

White Paper



Information Security Challenges In Shared Services Model

Best Practices that Work

Binoy Kumar Singh

Abstract

As the title suggests, this white paper focuses on some of the unique IT Security challenges experienced in a Shared Services Model and the best practices to successfully handle and/or reduce exposure to these.

Availability of information and the ability to use it in innovative ways is the success mantra of every organization but this also requires protection of valuable information from malicious intent, inadvertent incidents and natural disasters at all times.

The nature and framework of shared services organizations, characterized by shared infrastructure, service-oriented organizational units, service groups working in silos, overlapping responsibilities, etc pose multiple challenges to the adoption and roll-out of an effective Information Security Plan. But by having the right focus on IT security governance, creating lean processes, implementing appropriate RACI and SoD matrices, providing adequate and timely training, etc the impact of these challenges can be significantly reduced.

For more information, Contact askus@infosys.com

Jul 2010

Background

Shared Services Model¹ is being increasingly adopted by medium to large organizations with the goal of improving the financial performance of the corporation. It is achieved by eliminating redundancies, optimizing use of the limited resources, economies of scale and using common/reusable tools and artifacts.

While the financial upside is encouraging, the pitfalls of IT Security, when not managed appropriately, turn out to be significant deterrents in adopting a Shared Services Model.

This paper is organized into two distinct sections:

Section I	Presents the challenges faced with the intent of increasing awareness
Section II	Discusses Best Practices that can help handle/reduce the severity of such challenges

Section I: Challenges faced by IT Security

While the challenges faced in traditional IT setups are still prevalent, the Shared Services Model come with a few additional challenges, intrinsic to the very nature of the model.

- IT Security is assigned a low priority**
Migration to a Shared Services Model is marked by an organization's focus on analyzing the offered functions, defining the service units/bundles, developing the Customer, Financial, Supplier, Operations strategies. But when it comes to IT Security, there is either an absence or almost no focus.
- Ad hoc Security Governance**
Unfortunately, an upcoming audit, a security violation or an organization-wide initiative are the core drivers for establishing Security Governance. Leaders/Stakeholders initiate more of an immediate form of Security Governance to align with these requirements and loose focus as soon as the event is over. In addition to these drivers, the absence of an effective sustenance plan makes this ad hoc nature of security governance a repeatable and expensive feature of the organization.
- Ambiguity in roles and responsibilities**
Security responsibilities are meant to be distributed throughout an organization, requiring cross-functional interaction, cooperation, and execution. It cannot be assigned to a single unit or department within an organization and should be "Everyone's" responsibility.

¹ Shared Services Model – An internal organization becomes the centralized service provider for all Business organizations in the company, promoting reuse and sharing. The Business organizations choose and request products and services as necessary from this shared service provider.

But in a Shared Services Organization (SSO), due to the bundled nature of service delivery and the overlapping responsibilities of different functions, ambiguities develop with respect to the roles and responsibilities of different players.

- **Between SSO and Business Organizations** – due to the lack of a clear definition and distinction between the roles and responsibilities, there is a tendency to assume that this is the ‘Other team’s’ responsibility.
- **Within the SSO** – the SSO is divided into multiple teams working in ‘silos’ with a number of barriers (lack of knowledge/awareness of other teams, no communication at middle management levels, insecurity amongst vendors, etc) to effective communication, effective work practices, information sharing, etc.

4. **Inadequate Separation of Duties**

The primary reasons for this inadequacy are:

- Service offerings are the combination of one or more of the functions (in whole or parts) offered by different teams. Multiple personnel are associated in different capacities in the delivery of a single service unit – playing different roles in different hierarchies.
- In an effort to enhance the utilization of limited IT resources, personnel get assigned to multiple roles and/or functional teams (extra access privileges).
- In some situations, the technological attributes limit the capability to adhere to the Separation of Duties principles.

5. **Varied Interpretations of Security Requirements**

The security requirements are often defined at a high level and say “what” needs to be done but never state “how” the requirements should be met. It is left to the IT teams to appropriately interpret, define and implement/practice them. Being left open for interpretation, individual preferences and biases of IT Managers influence the interpretations resulting in inconsistent security practices/strategies both within and outside the SSO.

6. **Tendency to reduce Risk level**

In a Risk based approach, the organization defines different levels of security controls based on the level of risk; impact and likelihood of Disclosure, Modification and Loss of information. In such an approach, there is a tendency to assess the content (information) at lower levels of ‘Risk Exposure’ to reduce the rigor of the governing processes; to be able to bypass certain procedures, review gates and approval mechanisms.

