2016 International Conference on Intelligent Manufacturing and Materials (ICIMM 2016)
ISBN: 978-1-60595-363-2

The Study on Information Integration Broker Controls

Chen Chen

ABSTRACT

The paper initiates a major project effort to the information integration technology general controls over business applications. It built up existing Company-wide systems, detailed procedures manuals and individual applications. The scope of the effort was global and encompassed all applications. The controls framework that could be adopted and modified as required by application owners who uses it to document the specific controls implemented by application and provide effective operation controls.

INTRODUCTION

Traditional security mechanisms cannot fully meet the present security requirements. so access control based on role is the key to Information integration and application integration involves with different services across multiple domains. The controls have been reviewed and revised to enhance enterprise's overall IT control environment while eliminating redundant, less effective and/or less important controls.

CONTROL CATEGORIES

The general controls has been developed in response to the perceived threats or risk, has organized controls around eight major control categories summarized in the

Chen Chen, Dalian Institute of Science and Technology, Liaoning, China

Table 1. Each category recognizes a number of control objectives and suggests specific controls aimed at addressing identified risks. Many controls are a combination of manual and automated processes. Each control should be designated as "Manual" or "Automated". As the probability of occurrence and the threat impact varies by application, so will the definition of controls for each application.

CONTROL STRUCTURE

User Access Administration Controls(UA)

The structure has implemented administrative, technical and physical controls to guard against unauthorized access. Basic internal controls require the separation of duties for "incompatible" system support functions. No single individual should be able to control key aspects of operations and thereby conducting unauthorized actions or gaining unauthorized access to assets or records. The detail description of UA controls are provided as following: (1)user access administration(e.g. authorizes and monitors Terminated Employees、New or Modified Employee、Non-Employee and Periodic Review Of User, eliminates Users, Update Rights); (2)System Access Control (e.g. guest accounts, Password Structure followed as Table II, Password Revisions, Inactive Terminal Sessions); (3) Security Maintenance; (4)Data Access.

TABLE I. CONTROL CATEGORIES.

Control Type	Control Category	Description
Application Controls	End User Access (UA)	Controls over user access to applications by end users. Many of these controls are designed to leverage other network access controls and delivered software functionality.
	Change Control Maintenance(CC)	Change controls define the processes that must be followed for making changes to the application or environment for break/fix and ongoing maintenance and enhancement efforts.
	Operations(OPS)	Most operational controls address a combination of operational effectiveness and internal control objectives.
	Major Implementation (SDLC Controls) (MI)	Controls over major development and implementation efforts including planning, executive level approvals, development, testing, user acceptance and implementation. SDLC controls apply to acquisition and implementation of new applications and/or major changes in the environment .
Operating System and Database Controls	Technical User Access(TA)	Controls over access to the Operating System and Database and application environments by technical support staff.
	Configuration Management(CM)	Controls over system and data access by technical personnel for performing system administration and management activities.
	Physical Access(PA)	Environmental and physical access controls governing access to the hosting facilities.
	System Software Implementation (SSI)	Controls over the configuration and maintenance of operating system software, database management systems and related middleware components.

