JOURNAL OF INFORMATION SYSTEMS APPLIED RESEARCH

Volume 14, Issue. 3
September 2021
ISSN: 1946-1836

In this issue:

iscap
Information Systems & Computing Academic Professionals

The **Journal of Information Systems Applied Research** (JISAR) is a double-blind peer reviewed academic journal published by ISCAP, Information Systems and Computing Academic Professionals. Publishing frequency is three to four issues a year. The first date of publication was December 1, 2008.

JISAR is published online (https://jisar.org) in connection with CONISAR, the Conference on Information Systems Applied Research, which is also double-blind peer reviewed. Our sister publication, the Proceedings of CONISAR, features all papers, panels, workshops, and presentations from the conference. (https://conisar.org)

The journal acceptance review process involves a minimum of three double-blind peer reviews, where both the reviewer is not aware of the identities of the authors and the authors are not aware of the identities of the reviewers. The initial reviews happen before the conference. At that point papers are divided into award papers (top 15%), other journal papers (top 30%), unsettled papers, and non-journal papers. The unsettled papers are subjected to a second round of blind peer review to establish whether they will be accepted to the journal or not. Those papers that are deemed of sufficient quality are accepted for publication in the JISAR journal. Currently the target acceptance rate for the journal is about 40%.

Questions should be addressed to the editor at editor@jisar.org or the publisher at publisher@jisar.org. Special thanks to members of ISCAP/EDSIG who perform the editorial and review processes for JISAR.

JOURNAL OF INFORMATION SYSTEMS APPLIED RESEARCH

Interpreting Organizational Security Governance Objectives for Strategic Security Planning

Sushma Mishra
mishra@rmu.edu
Computer Information Systems Department
Robert Morris University
Moon Township, PA 15108, USA

Abstract

The goal of this research is to conduct a case study examining the contextual use and purpose of organization security governance (OSG) objectives in strategic planning and preparedness for security initiatives. This study also explores for underlying dimensions of OSG practices. Mishra (2015) proposed 17 means OSG objectives that are theoretically driven and empirically grounded. An in-depth case study is conducted to examine and interpret the meanings of the above objectives in a real organizational setting and identify the dimension of OSG practices. There were 13 interviews conducted at various levels in the organization, and other secondary sources of data, such as policies, mission documents, and audit documents were reviewed. The findings suggest all 17 means objectives are useful in preparing the organization strategically for better security practices. The results also suggest four underlying dimensions of OSG into play in overall improving security practices. These dimensions are Structural, User, Facilitation, and Processual. This study empirically validates all means objectives for OSG from prior research. The OSG dimensions identified to provide a useful basis for strategic planning of comprehensive security. The practical implications lie in providing real organizational security governance dimensions that allow practitioners to use these as a tool to assess and implement security governance practices at all levels. The originality of the paper lies in its unique contribution to security governance literature in terms of empirically examining OSG objectives for strategic security planning purposes. It also proposes OSG dimensions that allow for in-depth preparedness for security initiatives at multiple levels.

Keywords: organizational security governance**,** case study, Facilitation, structural, processual, user, strategic, controls, IT audit

1. INTRODUCTION

Organizational Security Governance (OSG) objectives are critical in providing overall strategic leadership to the security preparedness of an organization (Mishra, 2015). OSG is a set of responsibilities and practices used by management to provide vision and direction to an organization and, in the process managing risks appropriately while optimally using resources available (ISACA Manual, 2012). Having the right security strategy requires the right OSG objectives for guidance. There are situations where security strategies created are not reflective of the values and strengths of the organization. OSG objectives provide clarity on "what is it that needs to be managed (Brotby, 2009)" and allow for meaningful management metrics.

Mishra (2015) proposed six fundamental and seventeen means objectives for OSG. In this study, the value-focused approach was used to develop theoretically driven and empirically grounded objectives. The study defines fundamental objectives as an objective that is essential and important in its own right for the decision context, in this case, security governance. An objective that leads to another objective being considered in decision-making is

a means objective. The role of an objective (means or fundamental) is determined by its direct or indirect impact on the decision making context. The proposed objectives in Mishra (2015), however, have not been studied in an organizational setting to understand its implications on security preparedness.

