Sarbanes-Oxley Information Technology Compliance Audit

Dan Seider

Sarbanes-Oxley Information Technology Compliance Audit of an Outsourced Microsoft and SAP System for a Specialty Manufacturer

Auditing Networks Perimeters and Systems

Practical Assignment as partial completion of Requirements for GSNA Certification

Version 4.0

Option 2

Dan Seider
Las Vegas 2004

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY / ABSTRACT

This paper provides a basic review of the background literature (i.e. extensive but not exhaustive) and develops a process model so that a professional IT Auditor may readily appreciate the subtleties of the Sarbanes Oxley audit process. The case study is developed to illustrate some of the effects of the issues described in the literature and other issues developed in the process model.

The literature, process model and case study develop sufficient detail so a professional IT Auditor may readily modify and apply it to a new audit. Experience demonstrates that the focus of IT audits conducted under the mandate of Sarbanes Oxley and its IT Section, Section 404, has important differences with the focus of a traditional IT audit.

A traditional IT audit typically focuses on component, subsystem and sometimes on the system level auditable issues of the environment being audited with a strong bias towards security matters.

Sarbanes IT audits add an entire layer of governance, financial, and controls matters to the audit process. The literature documents that a Sarbanes IT audit would rarely delve deeper than the system level since the primary objective of the Sarbanes audit is to assure the CEO, CFO, and Audit Committee that the financial information that is in the IT systems and being reported to the SEC is accurate and reliable.

While both the traditional IT audit and the Sarbanes IT audit are technical IT audits, the differences in point of view of the primary objectives of the audit are an important difference. The Sarbanes IT audit has a narrowly defined focus that is driven by Federal Law and is a system level audit that concentrated on the reliability and integrity of the hardware, software and information of the systems. That is, Sarbanes is a System Level audit vs. a device level audit; in much the same manner that one might audit a system's entire perimeter rather than a single firewall.

A second point of view difference lies with the audit process owner. The financial audit community accurately believes that it owns the overall Sarbanes audit process, which the IT part of the audit, and the IT Auditor, for that matter, belongs to them, and works towards fulfilling their objectives. As a result, the Sarbanes IT audit is typically part of a larger financial audit and responds to the requirements of the larger financial audit

An additional is an apparent level of controversy that surrounds the Sarbanes process. Literature searches and research clearly points to some controversy on question of "when, where, and how" the law is applicable to some companies, which implanting standard and/or framework should be used, and conflicting opinion, without significant insight, into the "where the rubber meets the road" specific detail of doing an actual audit.

These factors lead directly to the structure and development of the material

presented in this paper. The introduction provides some basic structure, limits and introduces the companies of the case study.

The second section provides a extensive, although not exhaustive, review of the literature that bears on the development of a the details of the Sarbanes IT audit process. It notes that, for the Sarbanes IT Auditor, controls are the biggest issue. It also provides some insight into the regulatory and framework issues that materially affect these audits.

The third section provides a process model for implementing a Sarbanes IT audit. This map may be used by an IT auditor to successfully structure and implement a Sarbanes IT audit. However, an IT auditor using it should recognize that any process map may be open to considerable interpretation and debate.

Additionally, an IT auditor who chooses to use this map should also be sensitive to the fact that the author observed several factors that complicated implementation; some of them wll sound like re-occurring themes.. First, the governing standards are still "up in the air" which allows for different interpretations of these standards. Secondly, the "noise" level is increased because a number of organizations, including professional organizations, with different agendas, have contributed to the literature and discussions. Thirdly, the implementing organizations themselves are in competition with each other and they have their own internal practices that, naturally, they follow.

Section four is a case study and is drawn from a recently completed Sarbanes IT audit. It is included so that a professional IT Auditor may review the workpaper of an actual audit.

1.0 INTRODUCTION

The *Public Company Accounting Reform and Investor Protection Act of 2002* [1] (hereinafter called "SOX" or "Sarbanes-Oxley") has changed how all public and certain private companies do business. Sarbanes-Oxley is a large complex piece of Federal legislation that is now the law of the land.

An internal Sarbanes-Oxley audit was conducted on behalf of Octopus Corporation as preparation for the annual independent audit of the Corporation. The principals to the this audit are Octopus Corporation and GIAC Enterprises, both of whom are briefly described in paragraph 1.2 and 1.3 respectively. [2]

1.1 Scope

Internal and external audits traditionally focus on financial matters. Likewise, traditional IT audits focus on technology issues. In the past, these two audits rarely interacted with each other. The passage of Sarbanes-Oxley has, as it is said, changed everything.

Compliance with the provisions of Sarbanes-Oxley focuses the corporation's CEO, CFO, Board of Directors, and Audit Committee on producing the documentation to support their attestations that the corporation's financial and other information is reliable, verifiable and secure. While a Sarbanes audit also focuses on financial matters, it has an equally important focus; that of producing the documentation to support the attestations that the companies IT systems and the information they contain are reliable, verifiable and secure.

The principal Information Technology section of Sarbanes is Section 404 and this section is commonly referred to as "SOX-404." An IT auditor will quickly recognize that the SOX-404 audit has important differences when compared to the "traditional" IT audit.

- First, Controls be in place; Section 404 is designed to ensure that there are sufficient controls to prevent fraud, misuse and/or loss of financial data and transactions.
- Second, Controls must be effective; that there are controls to enable speedy detection if and when such problems happen, and that effective action is taken to limit the effects of such problems.
- Third, it must be possible to note exceptions caught by the controls and follow audit trails in order to take appropriate action in response to those exceptions, and
- Fourth, a SOX Section 404 audit is invariably part of a larger financial audit and is invariably influenced by it's being part of a larger financial and governance controls audit.

While this paper concentrates on the issues of implementing a Section 404 audit, other sections and material may be incorporated as appropriate so as to facilitate this discussion. Other "environmental" matters that set the SOX process apart from the traditional IT audit particularly governance and regulatory control factors are also included as appropriate.

1.2 Case Study Companies

This paper utilizes a Sarbanes Oxley Section 404 Information Technology audit conducted for the Octopus Corporation's European Division and its Octopus' European Outsourcer GIAC Enterprises. The workpaper presented in the case study in Section 4 are the sanitized versions of the actual audit, although because of length or space limitations representative samples are sometimes used.

1.2.1 Octopus Corporation

Octopus Corporation [2] is a leading international producer of agricultural chemical and other products. The company employs approximately 2,500 people in North America and Europe and is publicly traded.

The company enjoys sales revenues of about $1.85 Billion. Europe represents about $200 million or about eleven percent (11%) of the total revenues of the company. The markets for the company's products are mature, stable, growing slowly and characterized by relatively low margins for a manufacturing concern.

Octopus growth program projects growth benefits through increased sourcing of lower cost raw materials, expanded product sourcing and distribution capabilities, a stronger industrial market position and access to new markets. Octopus owns and operates manufacturing facilities in the United States, Canada, South America, and Europe. The company's manufacturing plants are strategically located to efficiently meet the needs of the United States, South America, and Europe.

1.2.2 GIAC Enterprises

GIAC Enterprises [2] is an IT services company and provider of technology consulting and integration services to Fortune 1000 companies. GIAC Enterprises (hereinafter GIACE) focuses on IT solutions that can optimize their client's process workflows, implement the business systems that support them and managing those systems for peak operation. GIACE is headquartered in the European Union (EU).

In the EU, GIAC Enterprises is a major provider of outsource IT services emphasizing a full service, full lifecycle, "design, build and operate" approach. Particular attention is focused on Systems Integration, and Managed Operations. As can be seen with other EU companies, GIACE's management provides reluctant support for SOX process [3, 4, 5] particularly since GIACE's data center has been certified as a BS-7799 facility. [6]

2.0 BACKGROUND

Sarbanes-Oxley has changed how all public and certain private companies do business. The broad range of governance, control and reporting matters addressed by SOX can be seen by a simple review of the section headings of the Act; and provided in Appendix A, "Summary of Section Titles of Sarbanes-Oxley Act." [7]

2.1 Impact of Sarbanes-Oxley on IT Audits

Sarbanes-Oxley impact on IT organizations, operations, processes, security, etc. is far reaching, evolving, and here to stay. [8, 9, 10] For the IT auditor, the impact of Sarbanes falls firmly into assuring internal control, quality, and integrity of information generated by IT systems and assuring that the IT systems comply with the legal and regulatory requirements

2.1.1 General Purpose of Sarbanes-Oxley Section 404 Audit

The general purpose of a Sarbanes-Oxley Section 404 Audit is to identify weaknesses or deficiencies in the IT controls and resolves them prior to the start of an outside audit. Section 404, in part,

> Requires each annual report of an issuer to contain an "internal control report", which shall:
>
> (1) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and
>
> (2) contain an assessment, as of the end of the issuer's fiscal year, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.
>
> Each issuer's auditor shall attest to, and report on, the assessment made by the management of the issuer. [11]

In this usage, the SEC refers to an "issuer" as a company that has issued stock and become a public company under its jurisdiction.

2.1.2 Controls Focus

Section 404 of Sarbanes-Oxley requires public companies to adopt and maintain a controls focus. Internal controls are the practices, transactions, procedures and processes used to control the company's' financial transactions and protecting a company's property and assets. This includes, for example, controls that verify that that the financial-reporting systems have the proper controls, such as ensuring that revenue is recognized correctly.

It is the IT Auditor who verifies that the controls are in place and working

correctly because Sarbanes-Section 404 recognizes IT as a significant participant in the controls process because today, in but the smallest of companies, the financial information upon which the CEO and CFO will attest under other sections of SOX, is processed and stored in the IT systems. If the security or integrity of the IT system can be compromised, then the information in them can be compromised.

While the government dictates that companies must perform these internal controls audits and that CEO's and CFO's must attest to their accountant's findings, the standard by which the company's are to audit their books has not yet been approved. This leads to uncertainty as to which standard should be applied and how any or all standards should be interpreted.

2.1.3 Industry Frameworks

The implementation of SOX has met with and generated a significant quantity of competing opinions and advice as to the correct way to conduct a SOX audit. Virtually every audit or accounting standards organization has stated that if an IT system is integral to, or a significant part of the operations being audited, the audit should include the system so as to provide reasonable assurance that the information produced by the system is accurate, reliable, and complete.

These organizations include the: American Institute of Certified Public Accountants (AICPA) [12, 13, 14, 15, 16, 17], Institute of Internal Auditors Association (IIA) [18] U.S. General Accounting Office (GAO) [19], Information Systems Audit and Control Association (ISACA) [20] and its affiliated IT Governance Institute (ITGI), U.S. Public Company Accounting Oversight Board (PCAOB), [21] and Institute of Internal Auditors Research Foundation (IIARF). [22] These organizations campaign for their respective points of view in their respective professional journals. Table 2-1, Industry Framework Organizations and Key Publications, provides a listing of some of the key publications of these organizations.

A cursory review of these journals shows that all of them offer advice on SOX matters. However, two leading frameworks have emerged as being important to the IT Auditor contemplating a SOX audit. They are the COSO Framework and COBIT Framework. Other standards are also influencing the promulgation of a uniform standard of the conduct of SOX audits.

Organization	Publication
American Institute of Certified Public Accountants (AICPA)	*Statements on Auditing Standards* (SAS)
Institute of Internal Auditors Association (IIA)	*Standards for the Professional Practice of Internal Auditing* (IIA)
U.S. General Accounting Office (GAO)	*Government Auditing Standards* and *Title 2*, *Accounting* (GAO)

Information Systems Audit and Control Association (ISACA)	*General Standards for Information Systems Auditors* and *Statements on Information Systems Auditing Standards*
Institute of Internal Auditors Research Foundation	Systems Auditability and Control (SAC)

Table 2-1 - Comparison Industry Framework Organizations and Key Publications

2.1.3.1 The COSO Framework

In general, COSO [23] *Internal Control – Integrated Framework (Control Framework)* has been accepted as the internal control standard for organizations implementing and evaluating internal controls in compliance with both SOX and PCAOB Standard 2. [21] The COSO framework addresses how control risks should be identified within processes and the control methods to mitigate these risks. It refers to manual controls and automated controls and how the latter need to be supported by appropriate General Computer Controls.

The COSO framework is also generally recognized as the Securities and Exchange Commission's (SEC) *de facto* standard although it is not yet the *de jour* standard. As a result, most companies are using it to comply with SOX's legal requirements. The framework also states that the company must: have objectives and know how they are performing against them, describe what they would do if they didn't meet their defined requirements, and require that employees to be qualified and trained.

In most companies of any size, data moves between multiple business groups and between multiple IT systems on its way from initial transactions to the reports that the CEO and CFO must attest to. Attesting to the accuracy of these data requires confidence in all of the accounting and other procedures and controls.

Likewise, the SOX attestation that the CEO and CFO must attest to also requires confidence in the IT systems that house, move, and transform the data. This requires confidence in the processes and controls for those IT systems and databases. The importance of IT controls is embedded in the SEC-endorsed framework developed by the COSO.

2.1.3.2. The COBIT Framework

Numerous observers have pointed out that COSO doesn't do enough to help identify, document, and evaluate the IT controls necessary to comply with SOX's legal requirements. The "Control Objectives for Information and Related Technology," or COBIT framework was designed to address the IT concerns observed in COSO.

COBIT is an interpretation of COSO from an IT point of view, was established by the IT Governance Institute (ITGI), [24] In an important report, "IT Control Objectives for Sarbanes-Oxley," [25] ITGI, specifically proposes that a company's first priority should

be demonstrating that strong IT controls over financial reporting are in place [26] and that COBIT is a robust framework, comprising four domains, 34 IT processes and 318 detailed control objectives. It is a comprehensive approach for managing risk and control of information technology. [27] COBIT is may be adopted by many corporations as a guide for their IT related Sarbanes-Oxley compliance efforts.

2.1.3.3 Other Frameworks and Standards

Several other standards bodies are important "players" in this arena. Chief among them are the International Organization for Standardization, and the National Institute of Standards and Technology.

The National Institute of Standards and Technology, or NIST, is a non-regulatory federal agency within the U.S. Commerce Department's Technology Administration. NIST's Computer Security Division (CSD) seeks to improve IT systems security by developing standards, metrics, tests and validation programs and publications (e.g. Federal Information Processing Standards Publications (FIPS PUBS). [28]

The International Organization for Standardization, or ISO, is a voluntary, international, non-governmental organization that seeks to coordinate the international unification of industrial standards. It is the ISO17799 standard, its predecessor BS7799, and the formal certification and accreditation of systems under these standards that is of particular interest in the SOX process. It is "*a comprehensive set of controls comprising best practices in information security*". [29] It is essentially, in part (extended), an internationally recognized generic information security standard." [30]

COSO's Enterprise Risk Management (ERM) — Integrated Framework describes the elements of a enterprise risk management process. It describes how all important risks should be identified, assessed, responded to and controlled. Enterprise risk management is a new and evolving framework that can be expected to impact SOX-404 audits in the future. Appendix B provides a listing of the components of ERM.

