In this issue:

4. Digital Transformation and Geospatial Analytics
   Ileana Abot, Xavier University
   Thilini Ariyachandra, Xavier University

13. Examining Organizational Security Governance (OSG) Objectives: How strategic planning for Security is undertaken at ABC Corporation
   Sushma Mishra, Robert Morris University

25. An Exploratory Study of the Perceptions of Library Faculty and Patrons on Library Resources
   Kyle Herman, Georgia Southern University
   Hayden Wimmer, Georgia Southern University
   Carl Redman Jr., University of San Diego

33. Developing a GIS Dashboard Tool to Inform Non-Profit Hospitals of Community Health Needs at the Neighborhood Level
   Evan Copello, University of North Florida
   Jason Smith, University of North Florida
   Anna Mease, Mayo Clinic
   Karthikeyan Umapathy, University of North Florida
   Dan Richard, University of North Florida
   Ann-Marie Knight, Mayo Clinic
   Monica Albertie, Mayo Clinic
   Hana Hamadi, University of North Florida
   Aaron Spaulding, Mayo Clinic
   Emma Apatu, McMaster University

54. A Longitudinal Study of Google Privacy Policies
   Alan Peslak, Penn State University
   Lisa Kovalchick, California University of Pennsylvania
   Mauir Conforti, Geisinger Health System
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 issues a year. The first date of publication was December 1, 2008.

JISAR is published online (http://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. (http://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 EDSIG who perform the editorial and review processes for JISAR.

### 2020 Education Special Interest Group (EDSIG) Board of Directors

<table>
<thead>
<tr>
<th>President</th>
<th>Vice President</th>
<th>Past President</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jeffry Babb</td>
<td>Eric Breimer</td>
<td>Leslie J Waguespack Jr.</td>
</tr>
<tr>
<td>West Texas A&amp;M</td>
<td>Siena College</td>
<td>Bentley University</td>
</tr>
<tr>
<td>Professor</td>
<td>Vice President</td>
<td>Past President</td>
</tr>
<tr>
<td>Jeffrey Cummings</td>
<td>Melinda Korzaan</td>
<td>Lisa Kovalchick</td>
</tr>
<tr>
<td>Univ of NC Wilmington</td>
<td>Middle Tennessee State Univ</td>
<td>California Univ of PA</td>
</tr>
<tr>
<td>Director</td>
<td>Director</td>
<td>Director</td>
</tr>
<tr>
<td>Niki Kunene</td>
<td>Li-Jen Lester</td>
<td>Michelle Louch</td>
</tr>
<tr>
<td>Eastern Connecticut St Univ</td>
<td>Sam Houston State University</td>
<td>Carlow University</td>
</tr>
<tr>
<td>Treasurer</td>
<td>Director</td>
<td>Director</td>
</tr>
<tr>
<td>Rachida Parks</td>
<td>Michael Smith</td>
<td>Lee Freeman</td>
</tr>
<tr>
<td>Quinnipiac University</td>
<td>Georgia Institute of Technology</td>
<td>Univ. of Michigan - Dearborn</td>
</tr>
<tr>
<td>Membership</td>
<td>Secretary</td>
<td>JISE Editor</td>
</tr>
</tbody>
</table>

Copyright © 2020 by Information Systems and Computing Academic Professionals (ISCAP). Permission to make digital or hard copies of all or part of this journal for personal or classroom use is granted without fee provided that the copies are not made or distributed for profit or commercial use. All copies must bear this notice and full citation. Permission from the Editor is required to post to servers, redistribute to lists, or utilize in a for-profit or commercial use. Permission requests should be sent to Scott Hunsinger, Editor, editor@jisar.org.
Examining Organizational Security Governance (OSG) Objectives: How strategic planning for Security is undertaken at ABC Corporation?