This study examines the significance of the proposed seventeen means objectives in a real organization using a case study method. Fundamental objective, by definition, is established as critical for OSG practices; hence, the scope of this study is all the proposed means objectives. The main goal of this study is to assess and inform how the proposed means OSG objectives shape the strategic security planning and preparedness. This research also examines what are, if any, underlying dimensions of OSG objectives? The research question posed is: how do seventeen means (OSG) objectives influence security strategic planning and preparedness in an organization? The results suggest four underlying dimensions of OSG, namely, Structural, Processual, User, and Facilitation.

The section following the introduction presents the methodology section of the paper and describes the organizational context, data collection, and data analysis process. The subsequent section presents the results in the form of four underlying dimensions of OSG. Following the four dimensions of OSG, a discussion is generated that draws on research literature to explain the importance of the proposed dimensions. The implications and contributions are presented, and future research directions are suggested.

2. CASE STUDY

This study adopts an in-depth interpretive case study approach to understand the nature and significance of the developed governance objectives in an organizational context. Interpretive research does not predefine dependent and independent variables, but focuses on the complexity of human sense-making as the situation emerges (Kaplan and Maxwell 1994); it attempts to understand phenomena through the meanings that people assign to them (Orlikowski 1991). Case study help in getting a rich picture of the phenomenon under study without disturbing the natural state of entities.

Organizational Context

The case study site was the information technology (IT) department of a major City Council (hereafter referred to as CCIT) in the southeast of the United States of America. The (CCIT) is a state agency responsible for the administration of the City. The organizational goal is to work with customers to align business and technology objectives. A set of guiding values have been explicitly stated in the mission statement of the organization. Managing information security governance is identified as a strategic area of improvement by the agency. Security architecture at CCIT is focused on five areas: applications, authentication, networking & infrastructure, physical, and process. The management emphasizes that improving security controls will drive efficiency and effectiveness across the City.

CCIT helps its citizens to receive more from the state government in terms of the state of the art facilities enhanced by a strong information technology network. It also supports publicly accessible computers for free use by the citizens. The state uses an innovative technology planning process, which is driven by the business needs of the state and aligned with the City's business initiatives. The strategic plan of the organization is to establish a standard framework and processes that deliver IT services for each agency and sets an enterprise view. Such planning intends to develop more enterprise-level targets and evolves from an agency focused goals. The benefits of such an approach are manifold. An enterprise approach by the agency reduces the costs of maintenance and helps manage enterprise-level risks. Building standard services leverages the resources and establishes effective partnerships between CCIT and other agencies.

The organizational structure includes the CIO as the head of the agency. Five managers directly report to the CIO.

The technology planning process is integrated among agencies and requires investment of resources from all. The organization must keep its procedures auditable so that public scrutiny is plausible. The organization, having the ownership of IT services, acts as a service provider to all the other agencies supported by the state. To provide excellent infrastructure, the organization approaches every agency individually and assesses the agency's information needs and the current state of technology utilization. The organization targets improvements based on the specific needs of different agencies. These improvements are based on joint maps created with the IT organization and the agency.

Data Collection

Several sources of data were used for the case study. The primary source of data was the semi-structured interviews. Secondary sources include the policy and procedure manual, the audit manual at CCIT, the policy guidelines provided by the state agency, which is responsible for the security policies of the state agencies. Key stakeholders were identified at the case study site with the help of our point of contact at the organization. The participants were able to provide adequate insight into the organization's internal control structure in the context of information systems security. The target organization has four main divisions: IT development, IT infrastructure, Security, and Project management. Each division head and the manager from the particular department were interviewed. The CIO of the organization and the chief audit officer were interviewed as well. The overall representation of the respondents (top management, middle management, and operational level) provided useful insights into the applicability of the developed objectives in the particular organizational context.

Data analysis

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, which is relevant for the theoretical construct under study. With useful data, the researchers categorize and structure the data in a way the meaningful interpretations can be drawn. The categorization is done through writing summaries, synopses, or making networked diagrams that permit conclusion drawing. Finally, conclusion drawing is the interpretive process through which the researcher compares themes, patterns, and then compares and contrasts to triangulate the data. Walsham (2006) suggests that even though the researcher is the agent of the interpretation, but a theoretical framework should be used to guide and bound the researcher. Each of the above three steps was performed several times, iteratively before actual results emerged. The initial 17 objectives were converted into groups based on the data from the case study. These clusters were revisited multiple times to finally come up with four clusters of objectives based on underlying themes. Identifying an informant and the key stakeholders in the case study setting helped in applying the triangulation technique. Each dimension of OSG is discussed in the results section.