2.1.3.4 Mapping the Frameworks and Standards

COSO may be the *de facto* Framework but its unofficial status allows other frameworks and/or standards to be adopted in SOX-404 processes. As already noted, further complications occur as a result of COSO's vagueness on IT matters, the blurred lines separating which internal controls are relevant to the audit and what needs to be tested and how.

Procedures on which IT systems should be included in an audit also appear to differ according to the kind of company being audited. That is, it is reasonable to expect the validation tests for a company in which the firm is the IT systems (e.g. a application hosting business) will be different from the tests applied to a company in which the IT systems only do back office tasks.

The generally accepted approach is to use, when applicable, a combination of COSO and COBIT to create a comprehensive framework for evaluating the risk and security of IT systems. Other standards, (e.g. ISO-17799) may also be introduced to assist in the tailoring process. This intent may be seen in the following excerpt from *IT Control Objectives for Sarbanes Oxley*.

> *On 9 March 2004, the US Public Company Accounting Oversight Board (PCAOB) approved PCAOB Auditing Standard No. 2, titled "An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements." This audit standard establishes the requirements for performing an audit of internal control over financial reporting and provides some important directions on the scope and approach required of auditors.*
>
> *The PCAOB standard includes specific requirements for auditors to understand the flow of transactions, including how transactions are initiated, authorized, recorded, processed and reported. Such transactions' flows commonly involve the use of application systems for automating processes and supporting high volume and complex transaction processing. The reliability of these application systems is in turn reliant upon various IT support systems, including networks, databases, operating systems and more. Collectively, they define the IT systems that are involved in the financial reporting process and, as a result, should be considered in the design and evaluation of internal control.*
>
> *The PCAOB suggests that these IT controls have a pervasive effect on the achievement of many control objectives. They also provide guidance on the controls that should be considered in evaluating an organization's internal control, including program development, program changes, computer operations, and access to programs and data. While general in nature, these PCAOB principles provide direction on where SEC registrants likely should focus their efforts to determine whether specific IT controls over transactions are properly designed and operating effectively.* [31]

Other mappings illustrate both the differences between the various standards and the degree to which they build upon one another. An excerpted table from ISACA's article "A Comparison of Internal Controls …" illustrates this point and is provides as Table 2-2 - A Comparison of Internal Controls.

2.1.4 Exclusions of Independent Auditors

Under the provisions of Sarbanes-Oxley, the external (i.e. independent) auditors are prohibited from being involved in the details of the internal audit that they will later check and attest to. Under the provisions of SOX, it's the company's general management's responsibility to ensure that the financial documentation and processes are in place before the independent auditor appears onsite to carry out the attestation review. The purpose of this review is to reduce the chances of signs that a "material weakness" will be reported in the management letter.

	COBIT	COSO	SAC	SAS
Primary Audience	Management, users, information system auditors	Management	Internal Auditors	External Auditors
IC viewed as a	Set of processes including policies, procedures, practices, and organizational structures	Process	Set of processes, subsystems, and people	Process
IC Objectives organizational	Effective & efficient operations Confidentiality, Integrity and availability of information Reliable financial reporting Compliance with laws & regs	Effective & efficient operations Reliable financial reporting Compliance with laws & regs	Effective & efficient operations Reliable financial reporting Compliance with laws & regs	Reliable financial reporting Effective & efficient operations Compliance with laws & regs
Components or Domains	Domains: Planning and organization Acquisition and implementation Delivery and support Monitoring	Components: Control Environment Risk Management Control Activities Information & Communication Monitoring	Components: Control Environment Manual & Automated Systems Control Procedures	Components: Control Environment Risk Assessment Control Activities Information & Communication Monitoring
Focus	Information Technology	Overall Entity	Information Technology	Financial Statement
IC Effectiveness Evaluated	For a period of time	At a point in time	For a period of time	For a period of time
Responsibility for IC System	Management	Management	Management	Management

Table 2-2 - Comparison of Internal Controls

Furthermore, under Section-404, it's the company's IT management that is typically responsible for ensuring that the IT documentation and processes are in place *before* the independent auditor appears onsite. IT management should have found all the issues and be working actively on remediation of those issues so that when the independent auditor arrives, ideally any issues will have either been resolved or are well on the way to being resolved so that the external auditors remain independent.

2.2 Third Party Providers

If the services of a third party provider, such as an IT outsourcer, is deemed "significant," then Sarbanes-Oxley requires these companies to maintain the same level of internal controls as the "parent" company.

Therefore, an IT Auditor should expect to implement a full SOX-404 audit at the service provider company that includes all relevant internal controls, documentation of processes and procedures, and all other SOX-404 audit requirements.

To make these assertions, a company's management must identify the controls and have a basis for the assertions; and this usually involves performing testing. A service company can chose a specific report provided the supported company or it may chose a SAS 70 report. The Statement of Auditing Standards (SAS) number 70, Service Organizations, is an auditing standard developed by the American Institute of Certified Public Accountants, whose purpose is to enable an auditor to evaluate and issue an opinion on the controls that a service organization has in place.

The output of a SAS-70 analysis is the Service Auditor's Report and it contains the auditor's opinion, a description of the controls in place. If it is a Type II analysis/report, a description of the auditor's tests of control effectiveness is included. If it is a Type I analysis/report does not include the testing.

Regardless of the form or mechanism, however, a third-party service provider who provides a significant level of service to another company must meet the same requirements of the reporting company. This provision can be expected to apply to all first tier outsourcer service providers.

3.0 AUDIT PROCESS

This section provides a generalized process model of a SOX audit and is illustrated in Figure 3-1, Sarbanes Oxley Section-404 Audit Process as a Heuristic. Heuristics are general rules of thumb or principals that are applicable to problem solving in situations where algorithms (i.e. formal or rigorous procedures) cannot be applied for reasons of economy or inherent difficulties. They are designed to fit specific problems and are based on a common characteristic such as seeking a solution that is "good enough." The advantage of this approach is that it can handle problems that can not be solved by classical mathematical or statistical techniques.

The process model developed in this section is a heuristic because the business issues of cost, time and sufficiency are constant constraints. Most companies' management, therefore, will seek a solution that is "good enough" to meet the legal requirement of Sarbanes Oxley. This typically means that management will verify that adequate control documentation and processes are in place prior to the outside auditor's attestation review.

Likewise, a proactive IT management approach to Section 404 should seek to find all the IT issues and be working actively on remediation of those issues prior to the arrival of the outside auditor, and ideally, have most issues either resolved or well on the way to being resolved since this outcome reduces the chance of a "material weakness" being reported in the auditor's management letter. The process model developed here presents such an approach. This process model is then tailored for use in Section 4, the Case Study.

3.1 Preparation

The review of the literature described in Section 2 indicates and generally acknowledges that preparation tasks are some of the most important tasks that should precede a SOX audit in general and a SOX-404 Audit in particular. In this regard, a SOX audit is very similar to any other IT audit. Audit Preparation resolves the macro issues that the auditor may encounter during the conduct of the audit. Important tasks in this phase include:

- scoping of the audit,
- tailoring the regulatory factors that the audit is responding to,
- defining the business environmental factors, and
- establishing a project management activity to "own" and implement the audit.

3.1.1 Audit Scope

Proper scoping is a constant and re-occurring theme in all IT audits, including SOX-404. The most important reasons include cost control and responsiveness to the specifics of the individual company's issues in the form of regulatory tailoring. Cost is an issue because SOX audits can be very expensive.

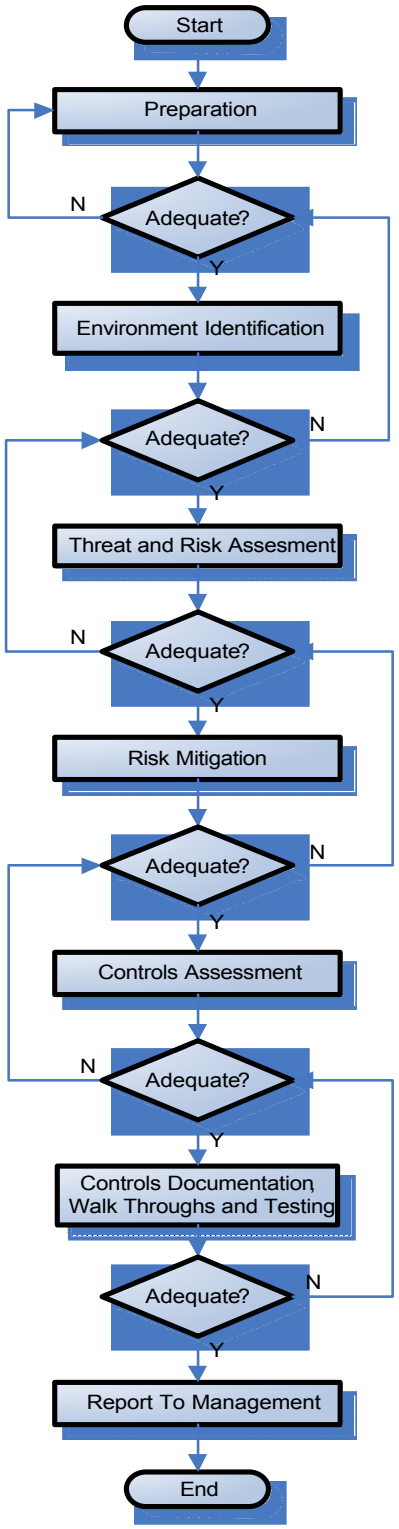


Figure 3-1 Sarbanes Oxley Section-404 Audit Process as a Heuristic

As a result, most companies want to minimize the cost doing no more than the specifics of the regulations call for. While a sound business case may be made for both the COBIT and COSO frameworks, many executive remain unconvinced. As with other types of IT and Security audits, the auditor may find it necessary to add cost-benefit education and business case ROI education to his task list in order to gain the full support of management.

The IT auditor should also actively participate in the tasks of interpreting the SOX requirements and deciding which IT systems are in the scope of the audit. She should additionally make sure that decisions about scope are documented and clearly communicated to everyone on the project.

3.1.2 Regulatory Tailoring

Sarbanes Oxley Section-404 has specific Securities and Exchange Commission (SEC) legal compliance and reporting requirements. The legal implications inherent in SOX, particularly the reporting requirements imposed on the CEO, CFO and Audit Committee argues that regulatory tailoring be implemented as a separate task. Additionally, a SOX-404 compliance plan should be in place prior to the start of the audit and be maintained by interested key participants.

The CFO must document identified risks facing the business, so the CFO should be a participant in the Section 404 tailoring process, particularly since a significant percentage of all company risks are risks to the IT systems. Since the Information Technology executive (e.g. CIO) will also be required to attest to the reliability and integrity of the company's information systems, data stores, and internal controls, he, too, should be a participant. The IT Auditor should validate the compliance plan that addresses IT controls and integrates them into the overall company compliance plan.

The review of the literature developed in Section 2 shows that the debate over "which framework" and "how much" of any given framework is not resolved. The IT auditor should be prepared to advise and. perhaps educate the company's executives on which aspects of COBIT and COSO are best suited for use and then carry these recommendations forward to the independent auditors for their concurrence. This concurrence, communicated to all participants, produces the agreed framework for the audit.

3.1.3 Project Organization

A SOX Audit in all but the smallest public company would, almost certainly, require the services of a Project Management activity or office. This need is well understood by the large CPA firms that conduct Sarbanes Audits. It is mentioned here as a reminder to the IT Auditor because Section-404 is only one part of the total Sarbanes requirement, as can be seen in the section listing provided in Appendix A. While a "standard" project model is an excellent implementation methodology, any discussion beyond noting that a project activity is, almost certainly, a requirement, is

outside of the scope of this paper.

3.2 Environment Identification

Identifying the auditable environment is a critical part of the overall audit process because it draws the line between the "macro, outside of the environment" (e.g. regulatory) issues of the audit and the "micro, inside of the environment" issues. For the IT Auditor, system Identification for a SOX audit has important differences with that of a traditional IT audit. The most important differences include:

- the system point of view of the audit (vs. a any individual component),
- the focus on controls,
- adherence to specific audit related frameworks,
- provisions for third party providers, and
- specific exclusion of the Independent Auditors from the process.

3.2.1 Organizational Structure

The organization chart of the participating company(s) is developed in sufficient detail to expose any control issues. This is documented by an organization chart with reporting lines, as illustrated in Figure 3-2 - Example Organization Chart along with the appropriate organizational charters that define the roles and responsibilities.

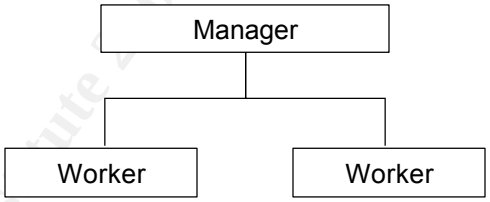


Figure 3-2 Example Organization Chart

A key control issue audited and documented at this phase of the Audit Process is the separation (or segregation) of duties or responsibilities. A matrix for each significant function (e.g. HR, Sales, etc.) of the organization (as illustrated in Table 3-1) is developed to document this separation of duties. The organization chart and segregation matrix usually provide sufficient documentation and they are included in the overall set of audit workpapers.

PROCESS Sub-Process	Authorization	Custody of assets	Recording	Control activity

Table 3-1. Example Segregation of Duties Matrix

3.2.2 System Environment

The IT Auditor defines the system environment in sufficient detail to identify any control issues that may be relevant to the SOX-404 process in the perimeter defense and/or in the key areas of Operations, Physical Security, Logical Access, Applications and Back-Up and Recovery. A system diagram or map, as illustrated in Figure 3-3, Example System Diagram, typically provides sufficient documentation and it is included in the overall set of audit workpapers.

Figure 3-3. - Example System Diagram

3.3 Threat and Risk Assessment

A "Threat," as defined by Webster is "An expression of intention to do injury or damage" and a "Risk" is defined as "the possibility of loss or injury." Threats beget risks and exploit "Vulnerabilities;" which are defined as "open to attack or damage" [33]

A company's response to the sum of all threats, risks, and vulnerabilities (Total Risk), how much risk is tolerable (Risk Appetite) and what level of response is reasonable is highly dependent on the specific situation. This seemingly obvious statement is at the heart of the entire subject area that is alternatively called "Risk Assessment" or more recently, "Risk Management." Consider the following simple situational example which illustrates some of the terms of this section in a situational context.

