be allocated to institute formal controls assessment functionality.

The strategic management of security focuses on the competing demands for enterprise resources and their opportunity costs and seeks to identify security benefits that justify related costs (Anderson & Choobineh, 2008). Resource allocation for controls is required for developing formal controls assessment functionality in an organization. Resources for controls are always an issue as controls assessment is not a separate functionality, and no department owns up to this cost. Adequate controls always require the right resources to protect business integrity. Developing control assessment functionality is instead a new concept introduced by this research and currently does not have much support from the research literature (table 5).

Table 5: Principle 5

Fundamental objective: Ensure Continuous Improvements in controls		
Means Objectives	**Support from Omega**	**Key recommendations**
Ensure Clarity in Control Development Process	"You got to put it [controls] in a way that it's not complex, it's not complicated. So you put together a checklist and put together a general list [controls]. More general the list, larger the deviation from what you want. You have to be specific, but you don't want so detailed [controls]. You have to define how far you want to go. So if you want City's webpage to be the homepage, you got to define in that checklist and make sure that it's [making City's webpage as homepage] one of the things you do."	Ensure risk assessment to develop controls Structure the information needs. Ensure that controls are easy to use Ensure timeliness in controls.
Maximize Resource Allocation for controls	"The other issue which we have had is the physical security of assets by temporary workers. The cleaning people are not the city's employees; they are from a company. They are brought in as temporary workers and are managed by a city employee. They come in, and they got a giant trash can with them. We have lots of equipment lying around, it's not a lot of money, but it is some money. They can take away anything they want. How can I control that? They got to get in and clean the trash. If someone puts all the papers in the trash can and take it away, I won't know."	Provide resources for compliance. Encourage coordination between IT and business for controls Establish controls proactively

Ensure Formal Control Assessment Functionality	"I would say sign off on the requirements that the key stakeholders have agreed upon. Develop the feasibility metrics so that you can take each requirement and trace it throughout the whole system from the requirement to functional design. This process has to be done formally."	Institute controls as part of organizational design Discourage planning about control implementation as an "afterthought." Increase understanding of stakeholder viewpoints

The clarity in control development also helps the cause to create formal control assessment functionality. Data suggests that if there is clarity in how controls are being defined, it would be easier to have a formal controls assessment entity that could validate the requirement of the controls and provide adequate support for it. Lack of clarity in controls can lead to vulnerabilities of endangering systems. Formal controls assessment functionality looks into the possible vulnerabilities and seeks solutions to the threats.

Principle 6

The study suggests that the fundamental objective of establishing controls conscious culture is facilitated by OSG objectives such as reliable communications, cohesive groups, and alignment of individual and organizational control values. Control-conscious culture is achieved when the tacit knowledge about security controls guides the employees' day-to-day activities. Control-conscious culture entails that controls have to become part of the corporate culture (Thomson & von Solms, 2008). Control culture requires that the employees internalize controls and have been accepted at an informal level. Consciousness about controls can be achieved if the individuals can align their values about controls with those of the organization. The control culture is crucial for security governance as it can act as a robust, underlying set of forces that establishes individual and group behavior within an organization (Schein, 1999). Encouraging group cohesiveness helps in propagating the right values for security controls. The sixth principle of OSG is:

P6: Controls consciousness shall be developed through regular communications and forming cohesive groups, which lead to the alignment of individual and organizational values.

Inappropriate beliefs and attitudes of the employees, if addressed by the management, lead to changed actions and behaviors of the employees and synchronizes with the overall corporate security culture in the organization (Thomson & von Solms, 2008). Communication channels should be established, and debating the controls in the open should be encouraged. Normative controls will always be required to hold together the security governance initiatives, and these controls comprise values, belief systems, and culture for the individuals (Mishra, 2015). Establishing a control culture requires enhancing group cohesiveness in the security teams (table 6). Group cohesiveness allows a coherent interaction channel with the management. A team approach to information security is necessary if an adequate level of information security is achieved (Mishra, 2015).