3. RESULTS & DISCUSSION

Mishra (2015) proposed seventeen means OSG objectives (table 1). In the data analysis stage, data triangulation from interviews, manuals, policies, and audit guidelines, these objectives were clustered together based on the emergent themes and underlying meaning represented. Four organizational security governance dimensions were identified, and a discussion about each is presented below.
Insert table 1 here

Structural Dimension

The first underlying dimension identified in the thematic analysis is the Structural dimension. In this dimension, the scope of the objective is top management in the organization, and the target is the entire organization. The objectives that are grouped under this dimension are: *Establish formal control assessment functionality, Encourage management commitment, Resource allocation, Ensure visible executive leadership, and Data criticality.* All objectives in this group are meant for strategic long term changes in the organization, providing a directional path to the future. Such decisions are under the purview of top management and measure instituted; as a result, are for an entire organization to follow.

Formal controls assessment functionality allows establishing security governance as a functional requirement. Security has always been considered a nonfunctional requirement. Also, a distinctive feature of security requirements is that they are asset-driven – their goal is to protect the set of identified assets (Savola, 2013). Having a centralized entity for controls assessment would allow separate budget allocation for security governance functions and help in establishing a business case for security governance. A controls department would integrate controls into the business processes.

Management needs to actively participate in security governance initiatives by rewarding conformity with controls and encouraging values such as dedication, determination, open-mindedness, and truth. If management communicates effective governance as "top priority," the controls instituted are considered seriously by the employees. Management at CCIT participates actively in ensuring that precise controls are developed and implemented in the organization. The input from upper management is crucial for the success of the controls. The CIO of CCIT gets involved in the development process of the controls and the

policies at every stage and demands a weekly progress report.

Resources are the lifeline of the security governance program. Before developing the precise controls and implementation plan, organizations need to take initiatives to build the right environment for controls. Some of the proactive control initiatives that this research suggests are getting adequate resources for developing physical controls, encouraging coordination between departments, and discouraging an environment of fear and politics in the organization.

An effective information security governance program requires visible leadership to provide the direction to controls management in the organization. This objective entails a leadership style and philosophy that gives momentum to the controls program (Mishra, 2020). The perception about security governance is created by the leaders who should be able to "walk the talk." This objective suggests that the leadership in that organization should present exemplary behavior and be able to nurture relationships with cohorts.

Data criticality entails assessment and classification of data according to sensitivity level and identification of data owners. Maintaining the confidentiality, integrity, and availability of the data is not only required for securing business processes but also needed for regulatory compliance purposes. Since CCIT forms and supports the backbone of the IT infrastructure for the City, it is imperative that the organization ensures the protection of critical data and make it available to all.

The management at CCIT feels that developing controls for proper access to data requires adequate segregation of duties. To summarize, all objectives in this dimension are essential, and the measures used have long term strategic implications for the organization and its OSG program.

Insert table 2 here

User Dimension

The User dimension emerged as the second dimension of OSG. The scope of this dimension is the individual user of controls, and the target is all controls instituted to implement the security plan. Objectives grouped under this dimension are: Achieving group cohesiveness, Alignment of individual and organizational values, Ethical and moral values established, Maximize trust building mechanisms. All objectives in this group are aimed at individuals who ultimately use the controls and ensure their success.

Enhancing group cohesiveness helps in regulating the group behavior about security controls. Peer pressure and groups' behavior influences and shapes the action of the individuals (Mishra, 2015). It is essential to encourage the ability to share the work and credit for the accolade, discourage favoritism and self-interest in groups and respect personal integrity in the group. Developing teams (Eloff and Eloff, 2005) is a vital, OSG objective. People derive part of their identity from workgroups (Hogg and Terry, 2000). The groups influence whether particular rules and controls would be followed or not. Thus encouraging cohesive groups with favorable security governance perceptions can help the organization's security program.

The management encourages groups to achieve goals. The groups' achievements could trickle down to the individuals. It was also evident from informal meetings and observations that the organization has an influential 'group' culture. Enhancing group cohesiveness would undoubtedly have an impact on the controls knowledge and behavior in this organization.