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

Abstract
Organizational security governance (OSG) objectives provide a strategic direction to the organization’s comprehensive security planning. It is essential that security planning has overarching objectives such that the proposed controls and measures are contextually grounded. Mishra (2015) proposed six fundamental and seventeen means objectives, theoretically and empirically developed, to provide a strategic basis of an organization’s security program. The purpose of this study is to examine the proposed six fundamental OSG objectives in an organizational context and assess how it guides the security efforts. A case study was performed to understand the use of the six fundamental objectives in the overall security program. The results suggest that the OSG objectives indeed provide a strategic basis for developing security measures of the organization. Implications are drawn and contributions listed.

Keywords: Organizational Security Governance, Strategic planning, Regulatory Compliance, Policy, Controls, IT Audit

1. INTRODUCTION
In today’s environment, cyber-attacks are on the rise, and security investment has grown manifolds for strengthening preventive measures. However, organizations are struggling for strategies to address such attacks (Ahmad et al., 2014). The biggest problem with such reactive security planning is that organizational security governance (OSG) objectives are missing and there is a lack of potential implementation strategies for such objectives. It is essential to understand how OSG influences strategic decision-making in information security and ensures that investments in security are not wasted (Tan et al., 2017). There is little guidance, in the research literature, on how organizations develop OSG and implement them.

Mishra (2015) proposed six fundamental and seventeen OSG objectives, grounded in theory and data, which could provide comprehensive security strategic planning and measures to ensure more secure organizations. Fundamental objectives are the core of the OSG program, whereas means objectives support the fundamental objectives. For a more detailed understanding of these objectives, refer to Mishra (2015). The fundamental objectives are essential to achieve strong OSG. All means objectives help in achieving one or more fundamental objective for better OSG practices. This study focusses just on the fundamental objectives as these form the core of the OSG program. The six proposed fundamental objectives are F1-Ensure Corporate Controls Strategy, F2-Encourage a Controls- Conscious Culture, F3-Establish Clarity in Policies and Procedures, F4-Maximize Regulatory Compliance, F5-Ensure Continuous Improvements in controls and F6-Enable Responsibility and Accountability in Roles (table...
The organizational structure includes the CIO as the head of the agency. Five managers directly report to the CIO. There is an application division that controls all in-house development. The database systems and the enterprise system are under infrastructure services that are managed by a manager. A training division provides administrative support functions. Project management division looks at the feasibility of all proposed projects and makes decisions about the ones that will get funded. There are well above 100 employees, multiple consultants, and many open positions for hire. 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. All the policies, procedures, and controls are transparent as the state agency is under the purview of public scrutiny and audit and compliance requirements on an ongoing basis.

For this study, ten interviews were conducted at ABC Corporation. Participants included top management, middle management, support staff, auditors, and developers. There were secondary sources of data examined, such as security policies, procedures, project reports, training documents, and audit manuals.

## 3. RESULTS & DISCUSSION

### F1-Regulatory compliance at ABC

Regulatory compliance ensures that the organization meets all the legal and mandatory requirements about security and internal controls. This objective entails formalizing the process of compliance in the organization and promotes the development of controls in accordance with legislation. The objective entails following the regulations in their entirety and using the legislation as a catalyst for the improvement of security governance.

ABC, as a state agency, has HIPPA and e-discovery as its principal regulations to comply with. The agency has a compliance audit, both from internal as well as external auditors. The culture in the organization is such that transparency about processes and availability of information are considered of paramount importance. The CIO is aware of people’s right to ask for different types of information about the agency and the use of taxpayer’s dollars in operations. By state law, most of the information about the agency’s current and future plans are accessible through the website. The common perception of employees, of the regulations and the compliance efforts in the organization is that
of a “necessary evil.” The middle-level managers and the line staff consider compliance as the “right thing” to do but not necessarily helpful. The sentiment of frustration is understandable, given the mammoth preparations required for compliance. Compliance with laws such as SOX is costly (Bennett & Cancilla, 2005). It needs managerial as well as technical support to create an infrastructure in organizations to meet the demands of this law. Some of the specialized areas that need particular concern for compliance purposes are: data management issues (Volonino et. al., 2004; Farris, 2004, Yugay and Klimchenko, 2004), security of data and system, choice of software development methodologies that could incorporate the compliance issues in its lifecycle, robust documentation for external auditing purposes, versioning and auditibility of electronic record needs and file systems in use (Peterson and Burns, 2005).