7. **Multiple vendors**

The organization usually employs multiple vendors with the intent of reducing the risk of being over dependent on a single vendor, keeping prices competitive, service levels high and encouraging innovation.

But an outcome of this, which is often ignored, is the reduced collaboration between vendors, steeper barriers in communication (due to a sense of insecurity) and a marked reluctance to share responsibility (either you or me and never we).

8. **Business/Operations spread across multiple geographies**

In a global setup, it is always a challenge to have a complete understanding of all the local information protection policies, procedures and practices. Every country and state has their own requirements of certain regulations and the same policies may have different requirements in different regions.

Apart from the local laws and regulations, in a global setup issues come up due to the diversity in culture and thought process across geographies – Language issues, lack of context, lack of informal communication, etc. This makes it very difficult for an organization to co-ordinate the entire global roll-out and move forward in a planned manner.

9. **Lack of Training/Awareness**

The root cause analysis of security incidents showed that most of them were a result of unintended or unauthorized actions of legitimate users and not from malicious external sources. The primary causes for these lapses being

- Inadequate training on security practices and/or
- Misunderstanding instructions from the management

Summary: Information Security Challenges

Sl #	Challenge	Description
1	IT Security is assigned a low priority	The organization and senior management have not instilled the right focus on implementing IT security practices.
2	Ad hoc Security Governance	Absence of an Information Security Management System (ISMS) or a structured governance mechanism.
3	Ambiguity in roles and responsibilities	Ambiguities exist on the roles and responsibilities of the different players (Business, teams in SSO, etc.) in an SSO.
4	Inadequate Separation of Duties	Overlapping and shared responsibilities in an SSO makes it difficult to implement appropriate level of separation in duties.
5	Varied Interpretations of Security Requirements	In the absence of standard interpretations, the different individuals and teams have their own interpretations.
6	Tendency to reduce Risk level	The teams show a tendency to reduce the 'Risk Level' to bypass the rigors of the governing processes.
7	Multiple vendors	Relentless competition and sense of insecurity have led to reluctance in sharing responsibility and little or no collaboration among the vendors.
8	Business/Operations spread across multiple geographies	The organization is based out of and functions from multiple locations spread all across the globe.
9	Lack of Training/Awareness	Inadequate training and awareness on security practices.

Section II: Effective Best Practices in IT Security

In its recent engagements with large pharmaceutical organizations, Infosys was successful in negotiating most of the challenges listed above; either completely eliminating the issues or significantly reducing the severity of the issues.

Some of the 'Best Practices' employed in these efforts are listed and discussed below.

1. Information Security Governance

At the beginning of the engagement, IT Security was being managed and supported by make-shift ISOs who took this as an additional responsibility to their regular job responsibilities. People were assigned to this role on rotation and there was no continuity.

To address this, a full-time ISO was appointed and an ISO network was formed to manage requirements across multiple sites. The operations were based on the following principles:

- Adoption of a top-down approach
- Ensure that senior management commitment was sought and their help was taken in creating security awareness and promoting good security practices
- The scope was not limited to a few business critical systems – Entire organizational end to end processes were covered in scope.

2. Tailoring ISO 27001/27002 Control Requirements

ISO 27001/27002 outlines hundreds of potential controls and control mechanisms, trying to cover legislative essentials and common best practices and serving as the best starting point for any organization attempting to identify the control requirements. But how and to what extent the requirements need to be met are unique to every organization.

Hence, instead of using the ISO 27K controls AS-IS, Infosys conducted a due diligence exercise and undertook the following to tailor the requirements to suit the organization's needs.

- Risk Assessment – To assess the business processes and identify requirements which were to be met under all conditions
- Ensured alignment to the organization's official risk acceptance criteria
- Ensured that all applicable legal and regulatory requirements and corporate policies were met
- ISO 27K controls which were not mandated as per the three gating criteria mentioned above were promoted as

controls that at times can be dropped with suitable business justifications, adequate approvals or compensating controls.

3. Interpretations of all Control Requirements

As mentioned earlier, the control requirements are typically laid down at a high level and often do not specify how or what should be done to successfully meet them. So, to bring in consistency in the interpretation and implementation of controls, Infosys, as a central team, defined these for all the teams to adopt and practice.

Infosys brought together SMEs from all cross-sections and developed “discrete actionable guidelines” for each of the control requirement. With this Infosys was able to specify what and how the teams need to do to ensure compliance.

4. RACI Matrix for all Requirements

In a shared services model (offering infrastructure and/or application support), even after transition of applications to the SSO for IT support, business sponsors retain the ownership of the applications and the business processes (information content). This arrangement causes the accountability for individual controls to be split between the Business Sponsors and SSO. But the lack of specific guidelines results in all kinds of confusion and uncertainty in defining these.