Security controls should be in alignment with the individual's beliefs and values such that the probability of success of the governance program increases. This alignment could be achieved in so many ways. Leach (2003) argues that in situations of conflict between individual and organization value systems, most people are unable to survive the tension for long. Even in the light of various legislations the agency had to follow, there were incidents of non-conformity with rules and regulations. An ethical organization would encourage the right work ethics and institute appropriate moral values in the employees to shape a favorable perception about security controls. Management should encourage people to take pride in their jobs and that the correct display of morality is rewarded and valued in the organization. Strong leadership helps in actually establishing the importance of ethics and morality in the organization (Mishra, 2020). At CCIT, the administration respects the personal integrity of people and rewards examples of ethical and moral behavior through a "star of the month" program. In this program, employees who have, in some way, set standards of proper ethical conduct, which can influence people, are

acknowledged publicly by the management monthly, and the description of the action along with the winner's name is displayed in the meeting areas.

Building trust is critical to ensure that individuals can work according to the expectations of the management without close supervision. Trust is the enabling of confidence that something will or will not occur in a predictable or promised manner. The enabling of faith is supported by identification, authentication, accountability, authorization, and availability (Mishra and Dhillon, 2006). Employee beliefs about strong security governance in the organization are a good predictor of security success in the organization (Stanton and Stam, 2005). Outsider stakeholders should be able to trust the security measures in the organization to work with it and develop a positive perception about the reliability of the firm in the market. In summary, all actions taken by CCIT under these dimensions is to align individual users of controls with the organization's values about OSG objectives. Table 3 below presents the summary.

Insert table 3 here

Processual Dimension

The third dimension that emerged, Processual, represents processes orientation of organizational security governance. The scope of this dimension is every process that comes under control implementation purview, and all people linked to these processes are the target of the dimension. The objectives that are grouped in this dimension are Efficacy of Audit Processes, Clear controls development process, Monitor and Feedback, Standardization of controls, and clarity in business processes. All objectives in here have the focus and intent of developing, improving, and sustaining the process of security governance to better security practices.

Auditing acts as a catalyst for the management to accelerate its efforts for information systems security governance. This objective is useful, especially in the context of change management, to ensure the segregation of duties in the organization. Audit efficacy is required to assess management's adequacy with dealing with vulnerabilities. The role of auditing in improving the effectiveness of security controls is well understood and communicated at CCIT. The perceived purpose of auditing at CCIT is to assure the quality of controls that are in place and active. The management believes that auditing "gives them meaning for doing things." Even though the medium of business transactions have changed from paper format to electronic data, the traditional wisdom accrued from auditing and accounting standards is still valid.

The transparent control development process creates a positive perception of the controls and ensures transparency in control activities. This objective emphasizes the importance of systemization in the control development process and defines achievable goals. This objective encourages developing simple, flexible, timely, and easy to use controls. The transparent control development process helps in protecting critical business processes through multiple layers of controls as the requirements of such complicated controls are established for everyone.

The clarity in control development processes is emphasized at CCIT. The management encourages employees to clarify any doubts about the policies and welcomes questions about them. The administration has created a channel through which such requests are formally processed. The human resources department in this organization is responsible for enabling all the employees to get access to any resource that the employees might need to understand the policies better.

Monitoring controls require effective and established channels to incorporate feedback for further enhancements. Periodic review from external auditors strengthens the structure of the control and helps in analyzing the alignment between control objectives and overall business objectives. Monitoring controls and incorporating the feedback from employees is emphasized by all the prevalent governance models (ISACA, 2012). CCIT believes in robust monitoring and feedback channels for the success of information security governance. It has a monitoring program, for the most part, for all its processes and controls.

Standardization of the controls helps in benchmarking the governance activities, such as design and implementation of controls and investment in security governance activities, against other players in the industry Standardization provides opportunities for learning from others and avenues for growth. It also helps an organization gain acceptance internationally in the eyes of regulatory authorities or third party vendors.

The controls developed at CCIT need to be specific to the organization. The standardization process also helps in meeting the compliance criteria and is seen positively by the external auditors.

Establishing clarity in business processes is essential to maintain business integrity. This objective emphasizes the role of an adequate understanding of the workflow. Unless the interrelationships of the business activities and the flow of information are established, it is challenging to integrate appropriate security controls seamlessly and protect the business. Many businesses suffer vulnerability because of the lack of a deep understanding of the business processes resulting in inappropriate controls being implemented.

At CCIT, the management believes that controls should be integrated into the business processes. For governance purposes, it is crucial to understand the dynamics of business processes within the system for good security (Savola, 2007). It is essential to recognize the linkages of information security with business processes and have abilities to create and distribute new knowledge horizontally and vertically in the organization by using regular business interactions (Savola, 2007).