The internal IT audit director for the agency considers the regulations as helpful in providing momentum to security and internal controls operations in the organization. Myler and Broadbent (2006) argue that evaluation of compliance with the policies and procedures in an organization and regular follow up of the recommendations are essential. The evaluation process helps in estimating the effectiveness and possible shortcomings of the controls process. Delineating audit controls and tools to determine areas for improvement (Myler and Broadbent, 2006) is what the IT audit director for the City believes in.

The chief agency head did not have a favorable opinion about the regulations, though. As the applications development manager commented:

“In my personal opinion, compliance is reactive, not proactive. You look at SOX. Enron collapsed, and so many people were ruined or hurt, and then SOX came. So compliance is a vehicle, the way compliance operates today, I don’t think that an organization should say ok...we rely on compliance as a mechanism for developing our internal controls. If you do that you are going to be in bad shape”.

The general perception of the management about compliance is that it drives the security governance efforts backward. The regulations enforce activities that should already have been a part of the governance program in the first place. This perception is consistent with the majority of research in this area. One of the most significant managerial issues that regulations imply is for IT governance purposes (Fox, 2004). Effective IT governance would require the management to plan for preparedness for quarterly reporting, security policies, cost management for compliance, and preparation for external audit. These measures need planning and effective internal control assessment (Chin and Mishra, 2013). The administration believes that the preparedness should be there, to begin with, and not inserted as an afterthought while preparing to be compliant.

Compliance acts as a driver in getting all the resources that are required for the agency. The security officers shared how in the name of compliance, they order software, get management’s attention, and other required resources. The responsibility of the regulatory compliance efforts for the city does not lie with ABC but the larger agency. The lack of authority for regulatory compliance explains a lot of discontentment with the use of regulations in the organization. Officials at ABC comply with the requests of auditors and supply all the paperwork required. The organization plays a passive role in the City’s compliance plan.

Overall, it did appear that regulatory compliance is vital for the agency. Since the prime responsibility of being compliant did not lie with this agency; managers in the organization were candid about it. ABC used compliance as a means to get things from the City, which they would never get otherwise. Also, the organization is in the process of developing new policies and controls. It remains to be seen how these new controls are implemented and assessed. To sum up, compliance is important to ABC but not in the right spirit of the legislation. A summary of regulatory compliance at ABC is presented in the table below (table 2).

**F2-Ensuring continuous improvements in controls at ABC**

Instituting continuous improvements in controls implementation process has been identified as a fundamental objective for maximizing security governance. The control implementation process should be iterative, continuous, and adaptive. Effective implementation of controls calls for putting the right controls in the right place at the right time, and this can only be achieved through flexible implementation practices.

At ABC, the management identifies the need for a constant reevaluation of controls under
changing business conditions. Regular revalidation of the controls is important, as the Chief Security Officer shared:

“You have to keep up with it…It’s not what you are getting over with…you have to constantly keep up with it…we do have some machines and software that are from over ten years old…but you have to keep up with it….what else can we do…we need constant reevaluation as controls implementation is an evolving process”.

This Chief Information Officer at the firm has a similar vision of regularly testing and updating the control structure. The organization provides training and education to the security staff about the changing needs of controls and policies. The security officers are encouraged to attend conferences and seminars in the relevant area to keep abreast with the upcoming trends and technologies in the security area. As one of the security officer said:

“I am a firm believer that you can put whatever you want in place, but if the end user doesn’t own it up, it is not going to work. I have been in seminars where I dealt with fortune 500 companies, people who are making billions of dollars a year as revenue, and they still have the same problem. You know those guys have everything, they have done everything, but it [control implementation] needs to be a constantly evolving process. They have to learn and then reeducate because things change.”