- A farmer owns and keeps a prosperous farm in Kansas. Since his farm is in Kansas, it is in "Tornado Alley" (Threat) and may be damaged or destroyed (Impact or Harm) by one of these storms (Vulnerability). He also knows that the probability of a tornado coming his way is small (Probability of Occurrence). Farming provides a good livelihood, so he doesn't move away. He also knows nothing can be done to stop a tornado. (Risk Appetite/ Risk Tolerance)

- The farmer responds to this threat by building a storm cellar so that he and his family will have a shelter if a tornado does come his way (Risk Mitigation). He also recognizes that some or the entire farm may suffer damage but he is still willing to continue farming in Kansas as there are no other threats. (Total Risk).

As with the farmer, the IT Auditor should be aware of his company's IT threats, vulnerabilities and consequentially system risks.

A Risk to an information system is the measured hazard that can be caused by a threat and that will, in some way, cause harm or reduce the operational utility of either the information system itself or the information contained within the system. It is a measure of the probability that an event will occur and the amount of damage that event has the potential to cause

It is the company's threat, vulnerability, risk conditions, and environment that drives the creation of the SOX-404 controls which, in turn, are tested to measure the accuracy and reliability of the IT systems. The IT Auditor should be able to review risk matters as a prelude to reviewing the details of SOX controls

To summarize, the IT Auditor should also recognize that threat, vulnerability and risk analyses have the goal of risk mitigation and security and that the audit should address and answer the following questions:

- Threats what could harm an IT system, its processing environment, or information?
- Vulnerabilities – what are the gaps between current processes and the standards and specifications for administrative, physical, and technical safeguards?
- Impact or Harm – what is the impact or harm on an organization's assets or ability to operate if a threat should exploit a vulnerability?
- Probability of Occurrence – what is the likelihood that a threat will exploit a gap?
- Risk Appetite/ Tolerance - what amount of risk is an organization is willing to accept?
- Residual Risk– what amount of risk that can never be completely eliminated?
- Total Risk – what is the sum of all possible risk exposures?

These details underling these questions are expanded upon in the following sections.

3.3.1 Threats

Threats to an information system are:

- events that may occur to the system being audited, and
- that are independent of the system being audited.

While there is a broad spectrum of possible threats, most general business corporations are susceptible to a limited and well understood set of threats. These threats are listed in Table 3-2 - Common IT Threats.

Threats	Description
Abuse of Access Privileges by an Otherwise Authorized User	An authorized user - whether an employee, contractor, etc. - may attempt to perform operations that are unauthorized to perform or otherwise is denied to them.
Abuse of Access Privileges by Employees	Acts by employees who are authorized by the Security Policy to perform certain functions on the system but then attempt to perform operations that they are not authorized to perform.
Accidental Errors	Improper use of information technology due to mistaken incorrect use rather than malicious intent.

Attempted Unauthorized Access by Outsider	Non-employees or personnel not who are contracted or authorized to access the system and are attempting or gaining access to the system.
Communication Loss	The inability to transfer information to and from the organization through the defined system parameter.
Computer Virus	A Program which spreads by attaching itself to "healthy" programs. After infection, the program may perform a variety of non-desirable functions.
Data Integrity Loss	A realized, or perceived possible, alteration of the data and/or information maintained by or consisting of the specified asset.
Deliberate Attack	This would include Hackers, Crackers, “Hacktavists,” Industrial or Corporate Spies, Organized Crime, and Terrorists
Destruction of Data	The damaging or preventing the use of information held by an organization and includes data used by the systems to operate, applications, manuals, and any other data store.
Fire	This includes both major fires that destroy resources to those which prevent assets from being used for any reason.
Natural Disasters	Those occurrences which degrade some aspect of the system other than fire and earthquake and are not manmade. Examples would be flooding, a tornado, a near or even distant earthquake
Non-disaster downtime	When the system is unavailable for use and not caused by disaster; this includes maintenance, component failure and system 'crashing'.
Power Loss	The loss of the electrical power supply to the systems.
Theft or Destruction of Computing Resource	The unauthorized use or damaging of the computing capability by anyone through physical or other means.
Successful Unauthorized Access by Outsider	Non-employees and non-contractors using, and possibly destroying, information system resources. "Hackers" fit within this threat description.

Table 3-2. - Common IT Threats

Table 3-2 does not include systems that handle national security data since these threats and risks represent unique challenges that the typical business system does not deal with and are therefore beyond the scope of this paper.

3.3.2 Vulnerability

Vulnerability commonly refers to a weakness or exposure that a threat can take advantage of or otherwise exploit. This weakness or absence of security controls may be the result of procedural, physical, programming or technical deficiencies. Vulnerabilities increase risk because they may provide a path for a threat to harm the system.

The IT Auditor should be prepared to examine the systems vulnerabilities both in terms of deliberate attack (e.g. a hacker) or an opportunistic attack (e.g. an otherwise honest employee who might be tempted when he sees an account password on a post-it note in the side of the computer).

3.3.3 Impact and Harm

The impact or harm may be derived by identifying the dollar value of the asset(s) that is subject to damage or destruction. Impact or harm needs to consider any asset that may be damaged. Assets include tangibles such as hardware and software and

other physical items such as buildings. Assets also include intangibles such as information, intellectual property and company good will. A simplified analysis may use:

$$[\text{Impact}] = [\text{Probability of Occurrence } (\omega)] \cdot [\text{Cost of Harm}]$$

Impact also refers to the overall, aggregate harm that occurs in the near term and in the long term. These may include disclosure, modification, destruction of information, lost business, denial of service, failure to perform the system's mission, loss of reputation, violation of privacy, and even loss of life. As a result of these possibilities, the IT Auditor may wish to consider a more robust analysis of the expected impact if multiple outcomes are available. [34, 35, 36] Hence, the Expected value, $\mathbf{E}$ for the $\mathbf{i^{th}}$ action is:

$$E(a_i) = \sum_j V(\Theta_{ij})\, p_j$$

Where:

a_i = $\mathbf{i^{th}}$ alternative course of action (i = 1, 2,…n)
s_j = $\mathbf{j^{th}}$ = possible future (j = 1, 2,…m)
$\bullet_{ij}$ = Outcome resulting from selecting action $\mathbf{a_i}$ when the future turns out to be $\mathbf{s_j}$
$V(\Theta_{ij})$ = Value of outcome $\bullet_{ij}$
p_j = Probability that future $\mathbf{s_j}$ will occur

The IT Auditor should be prepared to examine the system both in terms of impact and cost, keeping in mind, that the more severe the consequences of a threat, the greater the risk to the system and the organization.

3.3.4 Probability of Occurrence

Probability theory describes two conditions under which decisions are made based on the completeness of the information available to the decision maker. These are: Decisions under Risk and Decisions under Uncertainty. A decision under risk is when all of the possible outcomes are known and the probability of any one outcome can be stated. The only question is which outcome will occur. A coin toss is a classic example of decision making under risk.

A decision under uncertainty occurs when all of the possible outcomes may or may not be known and the probability of any one outcome can not be stated. As a result, the simplifying assumption of a "Decisions under Assumed Certainty" is commonly used. A common manifestation of this assumption is to ascribe a small number of possible outcomes, (e.g. "Low-Medium-High") as the probability of occurrence (ω) to an event.

The IT Auditor should recognize whether this simplifying assumption has been made in the first place and whether the assumptions are reasonable. Using assumed certainty is commonly accepted when the difficulty or cost of collecting risk data is

prohibitive or when the choice would still only depend on average values of the outcomes.

3.3.5 Risk Appetite

Risk appetite is the amount of risk that an organization is willing to accept. Measurement of risk appetite may be measured in quantitative or qualitative terms (e.g. "x" dollars of earnings at risk vs. reputation risk). The IT Auditor should be aware of or make herself aware of his company's risk appetite. The auditor should also incorporate her findings into the workpapers so that these conclusions can be documented and reviewed by management.

3.3.6 Residual Risk

Good general IT practice and IT security practice recognizes that there will always be risk and it can never be completely eliminated. This "left over" risk commonly referred to as residual risk. Good IT security practice indicates that the implementation of appropriate and reasonable safeguards to protect the confidentiality, integrity and availability of both the information and systems can mitigate the total risk of the system and that a functional relationship can be defined. In other words, residual risk equals total risk minus risk that is mitigated by a function of the standards effectiveness. Procedures or security mechanisms may be reasonable substitutes, and Residual Risk could be expressed as:

$$(\text{Residual Risk}) = (\text{Total Risk}) - f(\text{Standards Effectiveness})$$

Residual risk can be used as a validation test of risk appetite by appetite since it should be roughly equivalent to the reciprocal value of Risk Appetite. That is, if risk appetite is "high" then the residual risk should be expected to be fairly low. The IT Auditor should consider developing the risk appetite and residual risk values independently of each other so that they can be used to validate the other value.

3.3.7 Total Risk

The Total Risk that an organization faces may also be viewed as being the sum of all possible events, weighted by their probability of occurrence (ω) of each Event (E) and for some number of events $(_n)$, and multiplied by their impact (most commonly measured in cost or opportunity cost). A more explicit value for Total Risk may be derived as follows:

$$(\text{Total Risk}) = \Sigma_{n=1} (\omega E)_n (\text{Impact})_n$$

3.3.8 Risk Synthesis

Risk synthesis rank orders the list of risks so that mitigating controls may be implemented. Rank ordering is also useful in the allocation of scarce resources. For

example, an identified risk may be within the range of acceptable risk (i.e. risk tolerance) and therefore, ignored.

There are a variety of ways that this synthesis may be organized. The IT Auditor's review of this process should keep the criteria of consistency and accuracy in the forefront of the review. Consistency, in this case, means that all areas of the company use the same metrics and definitions in exactly the same manner. Accuracy means that the data is valid (true). As has been noted in the discussion of probability, simplifying assumptions, such as "Decisions under Assumed Certainty" may be reasonable and acceptable as long as they are explicitly documented.

One presentation of the synthesis data is illustrated by the simple matrix in Table 3-3 – "Risk Control Matrix - Development of Adequate Controls." Here, the values of "low," "medium" and "high" on each axis allows for the consistent mapping the probability and impact of each risk. The cells of the matrix provide the need for the development of adequate controls.

INDIVIDUAL RISK FACTOR		Amount of Loss/Risk		
		High	Medium	Low
Risk Likelihood	Most likely	Very Strong	Strong	Individual Case Decision
	Likely	Very Strong	Strong	Individual Case Decision
	Unlikely	Individual Case Decision	Individual Case Decision	None

Table 3-3 - Risk Control Matrix - Development of Adequate Controls

Table 3-4 - Risk –Payoff Matrix, provides a somewhat different approach to the risk synthesis process by including a benefit (payoff) factor and a cost factor. Inclusion of cost and benefit factors is a well established technique. [37]

FACTOR	RISK	COST	PAYOFF	NEED
Risk Factor 1	**L**	**M**	**H**	**L**
- - -				
Risk Factor n	**H**	**L**	**M**	**M**

Table 3-4 - Risk –Payoff Matrix

The IT Auditor conducting a SOX-404 audit is particularly interested in identifying and documenting the flow thread that starts with an identified threat to the control which will mitigate the risk of the threat. These tables are intendeds to aid the auditor's identification and documentation.

3.4 Risk Mitigation

Information risk mitigation in the form of risk assessment and risk monitoring is becoming a significant priority for inclusion in the SOX process. New legislation and best practices first established under BS-7799 and currently under ISO-17799 point to information Risk Mitigation as a critical element of any program designed to safeguard information assets.

While the emphasis for the SOX-404 auditor is on controls, achieving a reasonable level of assurance also requires security process that should be reviewed. These security processes include:

- Initial and on-going risk analysis and threat assessment
- Enterprise security management process
- Computer security (includes monitoring)
- Communications security (includes monitoring)
- Physical security: access to premises, equipment, people, data
- Personnel security
- Procedural (business process) security
- A pervasive security culture

The IT Auditor should also recognize that some IT risk mitigation decisions may have been made prior to the start of the SOX-404 audit and become *de facto* elements of the audit.

Since the current emphasis on control in Sarbanes-Oxley is primarily focused on internal controls over financial reporting and the generally accepted COSO framework likewise has this focus; this focus is changing. This change is the migration to COSO's *Enterprise Risk Management – Integrated Framework* [38], which is broader than internal control, and actually incorporates the key concepts set out in COSO's earlier *Internal Control – Integrated Framework.* [39] This new framework will significantly affect future SOX-404 and IT audits

The IT Auditor should appreciate that the enterprise risk-management framework goes beyond the internal control framework by addressing non-financial risks. The internal control framework is, for example, intended to ensure the reliability of published financial statements. The enterprise risk framework is intended to ensure the reliability of all internal and external reports, including regulatory filings. The framework also adds the concept of setting strategic objectives based on a company's appetite for risk, which governs all major business decisions.

The evolving COSO frameworks directly impacts the IT Auditor because IT management is typically charged with the responsibility of assuring the availability and timeliness of information. The framework also defines two categories of information systems controls: general controls and application controls.

General controls include technology management, infrastructure management, security management, and software acquisition, development, and maintenance. Application controls focus on the completeness and accuracy of information, such as error detection, data reasonableness tests, logic tests, and providing users with predefined lists of acceptable data.

The audit narrative, which is developed as part of the controls assessment, provides context, story line, acknowledgement of threats and risks, and identification of the controls used to address mitigate the threat and subsequent risk. Over time, the IT Auditor should expect Enterprise Risk Management to become the accepted standard. In the nearer time horizon, the Risk Mitigation Process in Figure 3-4 is a middle ground and provides some structure to the risk mitigation process.