INSERT table 4 here

Facilitation dimension

The final dimension proposed in the study is Facilitation. The scope of this dimension is all the other three dimensions, and the target is all employees, management, and processes. The central role of these dimensions is to facilitate the interaction of three dimensions with one another. The OSG objectives grouped under this dimension are: *Communication about Controls, Training, and education about controls and Ensure punitive structures.* All measures taken under these objectives are to ensure that management, user, and processes interact as intended and aligned with the overall aim of securing informational assets.

Communication about controls is vital to articulate the vision of the management about security and establish a constructive debate about the usefulness of such activities. The management at CCIT is serious about communication with the employees regarding controls. The CIO has an informal meeting every second Friday with the employees where the pertinent issues about security and controls are discussed, employee feedback is taken, and agreement on the future course of development is reached. The emphasis on developing communication channels help employees to identify with the organization and the work that they do in groups.

Education about the need for controls creates awareness in the organization about risks, responsibilities, and social engineering issues. Training employees about usage and scope of controls help the end-users in understanding the impact of controls on day-to-day work and also reminds people to apply their knowledge in practice. Training should be enforced, and the effect of such measures should be assessed periodically. Regular training programs should be designed early on in the security governance strategy.

Training and education are much emphasized in CCIT, in theory, and practice. The upper management in the organization schedules regular training of the employees on various issues, including security awareness and controls.
Training the employees on the use of various applications for business processes and other related technologies ensures a better understanding of the expectations of the employees.

The training and education emphasis at CCIT has helped create awareness about security controls and governance. There is evidence in the research literature to support CCIT's efforts on training and education. The management utilizes resources for the knowledge of its employees about security control issues, which in turn prevents the unintentional breaches of security. Training could communicate higher-level concepts such as security action cycles but also detailed information about specific vulnerabilities (Yaokumah, 2014).

Punitive structures require the management to establish clear consequences for non-compliance with policies and ensure disciplinary action against unacceptable behavior. The impact of deterrence activities, according to our data, is significant for impeding non-compliance with controls and procedures. Developing countermeasures helps in conformity with rules and regulations. Information systems security research has established the importance of deterrence criteria for better security (Dhillon and Torkzadeh, 2006; Straub, 1998).

A punitive structure continually reminds the employees about the consequences of their

actions. A combined proactive and preventive approach to security prevents users from IS misuse (Darcy and Hovav, 2007). Repeated efforts are required to instill the results of non-conformity with polices into the minds of the employees. The top management also feels that one of the biggest drivers for establishing deterrence in not adhering to the controls in the organization is frequent auditing. The management believes that the process of auditing implies that "you are being watched" and "you will get caught" if you are deviating from the accepted behavior.

Insert table 5 here

4. DISCUSSIONS AND CONCLUSIONS

This study presents four dimensions of OSG objectives based on the scope and targets these objectives in an organization. These dimensions are well supported by research literature (table 6) and overall provide end-to-end coverage of security initiatives in an organization. The first three dimensions present a holistic picture of an organization and every possible security activity that could be performed to negate threats. The last dimension, Facilitation, enhances the interaction of these dimensions with each other. For example, training and education enable end-users to understand and comply with policies in a better way. The clear punitive structure ensures that users follow procedures at all times. The proposed dimensions of OSG are essential in undertaking holistic, comprehensive, and strategic security planning for controls.

Insert table 6 here

This research makes a unique contribution to the security governance field. This study empirically validates the OSG objectives that are developed are grounded in the values of the organizational stakeholders (Mishra, 2015). OSG objectives, such as *ensure clarity in controls development processes, ensure corporate control strategy, ensure punitive structures, ensure formal control assessment functionality, and maximize group cohesiveness*, are relatively unused in the research literature in this area. This case study examines and supports the importance of such objectives and calls for better use of these constructs in real settings. This study contributes to practice significantly by establishing that these objectives are ready to be used and can improve an organization's comprehensive security plan and elevate their security posture. The dimensions of OSG proposed in this study allows management to focus on specific areas relevant to their environment. This study should fuel further inquiry in this area. Further studies in this area could look at correlations of these objectives and their statistical significance.