It was apparent from the observations at ABC that management understands the importance of the controls implementation process. There were frequent meetings and seminars about security controls and discussions on how controls should be used to overcome common security breaches. However, a sense of disconnect in the attitude of the managers and the operational people, about continuous changes in controls, was felt. The knowledge about the benefits from revalidation of controls is concentrated more on the management side than on the operational side of the organization. The business folks considered control implementation as a technical requirement for the organization and distanced themselves from it. The perception in the non-security staff, working in development or other IT related areas, is that control implementation is primarily the work of security staff. The majority of operational people believe that the security staff should be responsible for the success or failure of the controls.

The enabling value of security controls has to be clearly articulated. Benefits of security governance should be linked with business objectives so that the stakeholders see the positive impact of security on attaining profits, productivity, and growth. Security governance can help in avoiding negligence and enhance strategic business goals hence acting as a motivator for top management (Wright, 2001). It is crucial to ensure that security controls and security management practices of the organization are regularly reviewed. Such reviews could lead to finding misconfigurations in the systems and identify areas where security protection is such that a single failure could result in prolonged exposures (Wilson, 2007).

**F3-Responsibility and accountability structures at ABC**

Responsibility and accountability structures ensure that roles are defined in a way that appropriate responsibilities are shared, and stakeholders are held accountable for their actions. The objective prescribes that job descriptions should be not changed abruptly, clear organizational responsibility for compliance should be defined; individuals should be made responsible for appropriate accesses, and transparency about the accountability should be encouraged.

The management at ABC completely identifies with the criticality of having clear responsibility and accountability structure for information systems security governance. The Chief Information Officer said:

“If you are talking about the outcome of the controls, then to me, its management. The idea of having a documented hierarchy, especially around data, is a must. If you think about it; we publish corporate organizational charts all the time. We should have a controls organizational chart which says, okay, if you are at this level, this is what you get [controls].”

The CIO believes in the concept of having a “controls chart,” which is similar to the organization chart. The controls chart clearly defines the responsibilities of the members regarding security controls. The controls chart is like adding control responsibilities to the organization chart. It helps in documenting the requirements for a role in owning up to the responsibility of controls. As we go up in the
controls chart, roles become more crucial for security governance; the individual higher up should have more controls and accountability associated with their work. Research in security governance suggests that increased awareness and individual accountability can significantly affect how security practices are implemented in an organization (Mellor and Noyes, 2006).

People higher up in hierarchy have greater accessibility to sensitive data and have a higher probability of creating vulnerability in the system. Mellor and Noyes (2006) found that adding personal accountability into roles helps the cause of security governance. The concept of controls chart is not implemented yet at ABC but would be helpful for security governance purposes. As explained by the CIO, it is crucial to understand what is it that we want to protect from a management point of view. If there is clarity in responsibilities and roles, better controls can be associated with the position and the individuals. For example, if the human resource people have a high level of access to crucial personal identifiable data of personnel in the organization, there should be stringent controls for people in this department. As suggested by the CIO, such managers should be audited for their access pattern every quarter to ensure that the managers are doing what they are supposed to do, and security is not being compromised. Given the nature of the sensitive information that human resources people have access to, it makes sense to have better protection and accountability for such people. Research literature suggests that top management should be proactive about responsibility assignment to roles. Myler and Broadbent (2006) argue that corporate boards that undertake the challenge of plugging IT oversights show that they understand the scope of their corporate accountability and responsibility, and are proactive in their leadership duties. If organizations do not ensure that all employees understand their information security roles and responsibilities, it may become challenging to protect the confidentiality, integrity, and availability of information assets (NIST Special Publication 800-16, 1998).