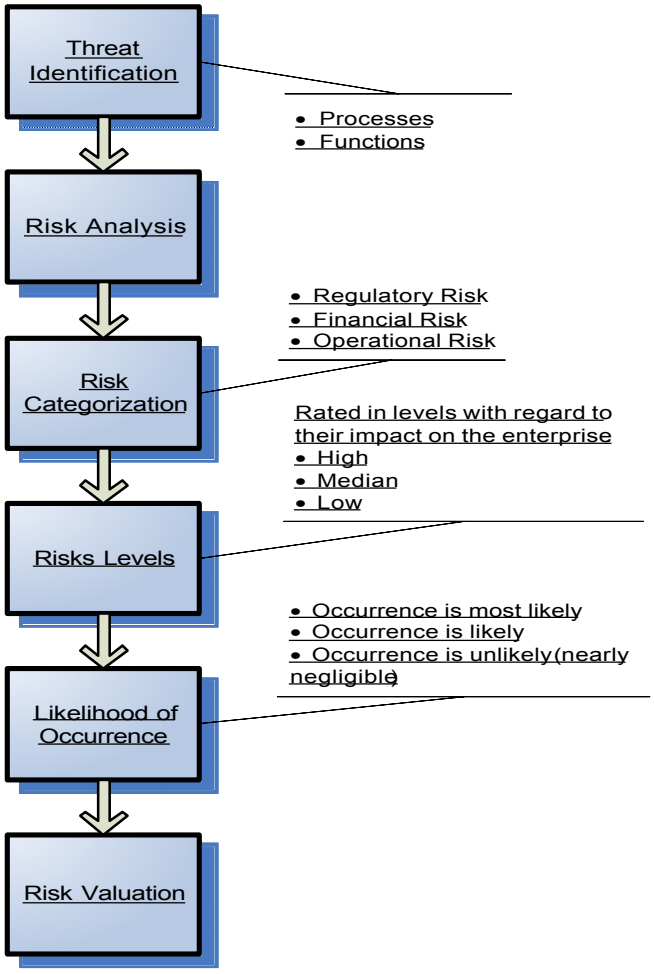


Figure 3-4 - Risk Mitigation Process

These definitions and requirements are already filtering into SOX-404 activities.

[40, 41] However, it is beyond the scope of this paper to do more than direct the reader's attention to this literature and suggest that such a program be considered.

3.4.1 Audit Risk Mitigation

Audit risk is a technical audit matter that an IT Auditor should be sensitive to since it deals with the risk of material misstatement. Combined inherent and control risk determines the risk of material misstatement. Inherent and control risk are characteristics of the client, its accounting system and records. SAS-47 requires the auditor to plan the audit to hold audit risk to a low level. [12, 15] The immediate impact upon the SOX audit is the determination of the nature of the testing and the size of the samples used in the testing. The Audit Risk Matrix illustrated in Table 3-5 here is drawn from the case study discussed in Section 4.

Inherent Risk[1] Assessment	Control Risk[2] Assessment			Audit Risk[3]	Detection Risk[4] Accepted	Nature of Procedure[6]	Extent of Audit Procedures[7]
	Maximum	Moderate	Low				
High	Value[5]	Value[5]	Value[5]	Value[5]	Value[5]	Nature[6]	Sample Size
Moderate	Value[5]	Value[5]	Value[5]	Value[5]	Value[5]	Nature[6]	Sample Size
Low	Value[5]	Value[5]	Value[5]	Value[5]	Value[5]	Nature[6]	Sample Size

Table 3-5 - Audit Risk Matrix

[1] Inherent Risk is the susceptibility of an assertion to a material misstatement, assuming there are no related internal control structure policies or procedures.

[2] Control Risk is the risk that a material misstatement that could occur in an assertion will not be prevented or detected on a timely basis by an entity's internal control structure policies or procedures.

[3] Audit Risk (Material Misstatement) is the risk of unknowingly failing to appropriately modify the audit opinion on financial statements that are materially misstated.

[4] Detection Risk is the risk that the auditor will not detect a material misstatement that exists in an assertion and is inversely related to the effectiveness of substantive tests.

[5] Value is the joint risk assessment value and may be either a "Low – Moderate – High" assessment or a numerical result.

[6] Nature of Procedure may be Analytical Procedures only or Tests of Details only or a combination of these two procedures.

[7] Extent of Audit Procedures is the sample size that will be used for testing and may be One, All, or a percentage of the population with a sample size limit in a given population size (e.g. 25 max or 25% if pop < 100

3.4.2 Risk Mitigation Analysis

This section suggests several alternative techniques to the IT Auditor who believes that his circumstance could benefit from a more rigorous analysis. These two techniques are drawn from the Decision Assistance Sciences, an area of research that is both broad and deep, [42] They are the Bayesian Approach and Probability Theory and provide, perhaps, the best trade off between complexity (difficulty to implement) and quality of result.

3.4.2.1 Bayesian Approach

The Bayesian approach is one of the best known methodologies for solving decision problems when facing uncertainty. … The mathematical tools of the Bayesians are similar to statistical decision theory, except that subjective probabilities are used. … The personal, judgmental, or subjective probability measure is interpreted as an expression of an individual's feelings about the relative likelihood of the outcome of the decision.

The primary usefulness of the Bayesian approach is its ability to handle non-repetitive, "one-shot", decision problems. Indeed, in situations which have never before occurred, and where no a priori information is available, Bayesian techniques are almost indispensable. However, Bayesian methods are useful also in repetitive situations. Bayes' theorem

$$P\left(\frac{A}{B}\right) = \frac{P(A) \cdot P\left(\frac{B}{A}\right)}{P(B)}$$

offers us guidance for modifying judgments in the light of new experience. This theorem is central to the Bayesian approach to learning. In fact, many elaborate learning schemes have been developed from this simple theorem …

We interpret P(A) to describe the decision-maker's judgments about the states of nature, future events, or hypotheses, before obtaining additional information; that is, P(A) is the a priori probability. P(A/B) is interpreted as the revised value of this probability after receiving additional information or a posteriori probability. [43]

3.4.2.2 Probability Theory Approach

Probability theory is based on the axiom that probabilities may be assigned to information structures in one of two ways. In one case the probabilities are regarded as the numerical weights that would be consistently assigned to events.
(This may be seen in earlier sections) …
The alternative is to represent an information pattern as a proposition or a collection of propositions (e.g., h(z)), and then ask what is the probability that h(z) is true. In either case the numerical probability values represent a

mathematically precise expression of the corresponding knowledge.

If the formulation of available information is done in a manner consistent with probability theory, then the well-developed mathematical apparatus of probability calculus is available for further information processing. This ability to draw upon the entire logic of probability theory is very important and useful. For instance, probability theory methods may be used to determine numerical measures of compound events from the measures assigned to individual events (aggregation of information). Or the probability calculus can be used to condense a body of knowledge to a form which is more readily comprehensible. Additionally, Bayesian methods provide us with a mathematical technique for gradually modifying earlier measures in the light of new information as this information gradually becomes available. One technique that has particularly powerful potential use is the ability to combine probability functions … For example, the probability function for the variable "x", is expressed as a distribution, or,

$$P(x_1 \le x \le x_2) = \int_{x_1}^{x_2} f(x)dx$$

where the probability of an exhaustive set of events is unity' and the distribution is continuous. (See Figure 3-5 – Distribution x).

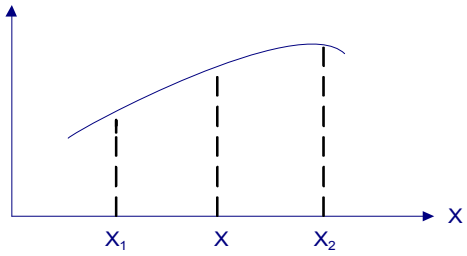


Figure 3-5 – Distribution x

The second variable, "y" is independent but nonexclusive. (See Figure 3-6 – Distribution y).

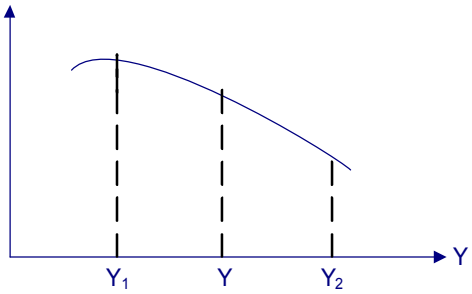


Figure 3-6 – Distribution y

The probability density function becomes f(x, y) and becomes the volume under the surface (see Figure 3-7).

$$P\begin{cases} x_1 \le x \le y_2 \\ y_1 \le y \le y_2 \end{cases} = \int_{y1}^{y2}\int_{x1}^{x2} f(x,y)dxdy$$

and

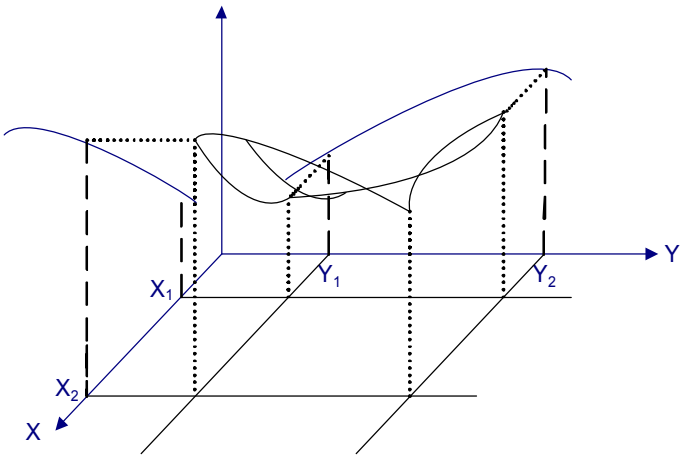


Figure 3-7 – Probability of X and Y

Therefore, the Probability of X and Y is:

$$P(x,y) = \int_{x1}^{x2}\int_{y1}^{x2} f(x,y)dxdy$$

In a similar manner, the variance can also be derived. [44] The real value and utility of this approach is its ability to cope with non linear probability relationships, its

ability to merge multiple probabilities into a single function with a variance, and its ability to handle a relatively large number of simultaneous probability functions. So, while it may be possible to only graphically represent the interaction of two probability distributions, as can be seen in Figure 3-6, the calculus allows for the creation of an "n-dimensional" solution space. Hence, it is possible to know, with some precision, the effect of the risk mitigation effort.

3.5 Controls Assessment

Controls are the response to identified risks. Two broad classes of controls are established by the SOX process. These are the Key Controls and the General Controls. They are designed to ensure that the controls are sufficient to:

- prevent fraud, misuse, and/or loss of financial data/transactions,
- enable speedy detection if and when such problems occur, and
- promote effective action to limit the effects of such problems.

Key Controls and the General Controls can generally be derived from IT best practices since they typically meet the intent of the Sarbanes-Oxley initiative. The SOX-404 auditor should be sensitive to conflicts between traditional best practices and SOX requirements, particularly in the areas of some open source strategies and "need to know" issues. The SOX-404 auditor should remember that one of the key ideas within Sarbanes-Oxley is that access to information should limited to a "need to know" basis, and that all key and most other processes should be controlled.

The SOX-404 Auditor can test the general quality of the controls by determining if a policy, procedure, or processes are:

- standardized across the company
- centrally administered
- centrally controlled
- repeatable

3.5.1 Key Controls

Key controls are generally defined in the literature as being the controls that are fundamental to ensuring that the values on the balance sheet are accurate and reliable. Therefore, all monetary transaction must be initialized, authorized, implemented, documented, controlled, reported, and validated using key controls. If one of these controls is IT based, then it should be covered by the SOX-404 audit.

One example of key control is a report that is used to check that two separate systems tally with one another. A second example is a trigger on a database table that ensures that adding any entry into the accounts receivable table automatically creates an entry into the general ledger. The SOX-404 audit would ensure that this trigger is in place, is correctly coded, and can be changed only by authorized personnel. Code reviews, design walkthroughs, unit testing, and user-acceptance testing are examples of ways in which reports should be validated as being reliable.

3.5.2 General Controls

General controls, for SOX audits, are commonly defined in the literature as being the controls that are applicable across all IT systems and are essential to ensuring the integrity, reliability, and quality of the systems. General Controls, in particular, are standardized across the company, centrally administered, controlled and repeatable. Examples of general controls include (but are not limited to):

- Physical Access and Security
- Operational Control Processes
- Logical Access Processes
- Backup and Recovery
- Disaster recovery policies
- Service-level agreement policies
- Application or Software development processes
- Testing
- Configuration and Change management

From the SOX Auditor's point of view, it is preferable if controls are automated since automation makes it more difficult for individuals to manipulate the control either in error or maliciously. The centralized automation of controls should include:

- Centrally administration of IT processes by the relevant MIS department
- Centralized document version control of policies and procedures
- Backup and recovery procedures using scripts, using clustering techniques, RAID, etc. as well as to automatically transfer control to backup hardware when the primary hardware fails.
- Authentication and access-control procedures using centralized directory services such as LDAP or Active Directory.
- Intrusion prevention and detection processes using centralized services such as IPS/IDS software.
- Antivirus processes using centralized software such as McAfee or Symantec antivirus software.
- A process for managing changes to IT assets or objects exists and documents that changes are reviewed and authorized.

If the company is developing software the SOX auditor should also ensure that:

- A common SDLC process for system design, development, and installation is used across all applications.
- Coding standards exist and are adhered to, and code is reviewed to enforce the coding standards.
- All changes to code undergo a standard approval process and are tested and documented prior to being implemented.

- Incident-management procedures exist, and personnel are trained in the appropriate response to incidents.
- A centralized inventory of all IT infrastructure assets (PCs, firewalls, servers, routers, hubs, etc.)

The granularity of the expansion of general controls depends on the industry (i.e. business type) in which the company operates. As a result, a consumer soft goods manufacture can be expected to have a number of significantly different controls than a internet services provider. Accordingly, the expanded granularity of most company's Configuration Management might include:

- Version management/release management procedures, and
- Source code/document version control procedures.

A software development company could be expected to add granularity to the software development lifecycle controls and should include:

- Clear process and structure, documented
- Design documentation standards
- Coding standards
- Testing standards
- QA processes/standards

3.6 Controls Documentation, Walkthroughs and Testing

The audit narrative, which is developed as part of the controls assessment, provides description of the threats and therefore risks confronting the system and the controls that should be in place to mitigate the risk. This section describes a methodology for documenting, walking through and testing controls in a SOX-404 Audit.

The IT Auditor will test the effectiveness of the systems controls by developing a narrative of the critical business processes. These processes are typically Operations, Physical security, Logical access, Applications, and Back-up and recovery. Other processes may be added (or deleted) as a company's individual circumstances require.

Controls may be tested by a range of methods. For both key and general controls the most common method includes interviews to ensure that procedures are followed and sample testing to ensure that documents and records are kept. The sample size reflects the objectives and constraints of Audit Risk Mitigation (Section 3.4.1). If development controls are being tested, then testing methods may include design walkthroughs and code reviews.

For each control, the IT Auditor needs to be able to show how the relevant policies, procedures, and processes are: Created, Approved, Implemented, Monitored for consistency and enforcement, Reported on an ongoing basis, not just a one-time report, and Changed including a feedback loop for changes or improvements to be

made

The illustrated methodology utilizes application controls in SAP or similar purchased ERP software packages. The level of documentation and how walkthroughs and testing will be performed are dependent on the type of the application control. Documentation of the control is typically referenced in the Business Process Narratives, Walkthroughs, and Testing workpaper.

For SOX, application controls mitigate the risks associated with the business processes that the ERP software package has automated. These application controls are generally configured application controls, programmed application controls or logical access-related application controls; which are described in the following sections.