Organizational security governance objectives provide the basis for strategic planning of security initiatives in an organization. The security controls, derived from OSG objectives, ensure that the corporate vision is reflected in and aligned with the security activities designed for day-to-day business operations. The means objectives developed by Mishra (2015) were reviewed to validate the objectives empirically. The results show that the objectives proposed in a prior study provided new insights into OSG practices in a real organization. The organization is using all OSG objectives, and the management acknowledged the usefulness of such objectives for comprehensive security in the organizations.

5. 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

Alotaibi, M., Furnell, S. and Clarke, N. (2019) "A framework for reporting and dealing with end-user security policy compliance," Information & Computer Security, Vol. 27 Issue: 1, pp.2-25, https://doi.org/10.1108/ICS-12-2017-0097

Brotby, W. (2009).Information Security Management Metrics: A Definitive Guide to Effective Security Monitoring and Measurement, Taylor & Francis Group, FL

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

Dhillon, G., and Torkzadeh, G. "Value-focused Assessment of information systems security in organizations," Information Systems Journal (16:3) 2006, pp 293-314.

Eloff, J., and Eloff, M. "Integrated Information Security Architecture " Computer Fraud and Security (11) 2005, pp 10-16

Hogg, M. and Terry, D. (2000), Social Identity and Self-Categorization Processes in Organizational Contexts, The Academy of Management Review, Vol. 25, No. 1 (Jan. 2000), pp. 121-140

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

ISACA 2012. COBIT 5: Enabling Processes.

Kaplan, B. & Maxwell, J.A., 1994, Qualitative research methods for evaluating computer information systems, in Evaluating Health Care Information Systems: Methods and Applications, J.G. Anderson, C.E. Aydin, and S.J.Jay (eds), CA: Sage, p.45-68

Leach, J. "Improving User Security Behavior," Computers & Security (22:8) 2003, pp 685-692.

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**.** (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

Nicho, M. (2018) "A process model for implementing information systems security governance," Information & Computer Security, Vol. 26 Issue: 1, pp.10-38, https://doi.org/10.1108/ICS-07-2016-0061

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

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

Savola, R. M. (2013). Quality of security metrics and measurements. Computers & Security, 37:78–90.

Stanton, J., and Stam, K. (2005). "Analysis of end user security behaviors," Computers & Security (24) 2005, pp 124-133.

Straub, D. (1998). "Coping with systems risk: security planning models for management decision making.," MIS Quarterly (22:8) 1998, pp 441-465.

Tan, T., Maynard, S., Ahmad, A. and Ruighaver, T. (2017) "Information Security Governance: A Case Study of the Strategic Context of Information Security" (2017). PACIS 2017 Proceedings. 43. http://aisel.aisnet.org/pacis2017/43

Tickle, I. (2006). "Data integrity assurance in a layered security strategy" Computer Fraud & Security), pp 9-13.

Walsham, G. (2006) "Doing Interpretive Research," European Journal of Information Systems (15:3) 2006, pp 320-3.30.

Yaokumah, W. (2014) "Information security governance implementation within Ghanaian industry sectors: An empirical study," Information Management & Computer Security, Vol. 22 Issue: 3, pp.235-250, https://doi.org/10.1108/IMCS-06-2013-0044

Appendices and Annexures

	Objectives	Key Lessons
M1	Ensure the Efficacy of Audit Processes	Have frequent internal and external audits Treat auditors as consultants to assess management's adequacy
M2	Maximize Clarity in Business Processes	Efficiently designed mature business processes are better protected Provide an end-to-end view of the business process and manage changes
M3	Ensure Communication about Controls	Have frequent debates about controls Develop communications policy for constructive communication within and outside functional groups
M4	Ensure Alignment of Individual and Organizational Values	Promote values such as respect for others, privacy, integrity, self-pride in job and honesty Involve users in the development process to understand an individual's attitudes and beliefs about security
M5	Ensure Data Criticality	Assess and classify data according to sensitivity Identify data owners to assign responsibilities according to information criticality Link data with authorizations for secure and reliable IT infrastructure
M6	Ensure Punitive Structures	Establish clear consequences and disciplinary actions against non-compliance with policies Explain the meanings of criminal acts and respond effectively in cases on non-compliance
M7	Ensure Clarity in Control Development Process	Develop a favorable perception and transparency of the controls Develop simple, flexible, timely and easy to use controls
M8	Ensure Formal Control Assessment Functionality	Develop formal entity for control assessment Differentiate between lines of business and industries before applying popular OSG frameworks Stakeholder's viewpoints need to be reflected in the governance process Perform periodic cost-benefit analysis and IT architecture review for the correctness of design for the security controls
M9	Maximize Monitoring and Feedback Channels	Helps in achieving the performance standards set for the IT processes Assures "what is being claimed" is accomplished Incorporate the feedback into the controls
M10	Ensure Visible Executive Leadership	Fundamentally helps in improving the perception of security governance Lead by example and nurture the relationships with employees executive
M11	Maximize Group Cohesiveness	Group behavior influences and shapes individual' perception of security controls Discourage favoritism and self-interest in groups and manage peer pressure
M12	Maximize Management Commitment	The reward for conformity with controls and encourage values such as dedication, determination, open-mindedness, and truthfulness Establish adequate controls as a "top priority."
M13	Maximize Resource Allocation for controls	Groundwork before developing controls requires coordination of multidisciplinary functions Allocate appropriate resources in a politics-free environment
M14	Encourage Standardization of Controls	Create systemization in the control development process and assess against mechanisms employed by others Benchmark security investments and governance practices to learn from others
M15	Maximize Training and Education	Awareness about social engineering issues can be provided with work-related examples