ABC has access to crucial data about the taxpayers in the City. The department has access to DMV data, readings for gas, water and electricity consumption, property details, and tax details about the residents. One of the duties of the department is to ensure that the meter reading for the household utilities is performed correctly as and when required. This operation, if not completed successfully, could present a severe threat to the integrity of the data recorded. As mentioned by the end user services manager:

“I think the accountability piece is required. How do they control, say even a meter reading application? How do we ensure that every meter gets read every morning? You have meters that haven’t been read, and there has been no consumption on that meter for over a year, and the service is still on, then there is a problem. So put controls and make someone accountable, that’s how you guarantee that every meter is being read and the consumption of gas and water is recorded.”

Reading a utility meter requires that there is appropriate segregation of duties defined in the organization else the security of the data could be compromised. It is essential to separate developers who make the application from people who read the meters and record the consumption by providing logical access to the groups. Else, it is possible for the developer to change the readings, through the application, for themselves or friends or whoever they deem appropriate.

At ABC, management is concerned about assigning appropriate responsibilities and accountability to users of the systems (see table 4). But it seemed that there is a lack of clarity about roles and responsibilities on many fronts. For example, when discussing the regulatory compliance issues in the organization, there seems to be confusion about who in the agency was responsible for the meeting compliance deadlines. People at ABC meet auditors’ request for submitting the required documents.

**F4-Corporate control strategy at ABC**

This objective suggests establishing a corporate risks management plan and developing controls guidelines using consensus. Controls should be viewed as a cost of doing business. Security controls should be a non-negotiable budget item, and adequate planning for the governance initiatives should be ensured.

The management at ABC believes that for long term strategic planning in the organization, it is essential to have a control strategy. A clear vision about the security governance and each department’s own controls plan along with an enterprise level risk assessment plan would go a long way. An information security risk assessment is the staged process by which an
organization's information assets are valued. Here, the vulnerabilities and threats are identified so that they then guide the implementation and monitoring of control strategies and measures (Whitman and Mattord, 2005).

At ABC, there is a lack of agreement between stakeholders on what should be put and how should the controls be deployed and monitored. This disagreement is a direct result of a fundamental lack of planning and understanding about what are the assets and what is that needs to be controlled. A controls strategy can provide a broad vision for the organization in this regard. As shared by the security manager:

"People should try to at first establish and see what the controls are. That’s reflected in your requirements to some degree. People need to know what they want to control. You have to know what you want to control, and the problem is that you don’t know what you want to control.”

The necessary process of controls development approach needs long term planning and undying commitment on the part of the management. The CIO believes that a strategy about controls needs to be established such that all pieces of governance program come together.

Observations at ABC suggest that a "bottom-up" approach of developing security initiatives would not work in this organization. The operational level management does not have a holistic picture of the role of controls in achieving overall security. The strategic inputs about security governance should flow from the top management to the entire organization. The lack of a controls strategy would cause the controls to be laid out without risks analysis and policies which could be expensive and detrimental. With a top-down approach to management, a more appropriate strategy in the shape of long-term policies, efficient procedures, and technical safeguards could be developed (May 2005).

An interesting observation was noted that there is inadequate planning about protecting the human assets in case of an emergency such as fire or flood. Without a sound strategy, efforts will be wasted. Therefore, a structured methodology for developing a strategy will increase the likelihood of success of corporate initiatives (Mishra and Dhillon, 2006). It is a serious issue: what is the strategy about protecting employees and equipment in case of emergency? The management at ABC seems distressed about the fact that the City does not consider this issue important enough to discuss at high-level meetings. The state of affairs at ABC does substantiate our call for a controls strategy which could plan about things such as this at the corporate level.