3.6.1. Configured Application Controls

SAP and other ERP systems tend to configure critical application controls. That is, a parameter is set by a human being, such as being either active or inactive, set to a certain limit, etc. The IT Auditor should test for these parameter settings. Consider the following example:

Process:	Accounts Payable
Risk:	Disbursements are fraudulent.
Control:	The System performs a 3-way match between invoice, purchase order, and receiving report

Table 3-6 – Sample of Configured Application Controls

In this example, the application control would be configured in the ERP system for accounts payable by activating the 3-way match option to systematically force a comparison between the invoice, purchase order, and receiving report prior to allowing a payment.

3.6.1.1 Configured Application Narrative

The narrative of the accounts payable process should discuss that the application performs a systematic 3-way match to prevent unauthorized disbursements. The discussion does not need to discuss specific system settings.

3.6.1.2 Configured Application Walkthrough

A walkthrough provides the process and design confirmation of the related key controls that have been documented in the narrative and that they are operating as documented. To accomplish this for a configured application control, assess the configuration setting on the application and document the results. This should include evidence of the setting (e.g., system report or screen shot).

3.6.1.3 Configured Application Testing

The walkthrough is, basically, a complete test of the application control since it validates that the settings are correct. To help ensure there is not a gap in testing documentation, there should still be a testing strategy defined to evaluate the setting, but do not re-perform the test, rather refer to the walkthrough. Additional testing should validate that the settings remain accurate over time. Controls that help ensure this are IT general controls and should be documented, walked through and tested in the IT General Control effort.

3.6.2 Programmed Application Control

Critical application controls tend to be programmed in applications that are custom developments or that are purchased and then highly customized. That is the validation routine, edit check, etc. is "hard coded" into program code. The IT Auditor is testing that the system reacts in the predicted manner. Consider the following example:

Process:	Claims
Risk:	Fictitious/duplicate claims are recorded.
Control:	Edit reports identify possible errors in claims transactions.

Table 3-7 – Sample of Programmed Application Control

In this example, the application control has been designed into the program code for the application to systematically identify unusual transactions.

3.6.2.1 Programmed Application Narrative

The narrative of the claims process should discuss that the application performs systematic edits to identify errors in the claims transactions, including duplicate claims, etc. The discussion should include the types of edits, how the system reacts (e.g., give a warning and logs the edit to a report, prevents the entry), any manual follow up processes. The discussion does not need to include the specific program code or program logic supporting this edit.

3.6.2.2 Programmed Application Walkthrough

A walkthrough provides the process and design confirmation of the related key controls that have been documented in the narrative and that they are operating as documented. The walkthrough attempts a transaction that should result in an error and verifies that the system reacts as intended. That is, the system should provide a warning when an attempt to enter the same claim is entered twice. This test should include tests for "false positives" as well as "false negatives." Support of the evidence observed on-line. Such as a system report or screen shot should also be included.

3.6.2.3 Programmed Application Testing

The walkthrough is, basically, a complete test of the application control since it

validates that the effectiveness of the edit. To help ensure there is not a gap in testing documentation, there should still be a testing strategy defined to evaluate the setting, but do not re-perform the test, rather refer to the walkthrough. Additional testing should validate that the settings remain accurate over time. Controls that help ensure this are IT general controls and should be documented, walked through and tested in the IT General Control effort.

3.6.3 Logical Access-Related Application Control

Critical application controls in general enterprise applications tend to be logical access-related. For example, a key separation of duties is systematically enforced through application security. The IT Auditor is testing that the system enforces access controls based on the separation of duties definitions and does so in a predicted manner. Consider the following example:

Process:	Sales Commissions
Risk:	Invoices don't reflect the right prices and terms.
Control:	Access to commission rate tables is restricted

Table 3-8 – Sample of Logical Access-Application Control

In this example, the control is the access security that has been implemented, restricting who can modify specific database tables, in this example the commission tables.

3.6.3.1 Logical Access Narrative

The narrative of the process should discuss that access to commission tables is limited to certain individuals. The discussion should include the job titles or department names of the individuals with the access. It should also identify the actual transactions (e.g., transaction ABCD) that are relevant to the function.

3.6.3.2 Logical Access Walkthrough

A walkthrough provides the process and design confirmation of the related key controls that have been documented in the narrative and that they are operating as documented. The audit should assess the configuration settings on the application and document the results. This should include evidence of the setting (e.g., system report or screen shot). Logical access-application controls should evaluate whether:

- the identified transactions perform as documented,
- the application security is functioning as expected, and
- tests for "false positives" as well as "false negatives."

To accomplish this for a logical access-related application control, the auditor may perform the following steps:

- Set up a test ID without privileges to perform the function

- Attempt to perform the function
- Verify the system functions as designed and prevents the transaction.

Support of walkthrough should include evidence by way of a system report or screen shot that the test ID account was set up and the access levels assigned to the test ID. In the even that the application is a basically an unmodified commercial software package and the transactions are commonly known, it may not be necessary to "drill down" very far since the commercial package is already well understood.

3.6.3.3 Logical Access-Testing

The IT auditor should validate the operating effectiveness of the control by testing and evaluating whether users with this level of access are appropriate. To make this assessment, the test procedure should include the following steps:

- Obtain a system-generated report of all users with this authority (in this case, access to modify rate tables)
- Select a sample of the users
- Assess the appropriateness of the access for the users.

Additional testing should validate that the settings remain accurate over time. Controls that help ensure this are IT general controls and should be documented, walked through and tested in the IT General Control effort.

3.6.4. General Control Tests

It is useful for the Sarbanes Oxley IT Auditor to regularly remind him/herself that the key driver behind the Act is to have the companies executives attest to the fact that there are sufficient controls to prevent fraud or misuse of company assets or loss of financial data, there are controls to enable rapid detection if and when such problems happen and that there are procedures to effective action is taken to limit the effects of such problems.

The Sarbanes-Oxley IT auditor should test for a number of important general controls. The "good news" for the auditor is that these tests are usually well know and well understood IT audit tests with only the SOX bias no financial matters influencing the testing process. The auditor should test for, at minimum, the following controls.

- User provisioning. Should ensure that new users are set up with the correct privileges, by creating a standard profile for each type of user. This profile should determine the permissions assigned to the specific user. There should be specific checklists to provide for the standardization of the process to enforce rules that prevent users from being assigned the wrong privileges.
- User de-provisioning. Should ensure that departing users are removed from all access points in the systems. There should be specific checklists to provide for the standardization of the process.
- Authentication. Should enforce the use of a central LDAP, Active Directory

repository, or similar identity management system for the establishment of roles and granting of privileges.

- Least privilege. Should be applied when assigning permissions within the operating system, the applications, and the databases. Any individual should be given only the permissions he/she needs in order to carry out his/her job. This should be enforced at the operating system level, the network (component) level, the database level, and the application level
- Separation of duties, rights and privileges. As previously discussed, and as with any accounting/financial system, no single individual should be able to access all IT systems involved in financial transactions because knowledge of the full path through those systems could make it easier for that person to commit fraud; often implemented using the concept of "roles" within an IT system.
- Change management. Should check that a formal process is in place that ensures that unauthorized change cannot be made to the system by an unauthorized person, the company's assets are not used on changes that have not been authorized and system integrity is maintained for systems within the scope of the audit.

3.7 Report To Management

IT Auditor should expect the Sarbanes Oxley Audit Report to Management for Section 404 to be part of the larger Audit Report. The IT Auditor should also expect make several specific contributions. These include:

- the workpaper outlined in Table 3-9 – Sample Workpaper Index
- memoranda on any deficiencies and that were found and remediation that might be necessary If none were found, then this memo should note that also.
- other documentation of the testing, results, or specific issues that would have a material impact on the findings of the audit.
- In addition to the workpaper, the Auditor should expect to provide input to the “Findings” and “Recommendations” sections of the report.

Stylistically, the IT Auditor should expect her contribution to be fully in keeping with the larger document.

IT Processing Narrative – Overall
Operations Test Plan and Summary Results
OS Test Sheet 1 through n
OS screenshots and System checks information
Applications Test Plan and Summary Results

AISM Test Sheet 1 through n
AISM screenshots and System checks information
Logical Security Test Plan and Summary Results
LS Test Sheet 1, through n
LS Supporting Documentation, Policies, Procedures
Physical Security Test Plan and Summary Results
PS Test Sheet 1 through n
PS Supporting Documentation, Policies, Procedures
Backup & Recovery Test Plan and Summary Results
BR Test Sheet 1 through n
BR Supporting Documentation, Policies, Procedures

Table 3-9 – Sample Workpaper Index

3.7.1 Determining the Need for a SAS 70 Report

For the IT Auditor, part of the report to management may include the recommendation to include a SAS 70 report and most commonly a Type II rather than a Type I. This recommendation may also be made to the Outsource .Service provider. The auditor should determine if significant accounts' data is processed by the service organization. If this is occurring, then the controls will apply t it also. A Decision Tree for SAS 70 is illustrated in Figure 3-7 – SAS 70 Decision Tree. Ultimately, however, the use of SAS 70 will depend on the management of both the primary company and the service company.

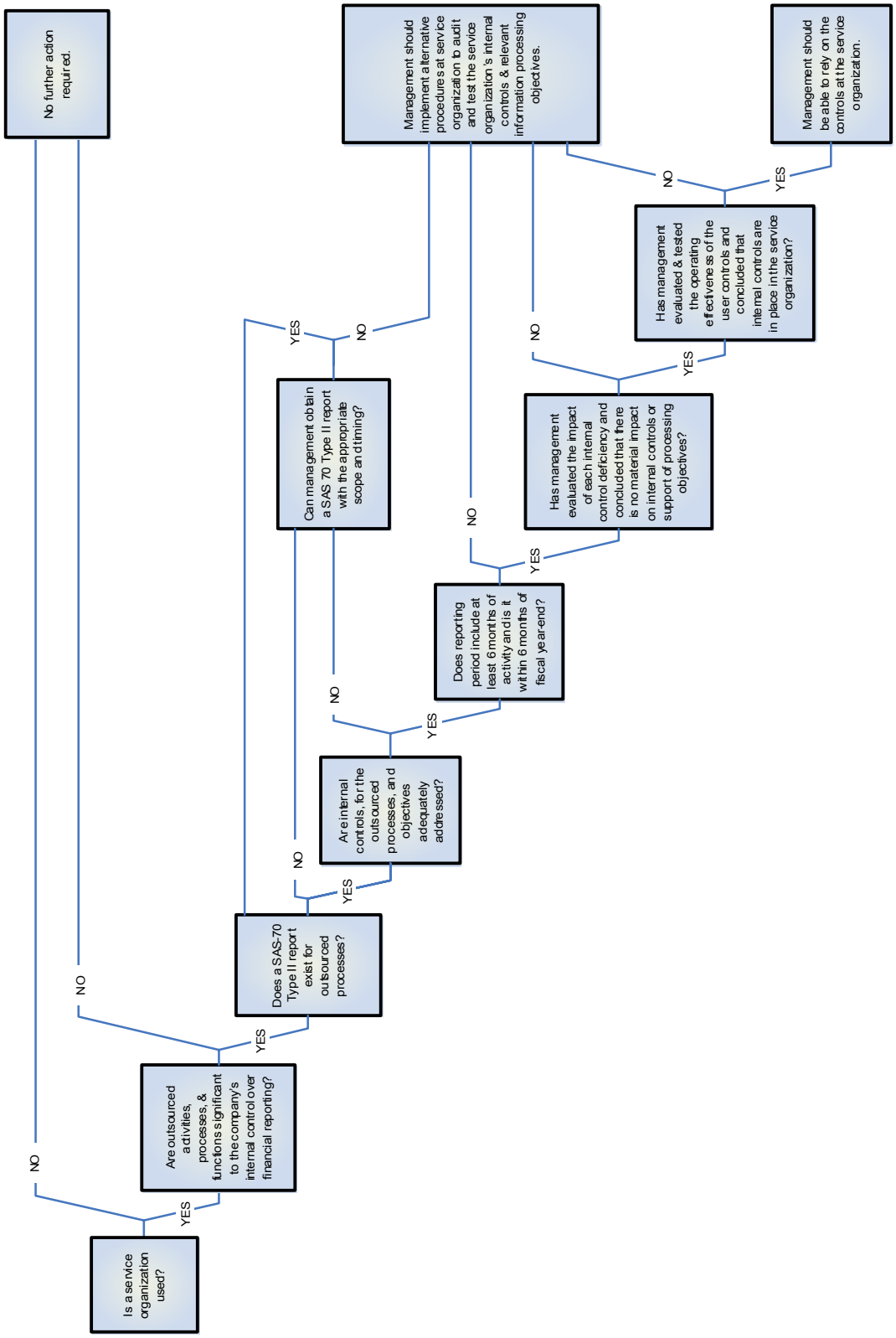


Figure 3-7 – SAS 70 Decision Tree

4.0 CASE STUDY

The case study presented in this section is drawn extensively from the actual workpaper of the audit implemented for the case study companies. Since the case study is intended to be illustrative of the process developed in Section 3.0, the workpapers have been edited to shorten the length of the narrative, reduce the number of control points without losing the character of the audit, while continuing to conceal the true identity of these companies.

The gentle reader should bear in mind that the case study audit did not implement all of the process steps developed in Section 3.0. Additionally, the material provided in Section 4.7 - Report To Management, is limited to the contributions that the workpapers would provide. It is assumed that a professional IT Auditor will competently handle the stylistic requirements of report writing. Therefore, only the material contributions that are included in the report are provided.

4.1 Preparation

The operations of Octopus Corporation are scheduled to be audited by their independent outside auditors. Under the provisions of Sarbanes Oxley, the outside auditors are required to maintain their independence and can not provide any other services. Therefore, Octopus has hired the CPA firm of Dewey, Cheetem and Howe to conduct an internal Sarbanes Audit to identify any deficiencies and then conduct a remediation program to correct the deficiencies.

4.1.1 Scope

Management has defined several essential objectives for this internal audit. One is to identify any SOX related deficiencies that may exist and have remediation actions underway prior to the arrival of the outside (i.e. independent) auditors. A second is to minimize or eliminate the possibility that the independent auditors report contains deficiency comments. A third is to hold the cost of all the Sarbanes activities to an absolute minimum.

Octopus Corporation's Information Technology operations in Europe are characterized by the following factors.

- All IT operations and functions are managed by GIACE under their outsource contract
- A SOX-404 audit of Octopus – Europe will be treated synonymously and will be, essentially, the same as a SOX-404 audit of GIACE; in accordance with Sarbanes statutory provisions.
- The European division of Octopus is relatively small. The total sales volume of the corporation is approaching $2 billion dollars; the sales volume for all European operations is only about $200 million dollars.
- Size and scope of the company's IT activities is small, even when measured against the size of the division of the company in which it operates.