		Apply the knowledge in daily practice with focused training and education
M16	Ensure ethical and moral values	Propagate right ethical environment Leadership establishes the right tone of ethics in organizations
M17	Maximize trust building mechanisms	Develop a conducive environment for controls deployment Enhance trust with partners within and outside the organization

Table 1: Means Objectives for Organizational Security Governance (OSG) in organizations as proposed by Mishra (2015).

OSG Objectives	Evidence from CCIT	Measures at CCIT
Formal control assessment functionality	"The biggest problem is that controls have limited resources. We want to do so many things but can't do it. Like it [controls] needs to be constantly modified and monitored, but that [modification and monitoring] needs investment. Do we have separate money for this as a department? We are always in a cash crunch."	Cost-benefit analysis for controls Ensure resources Developing a formal entity for centralized controls management
Encourage Management commitment	"Taking inputs from people is important, managers and directors. Decide how they want a particular environment, the money, and resources to be used, and the controls. Employees want more flexibility but don't know what they want. Employees are always asking- why do we need to do this when you incorporate their inputs. A better approach would be to stick to the top and find out what the management wants and work with your given constraints. Find out what it is that you can do with these resources."	Management seeks inputs from people Management ensures that a refined version of the policies and control is presented to the higher management as City level CIO is supportive and gets an updated every week
Resource Allocation	"We have tools you can buy and put them in place to protect that [data]. We don't currently have those; it's a great job to get those tools, to get the funding for that, to get the people for that."	Management ensures resources for the new development of policies and controls Enhance trust measures to encourage "demand for resources" being considered Seek more resources to get the controls working
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."	CIO is supportive of the new security policies and controls Management into confidence the leadership at the city level
Data criticality	"We do have data that is so crucial. We may have health data; we may have social security numbers and the names and dates and all of those things. Also, employee details that we need to keep private as well. We interact with other state agencies, and there is other information. We have access to DMV, which means details of basically anybody owns a car, so a lot of data. We must ensure that data doesn't go anywhere where it shouldn't be, so from that point, this is what we are going for. All of the IT security controls are all about the data."	Ensures confidentiality, integrity, and availability of data to all Provides a technically superior state of the art service center with 24/7 hotline and helpdesk services. Segregation of duties Stringent access control policies & authorization mechanisms Strict password policies

Table 2: Structural dimension of OSG

OSG Objectives	Evidence from CCIT	Measures at CCIT
Efficacy of Audit Processes	"I think that if I took over if I became the CIO, I would be looking at every one of my team members, and I would tell them to prepare for an audit. I would bring an auditor here, and each one of my team will get audited. That would give me a baseline as a new boss to work on; I can only improve. If it got any worse, my job should be gone, that's what I would do. Management should be responsible for what's going on. Economy improves if the government works."	Management believes in frequent audits Use audit as a deterrence tool Used to provide quality assurance "Audit on-demand" encouraged
The clear controls 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."	Encourages employees to clarify doubts Make all resources about controls accessible Simple and easy to use controls
Monitor and Feedback	"The system in which I am right now, I am in a place where I can 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."	Monitoring tools are used Sessions for obtaining feedbacks Feasibility analysis of the controls through monitoring
Standardization of controls	"I guess one of the other very important things and a lot of people don't do this, establish acceptance criteria. That means that you are going to determine what the controls will do and how everyone has to act, for it to work, and then to ensure that it does act. It has to be consistent."	Consistent controls Refer to the industry frameworks Required for the third party vendors
The clarity in business processes	"I think they [controls] should be designed to help to ensure that your data and processes are sound, that your money is accounted for, and your resources are applied correctly. Also, your performances and expectations are met as an agency. It should improve the business process."	Control the software purchasing system Controls build along the business process Controls are essential for business success