Table 6: Principle 6

Fundamental Objective: Encourage a control-conscious culture		
Means Objectives	**Support from Omega**	**Key recommendations**
Ensure Communication about Controls	"They [employees] like to know the reason, why? They like to hear things. People may not communicate to us, but people like to be communicated to, it may not go both ways all the time, but in my experience, I found that people like to be told."	Explain the rationale behind controls Explain the risks and values of controls to users Ensure damage assessment to the organization from lack of controls

Maximize Group Cohesiveness	"[We need to know] which roles have the greatest vulnerability to assign groups. A great example of that is, if you put multiple people together, collusion is a lot harder compared to one person doing something wrong. So it's a similar type of thing; people in groups are afraid that others might know what they are doing. Groups have an impact on their behavior."	Encourage sharing the credit for good work Encourage the ability to share work Understand the group behavior driven by peer pressure Discourage favoritism in groups Understand the influence of peer pressure on individual behavior
Ensure Alignment of Individual and Organizational Values	"So we can make a rule, we can make a law that you have, to be honest. I mean, in reality, our personal values, our own values should define that we are going to do the best we can, do the right thing at any point of time. If my values allow, then only I will follow the rules. My personal belief is that you can't legislate that; you can't provide enough legislation to do that."	Align personal and organizational values. Align security control objectives with enterprise objectives Understand people's attitudes and beliefs about controls Cultivate ethical values about security governance

Establishing open communication policies about controls helps in individual and organizational alignment of values and maximizes group cohesiveness. Communication about the policies, procedures, controls, and strategies is critical to ensure alignment of end-user values and organizational values.

Communicating about controls develops clarity about their intent and scope. At Omega, the controls were made appealing to the end users by communicating something that makes their work and life more comfortable; it is about them, not the bosses. Communications also influence group cohesiveness in functional groups. At Omega, intergroup communications about controls and security-related responsibilities make the groups more cohesive, and the managers strive to protect their group members against all odds. Cohesive groups influence the behavior of the individuals in the group, and there are chances that individuals will better align their values with those of the organization in the realm of security governance if the groups' values are aligned.

Principle 7

Data analysis suggests that the fundamental objective, clarity in policies and procedures, can be achieved through data criticality, frequent audits, and a transparent control development process. Information security policy is the basis for disseminating and enforcing sound security practices within the organizational context (Baskerville & Siponen, 2002). The strategic information systems plan is a critical prerequisite for policy formulation. Security policies are the foundations of information security management. Establishing data criticality requires clarity in policies and procedures. Effective audit processes and clarity in control development help in achieving data criticality. An audit process is a reliable tool to contrast the policies versus practices of an organization. The seventh principle of OSG is:

***P7: Data criticality shall be established by ensuring frequent audits and a transparent controls development process to enhance clarity in policies and procedures*.**

An audit provides traceability of user action and a chain of evidence that can be reconstructed to understand when and how the system broke down. Complicated controls that increase constraints on people should be minimized (Parker, 1996). The clarity in the controls development process and incorporation of controls in systems development would lead to better technical controls and thus enhance data criticality. Separating duties among developers, testers, and administrators in operational facilities reduces the risks of unauthorized actions (Myler & Broadbent, 2006). This separation is ensured by audit functionality, which gives users confidence in the integrity of data. The result is trust in the IT infrastructure, which is valuable in today's business world (table 7).

Table 7: Principle 7

F3: Establish Clarity in Policies and Procedures		
Means Objectives	**Support from Omega**	**Key recommendations**
Ensure Data Criticality	"Security controls are revolving around data, the ability to keep the integrity of the data. It [controls] revolves around internal and external access to the data. In processing all sorts of access where you want to make sure that all the access is limited to the data somehow there is a need to for segregation of the production data, and that is accomplished in many ways."	Establish a control structure to reflect sensitivity in data Define responsibilities according to the level of confidentiality of information Identify data owners for sensitive data Link data owners with authorizations Ensure ownership of information
Ensure the Efficacy of Audit Processes	"I think auditing provides very important quality assurance. If you don't have an audit, you have no compliance. Right now, you have to audit because all the process is not automated; you can't expect control at every single process. I think 60% of all processes here don't have any electronic support or computers at all. People do the work, so we have an audit."	Ensure adequate access to auditors across the organization Establish the difference between audit functionality and actions Treat internal auditors as consultants to ensure the effectiveness of controls
Ensure Clarity in Control Development Process	"Creating the policy and the procedure needs to be clear because if nobody knows about the controls and procedures or understands it, they are not going to follow it."	Define multiple layers of controls Develop achievable goals Develop simple and easy-to-use controls Discourage complex controls Ensure that control usage is simple.