There is a growing awareness of the need for such a strategy (Shedden et al., 2006). Information security should be integrated into an organization’s overall management plan (Lane, 1985). Firms have to integrate IT strategies with organizational strategies to attain business objectives (Lainhart IV, 2001). In the case of ABC, the management could have an oversight committee that sets an appropriate strategy for IT governance endeavors (Myler and Broadbent, 2006), especially about security events. A summary of the control strategy initiatives at ABC is provided in table 4 below.

**F5-Control conscious culture at ABC**

A control culture ensures an environment where individuals ‘watch out’ for each other. This fundamental objective emphasizes the importance of a control culture that creates and sustains connections among various security efforts such as policies, processes, and norms. A “prevention mentality” promoted by the control culture of the organization, helps in minimizing the friction among groups over security issues. It is essential to establish standard codes of conduct for the employees in carrying out their security responsibilities.

The CIO of the organization believes in establishing a culture that needs to consider all the information that ABC has and protects it as something personal for the employees. The CIO explained:

“I think you need to have a clear core value; a clear company recognized or accepted perspective, the role of having those controls. For example, in my mind, I think you should treat everything, every data you handle like it’s your information. Would you leave your wallet out in the middle of the street, on the bench when you go to get a coffee? What type of care would you take if it’s yours? That is the kind of care you need to take.”

Management espousing similar values as it claims should ultimately lead to the shared tacit assumptions of employees becoming aligned with these espoused values of the organization, thus progressing towards information security...
obedient culture (von Solms, 2006). The management realizes that it is a long and tedious process before a control culture is established. As the chief security officer enunciated:

“Establishing the concept [the importance of controls] takes much time and commitment, to do that you want to bring that culture and it takes time, and it is just a matter of time and that it will come after you do it for long.”

The management feels that establishing a control culture would help the policies and procedures in being appropriately followed, and the management become more involved in the security governance process. The tacit knowledge of information security practices and procedures and the resulting behavior guide the day-to-day activities of the employees in the organization. As a consequence, information security practices and procedures should become part of the corporate culture of an organization (Thomson and von Solms, 2005). Observations at various meetings and informal conversations with the employees suggest that the organization had a control culture where people treat the information as they would treat their property. Maybe it is the beginning of the long and tedious process of establishing a controls consciousness of this nature because the leadership at the organization did seem determined to drive the organization towards control culture. The 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. Ideally, corporate culture should incorporate information security controls into the daily routines and implicit practice of employees (Thomson and von Solms, 2006). If the beliefs and attitudes are addressed by the management, it leads to changed actions and behaviors of the employees and synchronizes it with the overall corporate culture in the organization (Thomson and von Solms, 2008). A summary is presented in table 6.

**F6-Clarity in policies and controls at ABC**

Policies should be fair, visible, and easily accessible to all in the organization. The clarity in policies communicates management commitment to security governance.

Policies and procedures are organizational laws that determine acceptable and unacceptable conduct within the context of corporate culture (Whitman, 2003). It is a means to communicate management’s commitment to security governance efforts (Myler and Broadbent, 2006). ABC emphasizes establishing clarity of policies and controls. The conventional norm is to explain the policies and procedures frequently so that it makes an impression on the user and stays with them eventually. Usually, the most common reason why employees make mistakes about controls in the organization is the lack of understanding as to what needs to be done. Research suggests that good policies can protect vulnerabilities (Lapke and Dhillon, 2008). Better policies lead to deterrence as policies give the employees responsibility and accountability in the job (Maynard and Ruighaver, 2007). The security team feels that people never come up and ask about policies or controls unless they are in trouble. The management at ABC explains the purpose and scope of the controls proactively before the employees get into trouble.

Research literature in security policy domain argues for revisiting the policies periodically. For instance, it is becoming a huge problem to prevent employees from wasting their time on browsing the Internet during office hours. Policies about personal use of computers during office hours need to be clearly defined. Limited Internet use or unlicensed software usage should be discouraged (Schauer, 2001). Maynard and Ruighaver (2007) maintain that beside the iterative nature, security policies need quality verification periodically. This assessment needs to be carefully managed to ensure a balanced approach and make sure that stakeholders have adequate skills and training to assess quality. The management also believes that policies should be developed as a continuous process so that changing business needs are reflected.