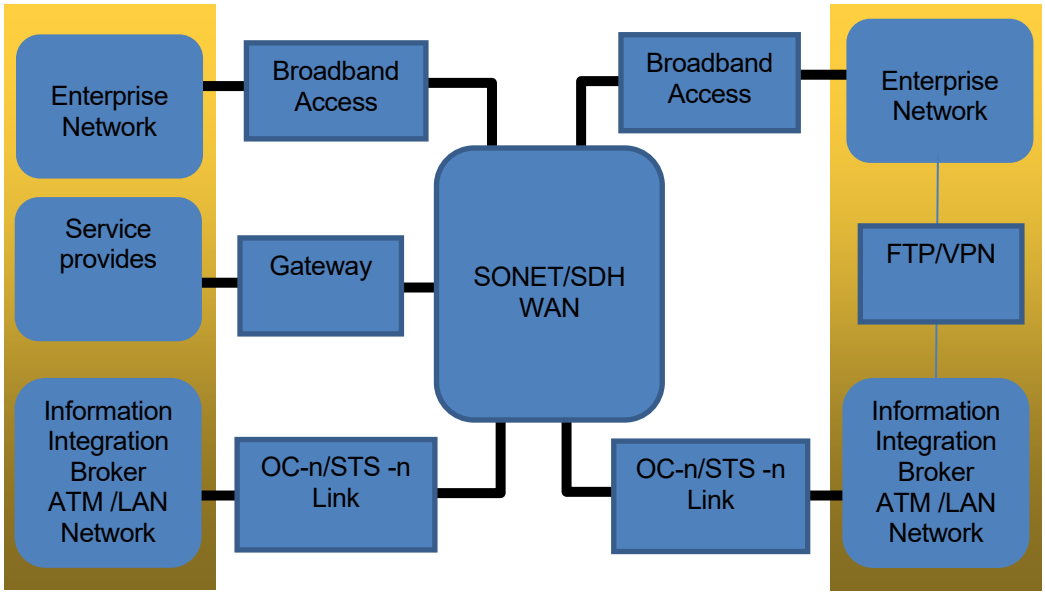

Figure 1. The Information Integration Network Controls.

Information Integration Network Controls

This service orchestrates data transfers between trading partners, exchanging data in a two sided synchronous, real time transactions. Transfers happen through the support team with the external partners by VPN or ftp. The process is illustrated in Figure 1.

Maintenance Change and Operations Control

These procedures include a review of all supporting documentation including the initial problem report, the nature of the corrective actions and the test results, ensure that all changes are properly authorized and adequately tested prior to being migrated to a production environment, maintain for future reference as required. The detail description are provided as following: (1) change Control Process; (2)initiate, assess, categorize, prioritize, approve or reject the Change Request; (3)ensure the resources only work on authorized changes; (4)interface Data and Code; (5)tracking software changes; (6)approve access to production data and files; (7)Program Migration and Version Control; (8)Back-up and Off-Site Storage; (9)Input/output Controls; (10)resolute Issue and Problem; (11)Schedule the Change and so on.

Configuration Management(CM) and System Software Controls

The Configuration Management controls focus on access to the environment through the network infrastructure and maintenance of the operating system and database, it also address the need for security software that further protects the business applications and underlying data. The detail description of CM are provided as following: (1) manage the Configuration; (2) change Vendor Default Passwords; (3) OS/DB Change Management; (4) Security Firewalls controls; (5) Encryption Algorithms; (6) System Monitoring Reports; (6) System Security Reports.

System Software Implementation refers to the processes supporting maintenance and operation of the underlying operating system and database management system supporting. Processes should be in place to monitor vendor supplied updates, patches, version upgrades and new releases of software. The controls should ensure that the application server, operating system, DBMS and support software are maintained at current levels to support current and planned new system functionality and ongoing operation. The detail description of controls are provided as following: (1) correct Security Weakness; (2) limit authorized personnel through the use of access control software; (3) support New System Functionality(ensure to support current application and software; keep and update planned new system functionality compatible with previous version and ongoing operation).

CONCLUSIONS

The net result is a "standard" set of control objectives that are generally applicable to all business applications. The standard set of IT general controls are organized in two parts: (1)The Applications controls should be addressed by all application owners in conjunction with the IT support staff for each application. (2)The OS/DB controls identifies IT control objectives pertaining to the environment and access to the underlying operating system, database and application environments. The OS/DB controls are normally developed for each data center or hosting site. Effective functioning of the IT general controls is essential to ensure proper functioning of the application and process controls. Many of these controls are performed by 3rd party hosting vendors as well as internal system administrators and technical support staff.

REFERENCES

1. Castro, L. Jackson, H. and Chang, M. 2007. "Scaling Down SOA to Small Businesses," presented at IEEE International Conference on SOCA, October 19 to 21, 2007.
2. Swartz, A. 2002. *A Semantic Web Services.* IEEE Intelligent Systems,76-77.