Audit efficacy leads to ensuring data criticality. It is essential that these controls and access are revalidated continuously and checked from an independent perspective. The constant revalidation is where the critical role of auditors comes into play (Mishra et al., 2022). Segregation of duties, right access, and adequate authorization mechanisms are required for data criticality. Auditors ensure that these mechanisms are sound and work for the organization. The efficacy of audit practices depends on how well the auditors can protect the data in the system. Auditing ensures that access to information is also changed during changes in roles.

The clarity in the controls development process also helps establish data criticality in an organization. It is essential to develop precise controls for access, authorization, classification, and segregation of duties in data usage to maintain the data's confidentiality, integrity, and availability. Also, change management controls are crucial in ensuring criticality, which can be a potential source of threat to an organization. At Omega, the management ensures that people follow the controls, or they will be consequences. Following the procedures requires everyone to be clear about the controls and the business process, which helps establish data criticality.

Principle P8

This study and research literature suggests that responsibility and accountability structures are established in an organization with the help of leadership guidance, ethical and moral tone, punitive structure, and trust-building measures. Responsibility and accountability in structures require visible leadership that motivates people to be responsible in their jobs and take the blame for their actions. Leadership can set an excellent ethical and moral environment, wallowing the members to trust the management's intentions. Increased awareness and individual accountability can significantly affect how security practices are implemented in an organization (Mellor & Noyes, 2006). The above discussion leads to our eighth OSG principle:

P8: Trust-building measures shall be appropriated through executive leadership and punitive structures to establish the right ethical tone for the organization to assign responsibility and accountability to its structures.

Corporate boards that undertake the challenge of IT oversight show that they understand the scope of their corporate accountability and responsibility and are proactive in their leadership duties (Myler & Broadbent, 2006). To establish trust and ethical conduct, leadership should be able to "walk the talk" and espouse critical controls and then follow these personally. The executive must set exemplary ethical and moral conduct for the employees to follow (Thompson & von Solms, 2008). Senior managers can communicate policies and codes of ethics to guide employees, and it is the responsibility of management to serve as a role model for the behavior it wishes to promote (Krull, 1996).

The security technology design often neglects the moral or ethical element of the governance process, which is one of the most critical aspects of security management (Gupta & Sharman, 2008). Instilling value-based work ethics would help ensure an ethical environment leading to employees abstaining from unacceptable behavior and a secure organization (Table 10). Mutual trust between employees and management is vital to ensure that the employees internalize responsibilities. A lack of trust in policies and procedures can make the employees alter systems and not comply with controls such as not sharing passwords or taking confidential data out of the office on laptops (Booker & Kitchens, 2008). The punitive structure also helps accept ethical codes in the organization. In other words, first, clarify what behavior is acceptable by clearly establishing the ethics and morality valued in the organization. Ensuring ethical and moral values helps establish an organization's punitive structures. The ethical environment in the organization creates normative pressure on the people to do the right thing and not break the law. Personal values and morality shapes an individual's tendency to conform to the laws and rules (table 8).

Table 8: Principle 8

F6 Enable Responsibility and Accountability in Roles		
Means Objectives	**Support from Omega**	**Key recommendations**
Maximize trust-building mechanisms	"They [employees] must learn to trust. When you say, you are doing something, [make sure] you are doing it. When you say you will get back to them, you get back to them. You got to have that consistency."	Discourage an environment of fear Discourage politics in the organization Encourage free expression
Ensure Visible Executive Leadership	"With the city, it's not hard to get the support of the CIO. He is supportive of our actions. The hard part is getting to his colleagues, the other directors, who need to approve it but have no clue about it."	Nurture relationships with employees Place committed IT personnel to be in visible positions Encourage control conscious attitude of supervisors