To manage this situation and to draw clear boundaries, we created a Responsible, Accountable, Consulted, Informed (RACI) chart covering all the control requirements. This laid down the role of each individual/team towards the security control requirements.

5. Separation of Duties (SoD) Matrix

While creating the SoD Matrix, organizations often do not take into account the following:

- Limitation of a standard template: Often organizations commit an error when they try to adopt a standard template. Though the principles for defining the SoD are the same and universal, the SoD requirements have to be specific to an organization and its setup.
- Compensating Controls: Though implementing appropriate levels of Separation in duties is one of the better ways to implement checks and balances, it is not the only way. There can be other equally strong methods like – audit trails, oversight, etc.
- Technological Limitations: Some technologies, by nature don't/can't allow the implementation of sufficient layers of separation.

Hence while creating the SoD, Infosys factored in all of the above and created multiple variations of the SoD matrix suiting different types of services and processes. Infosys also took the next step in identifying compensating controls deemed adequate to substitute separation in certain special scenarios.

6. Create Lean Processes

The existing organization had processes but the primary focus and intent was on operational performance management and standardization. There was no focus on building the operational security controls into the process. And over a period of time with multiple modifications, the processes gained in complexity and at times became difficult to follow.

So, Infosys conducted a redefinition effort to

- Create 'lean' and 'fit for purpose' processes with all the required controls (covering all laws and regulations)
- Retain information showing “what and why required” in the parent document and transfer process content depicting “how to execute” to work instructions, guidelines, templates, etc as necessary and applicable

7. Training

A structured training enablement process was established which defined the training requirements for each role and for each topic/process area. Though the primary intent was compliance to security requirements, the scope of the training enablement process was extended to all aspects of IT operations and not just security.

Summary: Successful Best Practices

Sl #	Challenge	Best Practices	Benefits
1	IT Security is assigned the least priority	Information Security Governance – Adopted a top-down approach	<ul style="list-style-type: none"> Renewed focus on developing and supporting the Security Management System
2	Ad hoc Security Governance	Information Security Governance – Setup the ISO Network	<ul style="list-style-type: none"> Security strategies became an integral part of enterprise governance
3	Ambiguity in roles and responsibilities	Created a RACI chart to cover all security control requirements	<ul style="list-style-type: none"> Removed ambiguities in roles and responsibilities
4	Inadequate Separation of Duties	Created multiple variations of SoD matrix, while accounting for compensating controls and technological limitations	<ul style="list-style-type: none"> Made it easier to adopt and comply to the SoD principles Provided other equally efficient means to manage checks and balances Provided means to counter technological limitations
5	Varied Interpretations of Security Requirements	Process Re-definition to create 'lean' and 'fit for purpose' processes	<ul style="list-style-type: none"> All the security requirements were built into the processes and were not left open for individual interpretations
6	Tendency to reduce Risk level	Tailoring of ISO 27001 / 27002 Requirements	<ul style="list-style-type: none"> Provided the option to bypass controls which did not make business sense – cost wise Allowed the organization to drop requirements which were not applicable/meaningful to their operational setup
7	Multiple vendors	Creating and implementing appropriate RACI chart	<ul style="list-style-type: none"> Removed ambiguities in roles and responsibilities – Reduced avenues to blame 'others'
8	Business/Operations spread across multiple geographies	Established a structured training enablement process	<ul style="list-style-type: none"> Increased awareness and focus on local information protection policies, procedures and practices
9	Lack of Training/ Awareness	Established a structured training enablement process	<ul style="list-style-type: none"> Increased awareness on organizational mandates and requirements Better enablement for process compliance Reduction in repetition of mistakes/violations

About the Author

Binoy Kumar Singh

He is a Senior Project Manager with Infosys Limited and has 11 plus years of IT experience. He has been managing global enterprise projects and directing teams with multi-million dollar budget for Fortune 100 clients in Life Sciences, Insurance and Health-care domains. Recently, in one of the engagements with a major pharmaceutical client, he helped in defining and establishing the ISO Network, implementing and managing the Information Protection Program and developing ITIL aligned processes in Shared Service Model.



For more information, contact askus@infosys.com

About Infosys

Many of the world's most successful organizations rely on Infosys to deliver measurable business value. Infosys provides business consulting, technology, engineering and outsourcing services to help clients in over 30 countries build tomorrow's enterprise.

For more information about Infosys (NASDAQ:INFY), visit www.infosys.com.