- Octopus Corp's industry and markets are highly seasonal and very mature and characterized by low but stable margins
- In the past year, the number of changes to the IT environment has been both small number of simple and simple in their relative complexity.

4.1.2 Regulatory Tailoring

Octopus management in conjunction with their internal CPA firm of Dewey, Cheetem and Howe have decided that Octopus Corporation will adopt only the COSO framework and not the COBIT framework.

One immediate consequence of this decision is that the regulatory framework will be general in nature and not provide a significant amount of detail with regards to IT matters. It also implies that significantly greater subjectivity in the decisions and values used will be tolerated by management as long as the COSO framework is supported.

4.2 Environment Identification

GIAC Enterprises is an IT services provider who provides outsourcing services, SAP services, system development, and a variety of other services to multiple clients, from their location in Elbonia. Virtually all of Octopus' day-to-day IT production activities in Europe have been outsourced to GIAC Enterprises.

4.2.1 Organizational Structure

As the primary provider of IT services to Octopus Corporation, Europe, the management of GIACE has designated that certain personnel positions be permanently assigned to the Octopus account. These include:

- Lead SAP Service Manager who coordinates and manages the SAP Services,
- Operational Services Manager who manages the Operational services side of the account.
- SAP Basis Technical Analyst who manages the SAP Basis matters,
- Service Support Manager, and
- Applications Enhancements Manager.

These individuals and their designees are or lead staff personnel are the key contacts within GIACE for this review. The organization chart is provided in Figure 4-1. Furthermore, the reporting structure, staffing, organizational charters and separation of duties were analyzed for appropriate segregation of duties. As a result of this review, no separation of responsibility issues were identified. A Segregation of Duties Matrix was developed. It is provided as Table 4-1 and incorporated into the audit work papers.

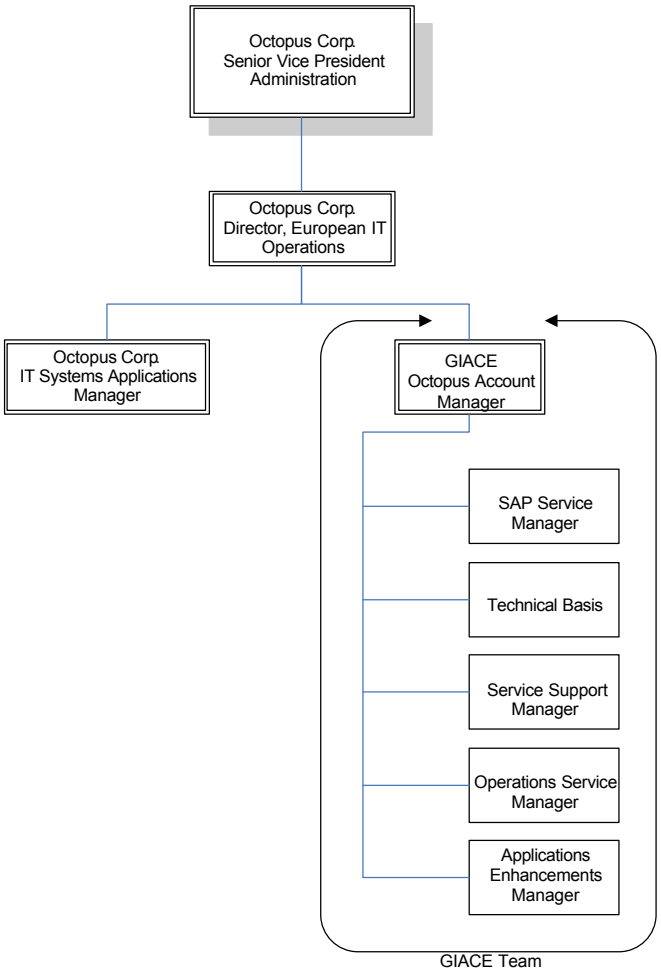


Figure 4-1 - GIACE Organization Supporting Octopus Corp

The Segregation of Duties Matrix is as follows.

Process	Authorization	Custody of assets	Recording	Control activity
SAP SERVICES				
SAP Service Manager	✓			
Receives Requests		✓		
Verifies Request and Permissions			✓	
Approves Action		✓		
Reconciles request and Action				✓
Controls the accuracy, completeness of, and access to data files				✓
OPERATIONAL SERVICES				
Operational Services Manager	✓			
Receives Requests		✓		
Verifies Request and Permissions			✓	

Approves Action		✓		
Reconciles request and Action				✓
Controls the accuracy, completeness of, and access to data files				✓
SAP BASIS SERVICES				
SAP Basis Technical Analyst	✓			
Receives Requests		✓		
Verifies Request and Permissions			✓	
Approves Action		✓		
Reconciles request and Action				✓
Controls the accuracy, completeness of, and access to data files				✓
SERVICE SUPPORT				
Service Support Manager	✓			
Receives Requests		✓		
Verifies Request and Permissions			✓	
Approves Action		✓		
Reconciles request and Action				✓
Controls the accuracy, completeness of, and access to data files				✓
APPLICATIONS ENHANCEMENTS				
Applications Enhancements Manager	✓			
Receives Requests		✓		
Verifies Request and Permissions			✓	
Approves Action		✓		
Reconciles request and Action				✓
Controls the accuracy, completeness of, and access to data files				✓

Table 4-1 - Segregation of Duties Matrix

4.2.2 System Environment

The system diagram is illustrated in Figure 4-2,

4.3 Threat and Risk Assessment

Interviews with Octopus' senior management has reveled that only a small number of threats and/or vulnerabilities are considered to be worthy of a defensive or risk mitigation action plan. The Potential Threats, Probability of their Occurrence and the relative amount of impact on the company was developed into a matrix in Table 4-2 and incorporated into the workpapers of the audit.

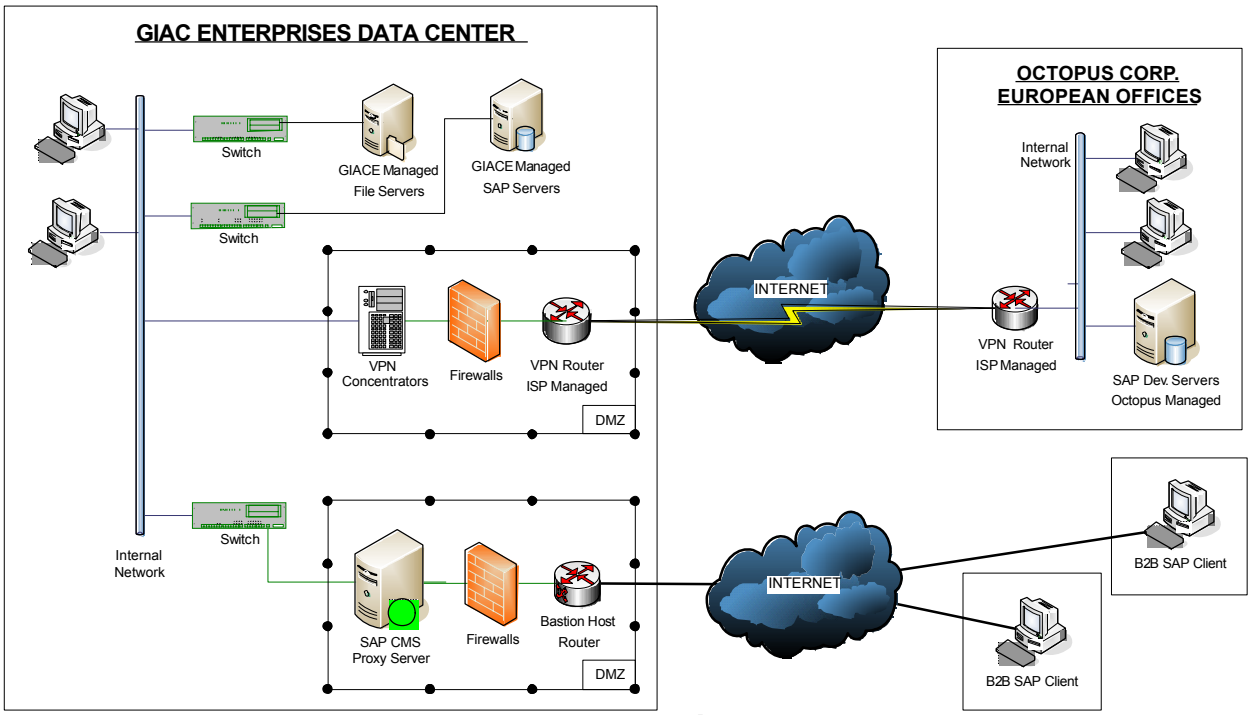


Figure 4-2 – System Diagram

Potential Threat	Probability of Occurrence	Impact
Errors and Omissions		
Accidental Release or Loss of Sensitive Information	Medium	Medium
Accidental Destruction of Information	Low	Medium
Fraud and Theft		
Theft	Medium	Medium
Fraud	Medium	Medium
Industrial Espionage	Low	Medium
Internal Attack		
Misuse of System Resources by authorized user	Low	Low
Unauthorized Release or Loss of Sensitive Information	Medium	Medium
Surreptitious access to information or assets	Low	Medium
External Attack		
Theft of System Resources by unauthorized user	High	Medium
Unauthorized Access to Telecommunications Resources (e.g. long-distance services voice-mail)	Medium	Medium
Destruction of Information (Malicious Code, Virus Contamination, etc.)	Medium	Medium
Hacker disruptions to operations	Medium	Medium
Loss of Physical Infrastructure		
Natural Disaster	Low	High

Table 4-2 - Potential Threats, Occurrence Probability and Impact

To summarize, Octopus' management does not see themselves, or the company, as a target for anyone or almost anything.

4.4 Risk Mitigation

Meetings between Octopus management and the SOX Auditors has determined that a number of risk mitigation decisions had been made prior to the start of the audit. The most important one, from the point of view of Octopus' management was the outsourcing of all European production and operational IT activities to GAICE. As a result, Octopus' management held the position that under the terms of their SLA's all risk management implementation tasks was fully GIACE's responsibility. Inspection of the SLAs supported this position.

It was also necessary for the IT Auditor to provide Octopus' management with the understanding that, under most interpretations of the provisions of Sarbanes Oxley, outsourcing of an area covered by the provisions of the law does not relive the part from its obligations of the law. Therefore, Octopus' management must still make the same attestations and has the same obligations and requirements, regardless of whether IT is outsourced.

While the nature of Octopus' the risk exposure changed as a result of the outsourcing decision, the fundamental factors of Octopus Europe, GIACE's threat and risk profile changed very little. In this case, GIACE's threat and risk model is very traditional and is incorporated into the control and monitoring and audit risk mitigation analyses. It is Management's opinion is that this level of detail in it s risk appetite is sufficient to address the risks that the company is likely to encounter. Table 4-3 provides a listing of the potential threats and implementation of controls and monitoring.

Potential Threat	Controls Implemented?	Monitoring In place?
Errors and Omissions		
Accidental Release or Loss of Sensitive Information	**Y**	**Y**
Accidental Destruction of Information	**Y**	**Y**
Fraud and Theft		
Theft	**Y**	**Y**
Fraud	**Y**	**Y**
Industrial Espionage	**Y**	**Y**
Internal Attack		
Misuse of System Resources by authorized user	**Y**	**Y**
Unauthorized Release or Loss of Sensitive Information	**Y**	**Y**
Surreptitious access to information or assets	**Y**	**Y**
External Attack		
Theft of System Resources by unauthorized user	**Y**	**Y**

Unauthorized Access to Telecommunications Resources (e.g. long-distance services voice-mail)	**Y**	**Y**
Destruction of Information (Malicious Code, Virus Contamination, etc.)	**Y**	**Y**
Hacker disruptions to operations	**Y**	**Y**
Loss of Physical Infrastructure		
Natural Disaster	**Y**	**Y**

Table 4-3 - Potential Threats, Controls and Monitoring

Inherent Risk[1]	Control Risk[2] Assessment			Audit Risk[3]	Detection Risk[4]	Nature of Procedure	Extent of Audit
Assessment	**Maximum**	**Moderate**	**Low**		**Accepted**	[5]	**Procedures** [6]
High	High	High	Moderate	Low	High	Analytical Procedures Only	Sample Size 25 MAX or 25% if pop < 100
Moderate	Moderate	Low	Low	Moderate	Moderate	Combined Analytical & Tests of Details	Sample Size 40 MAX or 40% if pop < 100
Low	Moderate	Low	Low	High	Low	Tests of Details	Sample Size 60 MAX or 60% if pop < 100

Table 4-4 - Audit Risk Matrix

[1] Inherent Risk is the susceptibility of an assertion to a material misstatement, assuming there are no related internal control structure policies or procedures.

[2] Control Risk is the risk that a material misstatement that could occur in an assertion will not be prevented or detected on a timely basis by an entity's internal control structure policies or procedures.

[3] Audit Risk (Material Misstatement) is the risk of unknowingly failing to appropriately modify the audit opinion on financial statements that are materially misstated.

[4] Detection Risk is the risk that the auditor will not detect a material misstatement that exists in an assertion and is inversely related to the effectiveness of substantive tests.

[5] Nature of Procedure may be Analytical Procedures only or Tests of Details only or a combination of these two procedures.

[6] Extent of Audit Procedures is the sample size that will be used for testing and may be One, All, or a percentage of the population with a sample size limit in a given population size (e.g. 25 max or 25% if pop < 100

4.5 Case Study Narrative and Controls Documentation

Octopus Corporation's European IT Operations that are outsourced to GIACE include SAP hardware hosting and support, LAN and e-mail server monitoring and system management, and Local Area Network monitoring and management. The Wide Area Network is a managed service of Enormous Telco Ltd. These various

services are implemented by formal contracts.

Interviews with GIACE's senior management revealed important basic information; which was later verified by document inspection. This information included the fact that GIACE is registered and audited to BS7799 and their support and management operations are registered and audited against ISO 9001:2000. It also included the facts that the IT function is regularly audited against its quality procedures by both internal and external quality auditors and that the external auditors of Octopus Corporation have carried out financial and management audits for the past 2 years.

The GIACE IT Manager is responsible for maintaining the Octopus European IT Strategy; the workpapers contain a referenced copy of the IT Strategy Principles document. Separate IT Steering Groups are in existence. These steering groups agree the IT strategy and hence to the broad direction of IT and prioritized use of resources. A part of the process walk through was the review of the IT strategy documents. The general approach is maintenance of the current processing environments in which changes are characterized as minor overall and enhancements reflect changes to the way business is conducted.