Ensure Punitive Structures	"I also think what you have to do is to have a clear punitive structure because big things are at stake. A punitive structure is a must. So you must have something that says even if the employee violates this, what is going to happen to him."	Encourage discipline in the organization Explain the meaning of criminal activity to the employees Create a fear of punishment in organizations Create countermeasures to deal with destructive actions
Ensure ethical and moral values.	"so we can make a rule, we can make a law that you have, to be honest. I mean, in reality, our personal values, our own values should define that we are going to do the best we can, do the right thing at any point of time. If my values allow, then only I will follow the rules. My personal belief is that you can't legislate that, you can't provide enough legislation to do that."	Encourage acceptable and respectable actions. Encourage access to individuals with strong moral values Encourage self-pride in the job Understand the morality of the staff

Visible executive leadership helps propagate ethical and moral values in organizations through "lead by example." Leadership also leads to trust-building mechanisms in an organization. Leaders have to win the confidence and trust of the stakeholders to implement the security program successfully. This study suggests that establishing punitive structures helps in trust-building mechanisms in an organization. Clear punitive structures in an organization establish the fear of consequences of non-compliance with the rules. This environment leads to more trusting relationships between employees and management. The employees need to know what is acceptable clearly and that it is their responsibility to ensure things do not deviate from normal behavior. It provides a fallback plan for the employees where they know they can trust the management to be fair and just in cases of breaches that are not their fault.

This study contributes in multiple ways. Theoretically, it presents OSG objectives and its inter-relationships for better security governance. OSG objectives and their interrelationships are a considerable contribution to security literature, and several studies in this area could be initiated. For practitioners, these principles provide prescriptive solutions to strengthening OSG practices. These principles of OSG provide unique insights into OSG activities and areas of improvement. These prescriptive principles are unique and provide paths to enhancing OSG practices and preparedness.

Conclusion

The case study presented in this paper examines the inter-relationships of seventeen means and six fundamental objectives and how these objectives allow organizations to accomplish strategic security planning. The emergent principles of OSG from the objectives (Mishra, 2015) were identified, and its implications for research and practice were discussed. These principles are prescriptions for strategic and comprehensive security preparedness for an organization.

References

Abu-Musa, A (2010). "Information security governance in Saudi organizations: an empirical study," Information Management & Computer Security, Vol. 18 Issue: 4, pp.226–276, https://doi.org/10.1108/09685221011079180

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

Anderson, E., and Choobineh, J. (2008). “Enterprise Information Security strategies,” *Computers and Security*, 27(1), 2008, p. 22-29

Anthony, R., Dearden, J., & Bedford, N. (1989). Management Control Systems, Homewood, Irwin, 1989.

Baskerville, R., and Siponen, M. (2002). "An information security meta-policy for emergent organizations," Logistics Information Management Science (15:5) 2002, pp 337-346.

Booker, Q., & Kitchens, F. (2008). "Examining security intentions of multiple security measures " 7th Annual Security Conference The Information Institute, USA, Las Vegas, 2008.

Breaux, T.D., Ant on, A.I.: Analyzing regulatory rules for privacy and security requirements. IEEE Transactions on Software Engineering 34(1) (2008) 5–20

D’Arcy, J. Hovav, A. and Galletta, D. (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach, Information Systems Research, Vol. 20, No. 1, March 2009, pp. 79–98

Fleming, S., (2007). "Implicit Trust Can Lead to Data Loss," Information Systems Security (16) 2007, pp 109–113.

Fuller, C., Biros, D., & Imperial, M. (2007). "Knowledge retention in information assurance computer-based training: a comparative study of two courses for network user " 6th Annual Security Conference, The Information Institute, USA, Las Vegas, 2007.

Goel, S., Pon, D., and Manzies, J. (2006). "Managing information security: Demystifying the audit process for security officers," Journal of Information System Security, 2006, pp 25-45.

Gordan, L., and Loeb, M. (2002). “The economics of information security investment,” ACM Transactions on Information and System Security (TISSEC), Volume 5 Issue 4, November 2002, Pages 438-457

Gupta, M., & Sharman, R. (2008). "Evaluating organizational social engineering threats: A metrics development framework," 7th Annual Security Conference The Information Institute, USA, Las Vegas 2008.