Table 3: Processual dimension of OSG

OSG Objectives	Evidence from CCIT	Measures at CCIT
Achieving group cohesiveness	"What can you say at the end of the day that you have contributed? Ideally, you want the employees to plan at the beginning of the day, what they can accomplish that day, what is the next thing that they can do to accomplish their goals, and then achieve something at the end of the day. Here is what I started to do, and here's what I did in the day, goals, and accomplish on a daily, weekly, and monthly basis in the way it's measurable. So control would be to motivate them as a group."	Set group targets Encourage group activities Track the people based on their groups Educate groups about controls
Alignment of individual and organizational values	"I mean, in reality, our values, our values should define that we are going to do the best we can, do the right thing at any point in time. If my values allow, then only I will follow the rules."	Use psychological measures to understand employees Have frequent lunches to "draw in" the employees Portray controls as something to protect the employees against harm. It's about them not the bosses
Ethical and moral values instituted	"so we can make a rule, we can make a law that you have, to be honest. I mean, in reality, our values, our values should define that we are going to do the best we can, do the right thing at any point in 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."	"star of the month" program Leadership is encouraged to "walk the talk." Management provides the right environment
Maximize Trust building mechanisms	"I am talking about the whole City. They [other agencies under the City] have to trust IT to develop these policies and controls. We have the best interest in doing so. It is good for compliance as well with any federal state and local law".	Equipment lying openly in the office as there is mutual trust about not stealing City's property Managers maintain consistency in "saying and doing."

Table 4: User dimension of OSG

OSG Objective	Evidence from CCIT	Measures at CCIT
Communication about Controls	"Typically, in our case, we would draft a policy, edit it, and go to the City. Managers and other directors from other agencies need to work on this, but there is no communication among them. So there is no feedback. If there is the thing that you don't agree with, tell us, we need to get there input. They need to be treated. Differently, they are different departments".	The manager meets with employees every second Friday Communicate with people even when they communicate back Prevention is better than creating vulnerability hence express to protect the people
Training and education about controls	"Human nature it is that they [employees] may read the policy and go "ok I do know that" but they wouldn't read in the details. There is an education factor also, to get the word out to people. When you sign these forms, this is what it meant, and you are held responsible. Part of the procedure and guideline will keep, make it standard this is what happens when you don't do this, first warning, second warning, third warning. I believe that our HR is working on some of that now."	Extensive training about applications and business processes Explain with work-related examples Encourage the use of knowledge in practice Provides incentives for education (gift cards)
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 some type of thing that says even if the employee violates this, what is going to happen to him."	Explain consequences and send reminders Clear punitive structure Punish in case of security breach or non-conformity with controls

Table 5: Facilitation dimension of OSG

Dimension	Scope and Target	OSG Objectives	Literature support
Structural (5)	Top management/ Corporate-wide	Formal control assessment functionality Encourage Management commitment Resource Allocation Visible Executive Leadership Data criticality	Tickle, 2006; Myler and Broadbent, 2006; Savola, 2007; Yaokumah, 2014; Alotaibi, M., Furnell, S. and Clarke, N., 2019
User (4)	employee/ Individual-level	Achieving group cohesiveness Alignment of individual and organizational values Ethical and moral values instituted trust-building mechanisms	Mishra, 2015, Mishra and Dhillon, 2006; Nicho, 2018
Processual (5)	Security processes/ Anyone part of that process	Efficacy of Audit Processes The clear controls development process Monitor and Feedback Standardization of controls The clarity in business processes	Goel et al., 2006; Mishra, 2015; Tan et al., 2017; Mishra, 2015
Facilitator (3)	Management/individual/ Processual/ Multiple levels	Communication about Controls Training and education about controls Ensure punitive structures	Darcy et al., 2009; Dhillon and Torkzadeh, 2006; Fuller et al., 2007; Abu- Musa, 2010

Table 6: The four dimensions of OSG