The narratives and controls are divided into five major areas or divisions. These are Operations, Physical Security, Logical Access, Applications, and Back-Up and Recovery. These five areas are the organizational basis for all subsequent testing and documentation.

4.5.1 Operations

The outsourcing contract between Octopus Corp. and GIACE describes the various agreements between the parties. The Service Level Agreements describes the performance requirements and services levels, stipulated between the parties that are used to manage the relationship.

4.5.1.1 Operations Monitoring and Control

The overall monitoring of the account is governed by monthly performance review meetings with future planning discussions. The GIACE Service Manager leads the review sessions since he/she is Octopus Corp.'s primary point of contact for all GIACE SAP support services. Typical Agenda topics include:

Service Scope

- Deliver service reporting
- Review progress on larger enhancements.
- Discuss planned future activities
- Resource allocation.
- Ensure a high quality of service is maintained.
- Customer satisfaction

Service Reviews

- Number of call hours used over previous quarter vs. hours expected
- Review of open support issues and follow-up actions
- Trends: any recurring support problems reviewed to help identify root causes and possible solutions
- Performance statistics of overall contract
- Plans for IT developments
- Performance against measures.

These meetings have recorded minutes that capture the decisions/actions determined as a result of the monthly review meeting

CONTROL OP-1
Standard Monitoring and Control documents are regularly used to standardize and document processes and activities.

4.5.1.2 Operations Certification

The Information Security Management of IT solutions provision for the design, development, implementation, operation and support of the following: Managed Operations, including: Data Centre Management, Help Desk Services, Desktop Services, Network Services, Communications Services, Print and Data Services, Transaction Processing Services, Software Services, Training Services and Applications Facility Management in accordance with the BS7799 Statement of Applicability.

CONTROL OP-2
The GIACE facility is a registered BS7799/ISO 9001:2000 site.

4.5.1.3 SAP Job Initiation, Approval & Scheduling

Octopus Corp has outsourced the support and maintenance of its production SAP environment to GIACE, the controls that are in place are those of the outsource organization with appropriate checkpoints; as per discussion with GIACE Team Members.

The Scheduling process details SAP production programs related to batch and on-line transaction processing, including the monitoring and corrective actions taken in response to exception processing. The process includes how production jobs are initiated, what approvals are needed for initiation, what procedures are followed when scheduling a new job, tools used in monitoring production processing, and what escalation procedures are in place to respond to exception processing.

The authorization of changes to the job scheduling is the responsibility of Octopus Corp. Management. A copy of the GIACE/Octopus Corp contract covering provision of SAP support and hosting services is held in the company's general offices. The primary scheduling tool in place at Octopus Corp that supports the production schedules for the SAP application is the standard SAP R/3 job scheduler supplied

within the SAP application.

All new production programs must follow the appropriate change management process for entry into the Octopus Corp IT production environment. The change management processes are outlined in the Change Management narrative as developed during interviews with GIACE Team Members.

CONTROL OP-3
SAP R3 Scheduling tools are used for the production of schedules.

Only specifically identified Octopus employees, identified as "superusers" can Add, Change or Remove an existing job from the production schedule. All requests for job changes (new, modify, delete) are logged into Help Desk ticket system. R3 jobs for execution have unique authorization IDs that is identifiable for all jobs. Job modifications in the SAP R3 scheduler must use a unique "SCHEDULER" ID in order to perform the modification and these IDs. Scheduling tools are regularly monitored for batch errors by the Basis team. SAP date/time stamps all job modification transaction and records the job properties. Documented procedures exist for the monitoring of the R3 schedulers.

CONTROL OP-4
SAP date/time stamp all job modification transaction and records the job properties

4.5.1.4 Change Management

Change Management ensures that all changes to current applications are properly authorized, tested, and approved before they are implemented. Changes to the SAP system originate from either problem/incident events such as the system is not operating correctly or from enhancements because the business or user requirements have changed or evolved.

The Change Management Process is initiated when a "Superuser" is unable to resolve the issue. If the "Superuser" is not successful then she logs a problem or enhancement request as a Help Desk Action Item where it is given a control number. This audit seeks to identify, document, and walkthrough key controls for Change Management including:

- Authorization of changes
- Approval of the change prior to the change being moved into production
- Appropriate testing of the change prior to the change being moved into production
- Monitoring of the change process (e.g. steering committee, management review of changes to production)

Action Items are categorized by the Help Desk as either: "problem/incidents" such as the system not working correctly, or an enhancement which is a modification to the existing system configuration.

Only authorized SAP modules are supported under the current contract. These are: Basis, EDI, SD, MM, FI, EIS, CO, and Authorizations. The log must reflect the module (or modules) that is affected or believed to be affected, since the impact may not be known at the time the incident is logged.

CONTROL OP-5
There are a limited number of manual jobs that can be initiated by end users in SAP

Problem-Incident Change Management describes the process if Action Item is categorized as a "problem/incidents" change. In general, resolution of the items/issues raised are the responsibility of GIACE, but they also raise awareness of other items e.g. failure of B2B messages and attention to these other possible errors is raised with the appropriate staff within Octopus Corp; per discussion with GIACE staff. Regular Service Management review meetings are held at agreed frequency dependant on the need e.g. the GIACE SAP contract is reviewed in a monthly videoconference. Enhancement Change Management describes the process if the call is categorized as an Enhancement Change.

CONTROL OP-6
Job changes (add or modify) are made and tested in a test environment separate from production.

CONTROL OP-7
For new R3 job plans, a test of the program and parameter is performed in QA ensure proper combination

CONTROL OP-8
For production systems on working days, a manual daily check is carried out. This identifies any problems that have occurred since the last check.

4.5.1.5 HELP DESK

The Octopus Help Desk is also outsourced to GIACE. The service is staffed for operation everyday between 08:00 a.m. to 5:00 p.m. (0800 x 1700 x 7). The GIACE Help Desk is manned 24 x 7 and out of hours calls will be logged by the Help Desk. Under the contract GIACE responds to major incidents covering non-availability of the site Local Area Network or servers, but the contract does not include desktop PC support out of hours. The Help Desk Services GIACE provides include:

- Fault and Incident resolution to agreed levels
- Ensuring all calls will be logged and tracked in GIACE Origin's problem management system.
- Maintenance of Incident records, response times, causes and related activities

All calls are logged and are given a priority, as agreed jointly between the GIACE Help Desk and the Octopus Corp. support representative, at the time the call is made:

Severity 1:	Critical	All or part of the system is unavailable or faulty, and is threatening the production of the business
Severity 2:	Serious:	An incident that has a serious impact on part of the business
Severity 3:	Medium:	An incident that has temporary impact on users, and is not critical, or a request for advice or Consultancy Services

Logged calls are acted upon within the following timescales; based on the Call Open date and time, and the agreed Fault Fix time, each call is assigned a Target SLA date

Severity	**Response Time**	**Resolution Time**
Critical (1)	Within 30 minutes	Within 4 hours
Serious (2)	Within 30 minutes	Within 8 hours
Medium (3)	Within 1 hour	Within 24 hours

CONTROL OP-9
Calls made to the Help Desk and the GIACE response statistics are reviewed in the quarterly Desk Top Service Contract review meetings.

4.5.1.6 Control Monitoring and Reporting

The overall objective of Monitoring and Reporting is to ensure that, over time, IT resources and applications continue to function as intended in accordance with contracted requirements, other standards, and legal obligations.

The responsibility for the support and maintenance of the Octopus Corp SAP environment is part of the GIACE outsource contract and a significant part of this process is undertaken by them. To a large part the Controls that are in place are those operated by the outsource organization with appropriate check points and approvals for change by authorized Octopus Corp staff.

The Control, Monitoring, and Reporting activities is focused on the creation of logs and other documentation which can be used by both GIACE staff and Octopus Corp. staff to validate the consistency and integrity of the computing environments and changes made to it.

GIACE measures the performance of each service component throughout each measurement period as listed within the SLA's and compare this with the Service Levels and Expected Availability Levels. It also provides a monthly report to Octopus. listing Service Levels or Expected Availability Levels, significant outages, any warnings of limits exceeded or potential capacity problems, complaints and steps that have been taken to reduce the chance of such failures from recurring.

CONTROL OP-10

The monthly Service Level/Expected Availability Level report warns of potential outages, capacity and other problems along with anticipated remedial actions.

4.5.2 Physical Security

GIACE's operates a central data center and office in a free standing two story office building. The computer equipment rooms are on the first floor of the building. Matters pertaining to the Data Centre were discussed with the Data Centre Manager.

4.5.2.1 Physical Security Monitoring and Control

The free standing two story office building's site enclosed within a perimeter 2 meter fence barriers on road access fitted with cameras and activated by cardkey. Windows are fitted with toughened glass fitted with "Crime Shield steel mesh" all fire exit doors are alarmed. Fire exits doors are additionally protected outside normal hours with steel shutters perimeter fence and barriers are locked outside normal hours.

Access to the site, building and the Data Centre is controlled with the use of cardkey and monitored by cameras and a 24 hour security guard presence. There are 6 control zones with computer machine rooms being a unique zone and the communications room is also a unique zone.

CONTROL PS-1
Appropriate physical security access control and monitoring policy, procedures, and mechanisms for the Data Centre are in place.

4.5.2.2 Employee, Visitor, Contractor Access Control and Monitoring

Access to any zone is on an "as authorized" and "as required" basis. Differences between Employees by job function, Visitors, and Contractors access maintained Employee, Visitor, Contractor access control and monitoring elements will be tested as part of the interviews, record inspections, and testing at the Data Centre. The subsets of these controls will be tested to provide additional granularity.

CONTROL PS-2
Access for employees and contractors is controlled by physical access control mechanisms at all access points of the facility

CONTROL PS-3
Access termination ("leavers") and new employees ("joiners") is controlled by Human Resources and that appropriate notification of are sent to management and security personnel.

4.5.2.3 Environmental Controls

Environmental Security control and monitoring is provided on an 24x7x365 basis. Electrical power supply is both protected in terms of its quality and availability with availability on a 7/24/365 basis and quality within the specified ranges of the

computing machinery connected to the protected power supply. Additionally there is a contract in place for a local vendor to provide diesel fuel if required to operate an extended period of time. The following Environmental Security control and monitoring elements were tested as part of the interviews, record inspections, and testing at the Data Centre. The subset controls were tested at this location and provide additional granularity.

CONTROL PS-4
Temperature, humidity, fire detection and water protection environmental security controls are implemented and monitored within computing machine rooms of the Data Centre**.**

CONTROL PS-5
Electrical power supply is both protected in terms of its quality and availability.

4.5.2.4 Automatic Reporting and Monitoring

The following automatic reporting and monitoring element was tested as part of the access control interviews, record inspections, and testing at the Data Centre. GIACE installed building management system that controls and monitors environmental, power, fire detection devices is in a central system and that in the event a problem is identified central security (guards) are notified.

CONTROL PS-6
GIACE installed centralized building management system that controls and monitors environmental, power, fire detection devices.

4.5.3 Logical Access

Logical Access ensures that the security elements of access are enforced. More specifically, Logical Access ensures that only authorized persons and applications have access to the data, resources, objects, tables and applications within the GIACE/Octopus Corp. environment. Logical Access also ensures that the people and/or applications only perform specifically defined activities based on their pre-defined privileges (e.g., inquire, execute, read, write, update) with regards to specific objects or resources. The primary GIACE organization responsible for management, control, monitoring and reporting of Logical Access is Systems Software Support. The key controls for logical access areas are addressed by identification, documentation and walkthrough.

Inherent within the access path are the authorization processes for granting employees, contractors, other third parties access (e.g., initial access, transfers, changes, terminations) to the path. The resources to which the users are granted access and the level of access (e.g., read, write, edit) is inherent within the access path as well as the tools used to manage the configuration settings (e.g., password controls, user controls) users access and Change controls over the tools. The Logical

Access Path:

- End User Access – Internet / Remote Access
- Network Access
- Operating System Access
- Application
- Database Environment Access

4.5.3.1 End User Access – Internet and Remote Access

The objective of GIACE's Systems Software Support activity for End User Access is to ensure a stable, reliable, and secure environment for the various applications that are run on behalf of Octopus Corp as part of its' outsource contract with Octopus Corp. Interviews occurred with GIACE Managers.

The primary focus of the End User and Internet/Remote Access for the Systems Software Support activity is Mandatory Access Control and Discretionary Access Control. A new policy that outlines security administration was approved by GIACE Origin Management that formally defines the process for granting systems access to all platforms.

CONTROL LA-1
A well defined security administration process is in place that includes appropriate approvals and an audit trail of user access approval and authorization.

CONTROL LA-2
Segregation of duties exists between those needing/wanting, approving accesses, and setting up/configuring access.

4.5.3.2 Passwords

Appropriate password structure and usage is enforced by the system. The passwords parameters are on the network are set at the operating system level (i.e. NT Windows 2000) and are also enforced by default in SAP system. Account set-up and password assignment is communicated to the user via the approved procedures.

CONTROL LA-3
Password rules, structure, and usage are enforced and apply to all users in the environment, regardless of their role.

Password rules structure and usage are enforced and apply to all users in the environment, regardless of their role. Appropriate password structure and usage is enforced by the system

CONTROL LA-4

All users are assigned their own unique ID and password and user accounts follow a consistent naming convention per the functionality of active directory.

Password rules structure and usage are enforced and apply to all users in the environment, regardless of their role. Appropriate password structure and usage is enforced by the system and have these parameter structures:

- Password Life Span = NN days. Users have to change the password at first logon and then every NN days.
- Minimum Password Length = N characters with alphanumeric values
- Password Alpha/Numeric = At least N letter character/N number
- Case Sensitive = Upper/lower case sensitive
- Password Uniqueness = N passwords
- Account Lockout = The account gets locked out after N invalid attempts.
- Lockout Duration = until unlocked by Employee support

4.5.3.3 Network Access

The objective of GIACE's Systems Software Support activity for Network Access is to ensure a stable, reliable, and secure environment for the various applications that are run over the network on behalf of Octopus Corp as part of its' outsource contract with Octopus Corp. Interviews occurred with the manager of Connectivity Technical Services.

Additionally, several other teams are responsible for different elements of GIACE's Network Security activity. More specifically, the Desktop Support team controls access to and maintains the Octopus Corp. Hub, the Network Administration Group established the standard configuration guidelines that were used to set up the CISCO routers and Access and Connectivity Services maintains the Bastion host router.