Huberman, A., and Miles, M. (1994). Data Management and Analysis Methods, in Handbook of Qualitative Research, N. Denzin, and Y. Lincoln (eds.), Sage, Thousand Oaks, CA, 1994, pp. 429-444.

ISACA. (2012). "CISA Review Manual," Information Systems Audit and Control Association, Rolling Meadows, IL, 2012

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).

Krull, A., (1996). "Whistleblowers and Informants, Part 2" Computer Fraud & Security, October 1996.

May C., (2003). "Dynamic corporate culture lies at the heart of effective security strategy," Computer Fraud & Security, Vol. 5, 2003, pp 10–13.

Mellor, M., and Noyes, D. "Awareness and accountability in information security training " 6th Annual Security conference The Information Institute, USA Las Vegas, 2007.

Mishra, S. (2015). "Organizational objectives for information security governance: a value-focused assessment," Information & Computer Security, Vol. 23 Issue: 2, pp.122–144, https://doi.org/10.1108/ICS-02-2014-0016

Mishra, S. and Dhillon G (2006). “Information Systems Security Governance Research: A Behavioral Perspective,” 9th Annual NYS Cyber Security Conference and Annual Symposium on Information Assurance, June 14-15 Albany, NY

Mishra, S. (2019). A Case-Based Analysis of Organizational Security Governance Dimensions: User Involvement, Process Integrity, and Resources Allocation, Issues in Information Systems, Volume 20, October 2019, pp. 128-138

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, Volume 13, Issue 2, July 2020

Mishra, S., Draus, P., Slonka, K. and Bromall, N. (2022). OSG practices in responsibility/accountability, awareness, compliance, and assessment: A qualitative analysis, Issues in Information Systems, 23(3), pp. 265-278

Myler, E., & Broadbent, G. (2006). "ISO 17799: Standard for security ", The Information Management Journal, November/December 2006, pp 43–52.

Savola, R. M., (2007). Towards a Taxonomy for Information Security Metrics, International Conference on Software Engineering Advances (ICSEA 2007), Cap Esterel, France

Schein, E.H. (1992). Organizational Culture and Leadership, Jossey-Bass, San Francisco, CA, 1992

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.

Shedden, P., Ruighaver, T., & Ahmed, A. (2006). "Risk management standards: The perception of ease of use," 5th Annual Security Conference, The Information Institute, USA, Las Vegas, 2006.

Shupe, C. & Behling, R. (2006). "Developing and Implementing a Strategy for Technology Deployment," Information Management Journal, vol. 40, no. 4, pp.52.

Sklovos N, Souros P. (2006). “Economic models and approaches in information security for computer networks,” International Journal of Network Security 2006;2(1):243–56.

Slonka, K., Mishra, S., Draus, P., & Bromall, N. (2023). Measurement, reporting, and monitoring in organizational security governance from the security professional’s perspective, CYBERSECURITY PEDAGOGY & PRACTICE JOURNAL. 2(1).

Solms, v., (2005). "Information Security Governance: COBIT or ISO 17799 or both? " Computers & Security (24) 2005, pp 99–104.

Straub, D., and Welke, R. (1998). "Coping With Systems Risks: Security Planning Models for Management Decision Making," MIS Quarterly (22:4) 1998, pp 441-469.

Swanson, M., & Guttman, B. (1996). “Generally Accepted Principles for Securing Information Technology Systems,” National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, 1996

Thomson, K., and Von Solms, R. "Information security obedience: a definition," Computers & Security. (24:69-75) 2005.

Orlikowski, W. (1991). Integrated Information Environment or Matrix of Control? The Contradictory Implications of Information Technology, Accounting, Management and Information Technologies (1:1) 1991, pp 9-42.

Westby, J. and Allen, J. (2007). Governing for Enterprise Security (GES) Implementation Guide, Technical Note, Cert Program, retrieved on 05/31/23 https://resources.sei.cmu.edu/asset_files/TechnicalNote/2007_004_001_14837.pdf

Wright, M.A. "Keeping top management focused on security " Computer Fraud & Security (5:1) 2001, pp 12–14.