The taxpayers should be able to access the security policies to have confidence in the city’s security measures about protecting their data. Also, the current policies have not been made easily accessible to the employees as well. The lack of clarity creates a potential rift in the minds of people about the policies. As the security staff officer explained:

“We had regulation and policies established but did people know that? Make all the required things accessible to people. Our policies are so hard to find on our website that I don’t know how anyone can ever read them. This is serious”.
The management is developing a new set of security policies and procedures. It is planned that the security policies would be made accessible to all the citizens at the web site. A central repository of security policy and control resources would be created on the Intranet which would be available to all Agencies Citywide. The management has planned extensive educational sessions to establish the clarity of new policies. It remains to be seen in the future though that how well these measures play out in creating effective security governance. A summary of how clarity of policies and procedures is being accomplished at ABC is presented in table 7 below.

The case study data suggests that all six fundamental OSG objectives are meaningful to ABC Corporation and are guiding the security program of the organization in many ways. The objectives thus examined are relevant to the organizational context and provide a strategic basis for planning current and future security initiatives. Both research questions are adequately addressed in this section.

4. CONCLUSIONS

This study uniquely contributes to research in information security governance domain. The empirical validation of OSG objectives proposed in the literature provides a meaningful way of developing comprehensive security governance program in organizations. It contributes to practitioners in organizations in terms of delivering overarching OSG objectives for strategic planning of security to prevent breaches. It also provides prescriptive measures that could be used to strengthen security initiatives.

5. REFERENCES


## Appendices and Annexures

<table>
<thead>
<tr>
<th>Objective</th>
<th>Key Lessons</th>
</tr>
</thead>
</table>
| **F1** Ensure Corporate Controls Strategy | Control strategy aligns the security governance and business objectives  
Antecedent to complete security and process integrity  
Provides the departments with control plans |
| **F2** Encourage a Controls-Conscious Culture | Risk consciousness in employees creates a “prevention mentality.”  
Helps in minimizing intergroup rivalry over security governance initiatives  
Creates an environment where individuals “watch out” for each other |
| **F3** Establish Clarity in Policies and Procedures | Ensure the proper use of the applications and technological solutions instituted  
Make policies easily accessible  
Reflect control requirements in the systems  
Develop visibility of fair policies |
| **F4** Maximize Regulatory Compliance | Meet legal, regulatory and contractual obligations  
Use compliance as a driver to develop security governance initiatives |
| **F5** Ensure Continuous Improvements in controls | Continuous and iterative control assessment improves the controls environment  
Understand the organizational context of particular controls  
Change in roles should be reflected in subsequent controls |
| **F6** Enable Responsibility and Accountability in Roles | Provide clarity in roles and ownership of decisions  
Promote transparency in roles and avoid sudden changes in responsibility structures |

Table 1: Fundamental Objectives for Organizational Security Governance (Mishra 2015)
Table 2: Regulatory compliance at ABC

<table>
<thead>
<tr>
<th>Objective Name</th>
<th>Evidence from ABC</th>
<th>Measures at ABC</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>F1-Ensure Regulatory Compliance</strong></td>
<td>“SOX and HIPPA and other kinds of things are to help protect those data but these are guidelines, and they really don’t mean anything by themselves because they don’t come down and tell you specifically what you are supposed to do.”</td>
<td>♦ Compliant with several legislations for the state as well as federal ♦ Internal audit department guides through the process ♦ Develop controls proactively that easily meet compliance requirements</td>
</tr>
</tbody>
</table>

Table 3: Continuous improvement in controls at ABC

<table>
<thead>
<tr>
<th>Objective Name</th>
<th>Evidence from ABC</th>
<th>Measures at ABC</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>F2-Ensure continuous improvements in controls</strong></td>
<td>“We need constant reevaluation as controls implementation is always an evolving process.”</td>
<td>♦ Constant reevaluation is done ♦ Considered an iterative process ♦ Attend seminars and conferences and learn about implementation practices form others ♦ Involve people across discipline and other agencies under the city, to help in implementation</td>
</tr>
<tr>
<td></td>
<td>“I have been in seminars where I dealt with fortune 500 companies, people who are making billions of dollars a year as revenue and they still have the same problem. You know those guys have everything, they have done everything, but it [control implementation] needs to be a constantly evolving process. They have to learn and then reeducate because things change.”</td>
<td></td>
</tr>
</tbody>
</table>

Table 4: Responsibility and accountability in structures at ABC

<table>
<thead>
<tr>
<th>Objective Name</th>
<th>Evidence from ABC</th>
<th>Measures at ABC</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>F3-Establish Responsibility and Accountability Structures</strong></td>
<td>“The idea of having a documented hierarchy, especially around data is a must. If you think about it; we publish corporate organizational charts all the time.”</td>
<td>♦ clear segregation of roles ♦ developing a controls chart with clear control responsibility and accountability ♦ encourages ownership of information</td>
</tr>
<tr>
<td></td>
<td>“So I think accountability piece is required. How do they control, say even a meter reading application? How do we ensure that every meter gets read every morning? You have meters that haven’t been read, and there has been no consumption on that meter for over a year, and the service is still on then there is a problem. So put controls and make someone accountable, that’s how you guarantee that every meter is being read and the consumption of gas and water is recorded.”</td>
<td></td>
</tr>
</tbody>
</table>

©2020 ISCAP (Information Systems and Computing Academic Professionals)
**Objective Name** | **Evidence from ABC** | **Measures at ABC** |
---|---|---|
F4-Ensure Corporate Control Strategy | “People should try to at first establish and see what the controls are. That’s some degree reflected in your requirements. People need to know what they want to control. You have to know what you want to control, and the problem is that you don’t know what you want to control.” | ♦ Provide more resources |
| | “You need to plan ahead and have a strategy about controls and its success. You need to figure out how am I going to be proactive rather than letting a reactive compliance approach drive my internal controls that we use.” | ♦ Enhance trust |
| | | ♦ Proactive controls approach versus reactive approach |
| | | ♦ Corporate level planning for security governance in advance |

Table 5 Controls strategy at ABC

**Objective Name** | **Evidence from ABC** | **Measures at ABC** |
---|---|---|
F5-Establish Control Conscious Culture | “I think you need to have a clear core value; a clear company recognized or accepted perspective, the role of having those controls. For example, in mind, I think you should treat everything, every data you handle like it’s your information. Would you leave your wallet out in the middle of the street, on the bench when you go to get a coffee? What type of care would you take if it’s yours? That is the kind of care you need to take” | ♦ An environment where individuals watch out for each other |
| | “we cannot have controls everywhere but should have control in the places where we can get the most benefit for the organization.” | ♦ Treat customers’ information as if it is your information |

Table 6: Control conscious culture at ABC

**Objective Name** | **Evidence from ABC** | **Measures at ABC** |
---|---|---|
F6-Maximize Clarity in Policies and Controls | “Make the policy and procedures clear and accessible. [Establish] Clarity in policies and controls, transparency in procedures, and gradually standardize the process; everyone knows what it could mean. What you [employee] can do to help & protect yourself without making those costly mistakes, make those very clear and understandable because if people don’t understand them and they are not clear, people can’t follow them and they make excuses” | ♦ Explain the policies repeatedly |
| | | ♦ Make the policies accessible easily |
| | | ♦ The continuous iterative process of development |
| | | ♦ Constant explanation of the benefits |

Table 7: Clarity in policies and controls at ABC