CONTROL LA-5
The network perimeter architecture consists of a layered defense of routers and firewalls

Network access security mechanisms are also utilized. These include: The use of Mandatory Access Controls including: password encryption; The Bastion host router tracking Login Id's, Passwords, IP-From, and IP-To, information; The TPG server only accepting 172.16 addresses prefixes thereby forcing all IP traffic to and from the Octopus Corp. boxes through the Bastion VPN concentrator; and all Logons to the Bastion host router requires a TACACE token. The token are only issued by GIACE-headquarters access manager.

CONTROL LA-6

A access request memo is created by the user's supervisor/department manager requesting and approving the access.

CONTROL LA-7
Audit logs are maintained for network logons and log offs and certain sensitive folders. The Network Administrator monitors and reviews these audit logs on a weekly basis.

External firewalls are configured to support automatic fail over.

4.5.3.4. Operating System

The objective of GIACE's Systems Software Support activity for Operating System Access is to ensure a stable, reliable, and secure environment for the various applications that are run within the Operating Systems run on behalf of Octopus Corp as part of its' outsource contract with Octopus Corp.

Under the outsource contract, GIACE is responsible for the application of system software patches for the Octopus Corp SAP and Local Area Network and e-mail server environments. The server support team is also responsible for Operating Systems changes, upgrades and patches; as per discussion with the team specialists.

Patches from Microsoft are centrally received with the security group. They subsequently route the information to the appropriate managers. The Internal Server Team Leader reviews them and then sends them to the client lead analyst who reviews them and in turn makes a recommendation to the Service Manager as to their disposition. The Service Support Manager then calls the client to discuss scheduling the installation of the patch.

If the client agrees that the change should take place in advance of the regularly scheduled maintenance period, a Change Request ticket is logged which formally initiates the change and tracking. If the decision is to waiting the information and disposition is complied for the monthly client service meeting for tracking purposes.

CONTROL LA - 8
There is only two persons in the IT department who has Administrator access on the network

CONTROL LA - 9
The Systems Administrator removes the access for terminated users A bi weekly termination report is received by the IT group from HR.

CONTROL LA-10
Changes to the configuration or hardware must go through the standard Change Management process by opening a help desk ticket and getting the appropriate approval from the service manager

4.5.3.5. BASIS Support

GIACE' BASIS Team handles the primary application support role and tasks. Basis Support provides for assistance with: Security Profiles, Oracle issues, SAP issues, Kernel and other transports, SAP Support Packs, and Operational Support. Operational Support includes Operation of a correction and transport system, Assisting with SAP system interface, and Assisting with set up of batch jobs, Monitoring of batch jobs and controlling the authorization process for customer transports

Basis Support also provides for: Database space management, Application of SAP kernel patches and database patches, and Daily performance monitoring. Daily support includes Daily Backup-Jobs, Daily R/3 system checks, Basis Online store Checks, Basis Business Connector Checks.

The objective of GIACE's Systems Software Support activity for Applications Database Access is to ensure a stable, reliable, and secure environment for the various applications that are run on behalf of Octopus Corp as part of its' outsource contract with Octopus Corp. Oracle is the under lying database.

The Basis team does the management of the Oracle resource. Updates/Patches come in from several sources, which include CERT, Oracle, SAP-OSS notes. The Octopus Basis lead reviews the notes and certifies they are recognized by SAP. When a patch is identified the GIACE Basis Manager discuses it with the Service manger and they discuss with client if it is critical. If not it is apart of the monthly technical report and videoconference. No Database tools other than the SAP specific are used on the Octopus Corp. account.

Once the change is applied to the environment they notify the customer and have them test/observe the environment for at least a week as a rule of thumb, prior to getting approval from the client to promote it to the next environment.

CONTROL LA-11
The passwords parameters are on the network are set at the operating system level and are also enforced by default in SAP system.

CONTROL LA-12
Oracle and SAP audit logging is implemented

4.5.4 Application Implementation and Maintenance

Changes to Octopus Corporation's applications systems are managed in accordance with the IT Quality Procedures Manual. Primary and secondary responsibility for approving changes is defined as part of the manual. The IT Quality Procedures Manual covers the SAP system as well as Exchange, Internet access, and changes to the LAN and WAN environments including servers, routers and hubs.

CONTROL ASIM-1
Steering Committees guide project work and timelines

CONTROL ASIM-2
Approval is required on all decisions to purchase or develop application systems

4.5.4.1 Process

The SAP Change Implementation Process is provided in Figure 4-3.

CONTROL ASIM-3
Access to the production environment is restricted (given only to the IT resources supporting the application) and a separation of test and production environments exists, including separation at the server level

E-mail is the medium by which SAP Change Implementation documentation is transmitted and retained. Authorization of SAP changes follows the same procedure but the authorization e-mails are stored in the SAP Enterprise Outlook Mail Box. E-mails authorizing changes other than SAP are stored in the IT Administration mail box in the appropriate Change Control Approvals sub folder according to the change type.

CONTROL ASIM-4
Project plans are developed for all major releases

CONTROL ASIM-5
An appropriate standardized methodology is used for major application system installments or upgrades

CONTROL ASIM-6
A standard migration path exists and is used for all configuration/ program changes for SAP

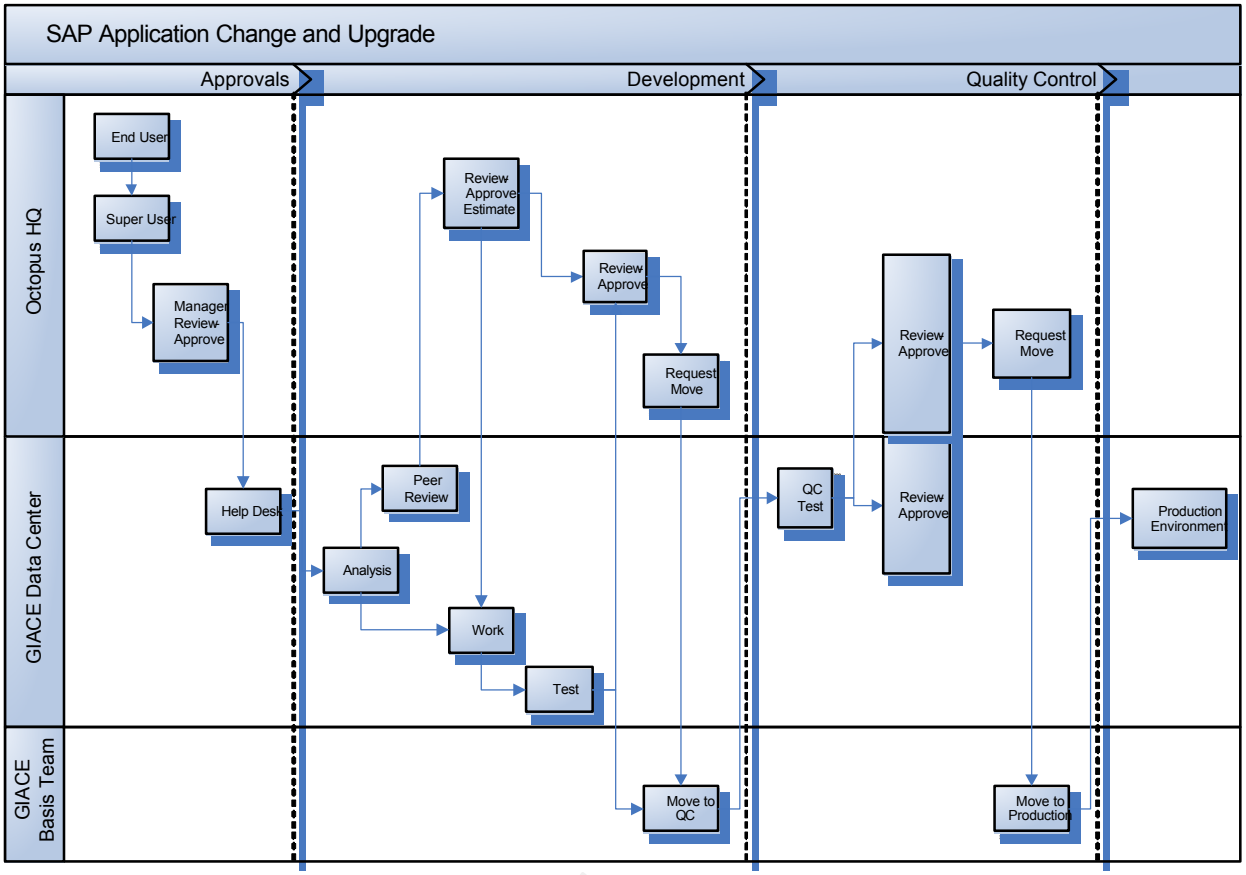


Figure 4-3 - SAP Application Change and Upgrade Process.

4.5.4.2 Change Categories

Changes are categorized as either being Major Projects, Intermediate Enhancements, or Minor Enhancements. Major Projects have a budget of more that $100,000; and an example would be an SAP Enterprise Upgrade. An Intermediate Enhancement has a budget of more that $10,000 but less that $100,000; and an example would be Electronic Trading using Spreadsheets.

4.5.4.2.1 Major Projects e.g. SAP Enterprise Upgrade

- Support to precede with an SAP Enterprise Upgrade this upgrade is given by the Commercial IT Steering Group, following which a proposal was agreed and negotiated between Octopus and GIACE management. Approval to proceed, including agreement to resource requirements, is obtained and if necessary, a capital expenditure proposal is raised and the relevant approvals obtained.
- Following approval, a Project Steering Group is set up to manage the project and ensure resources from the business were available and any issues that arose were dealt with in a timely manner.

- The development work was carried out by GIACE and the system tested in the SAP Development and the SAP QA environments against formal test scripts representing the Octopus SAP system business cases. The signed of successful trial data has been filed, as were the system status reports taken just before the old system was closed and after the new system was made operational. These status reports were checked and initial testing was carried out before the system was released for operational use. All key documentation is held in registry as an audit trail of the upgrade.

CONTROL ASIM-7
Cost/ benefit analysis is performed on all routine change requests prior to beginning any work

4.5.4.2.2 Intermediate Enhancements (Electronic Trading & Spreadsheets)

- The requirement is in line with the strategic business plan for the exploitation of eCommerce links.
- A quote was produced for the work and approval to proceed with the development given. A purchase order was raised to cover the cost of the development.
- The work was carried out by GIACE and tested in the SAP Development System by authorized staff and identifying any rework and retesting if required.
- The modification was approved and transported to production and was moved to the SAP QA environment to ensure there were no issues with the code. If the change has been one that has been identified as one that needs further trialing to ensure there are no regression issues, there would be further testing carried out in QA at this stage.
- Upon successful testing in QA the change would be signed off and then moved to the SAP Production environment.

4.5.4.2.3 Minor Enhancements (Addition of data field to a ship address)

- The process for approving the work to be carried out, testing and moving to production is as above. Payment of these Minor Enhancements will normally be made against a call off order rather than a specific one raised specifically to cover the package of work.

CONTROL ASIM-8
Approved projects are logged into the tracking software and updated throughout their lifecycle

CONTROL ASIM-9
Changes requests are logged and tracked to completion in the tracking system

4.5.4.3 Testing

The process for testing the requested changes to the system is outlined in the process map Additionally, the volume of changes, by category to the Production SAP environment for the period of 1/1/04 to 9/21/04 was limited and effected the sampling available to be tested. The summary of all changes for this period was:

- Small Changes =0
- Medium Changes = 15
- Large Changes = 0
- Mini Projects = 0
- Fast Track (Basis) = 19
- Total Changes = 34

CONTROL ASIM-10
A standard testing methodology is used in all SAP application upgrades

CONTROL ASIM-11
All SAP program changes are user acceptance tested and approved prior to implementation into PROD

4.5.4.4 Enhancement Change Process

A Change Request come into the system via the Help desk from a Super User and is logged using an "NL" number for tracking. A GIACE analyst assigned to the Octopus account reviews the enhancement request and determines which Change Category (section 4.5.4.2) it falls into. Based on this category, a standard set of procedures is used.

If the change is determined to be medium or higher an estimate is required to be completed. Based on the analysis the change is then estimated and reviewed by a peer. Upon completion of the work estimate it is forwarded to the SAP service manager for a discussion with the client. If the client approves the estimate work is commenced. Separate environments are maintained for development, Test and QA and finally Production.

E-mail with details of estimates will be sent to SAP Enterprise mailbox and approvals will be copied to SAP Enterprise mailbox. Work will be carried out if subject an estimate when the estimate has been approved. The modification will be tested in Development environment and the tests will be documented. If QA testing has been identified as being required, the IT Systems Application Manager will approve the modification for transported to QA and the tests will be carried out according to the test

plan and documented.

If testing is successful, the modification will be approved for transport to production, via QA if only Dev testing has been necessary, and an e-mail sent to Atos Origin copied to the SAP Enterprise mailbox. The IT Systems Application Manager will update any local working practices and arrange training as necessary. Following successful use in production environment, the modification will be signed off by sending an e-mail to the Support Manager copied to the SAP Enterprise mailbox.

CONTROL ASIM-12
Test scripts used in SAP application upgrades are documented

CONTROL ASIM-13
End user, operations, and technical documentation is updated as part of large application upgrade

CONTROL ASIM-14
CTS numbers are automatically generated when a configuration or program change is made in SAP

CONTROL ASIM-15
Post implementation, all technical documentation relating to emergency changes is updated

4.5.5. SAP Production Backup and Recovery

Backup for the all Octopus Corp. SAP processes are controlled by GIACE locally at the GIACE Data Centre, per discussion with the Internal Sever Team Leader. GIACE's Back-Up tape vault is a separate room in their Data Centre. The door is controlled by a manual cipher lock whose combination is known only to the tape operators and the Data Centre Manager.

CONTROL BR 1
Written procedures governing the back up tape handling policy are included in the Work Instruction: Dispatch of Magnetic Media to the Off Site Store, Work Instruction: Octopus Corp. SAP/NT RNH2KBU1 Tape Changing and Work Instruction: Receipt of Magnetic Media From The Off-Site Store

A full volume backup of the Octopus Corp. production SAP system is done each weekday (except weekends). Additionally the transaction logs baked up at lunchtime every day. Each day's tapes are locked in a metal case that is picked up by a courier from RS, the offsite media storage facility company. The off site storage facility operates 24hrs, 365 days a year. RS is ISO-9001 registered.

4.5.5.1 SAP Production Backup and Recovery Scheduling

The daily scheduled off site movement of the tapes is coordinated by the Data Centre operators and supervised by the Data Center Manager. Tapes are picked up and delivered by a courier of RS for offsite media storage. All tapes are labeled and sent offsite in a locked aluminum transit case and only GIACE staff has the case's keys.

Every morning, backup/archive tapes from the previous night are logged, inventoried, and locked in a metal case as part of the case packing process prior to the pickup by the RS courier. The RS courier both picks up the current day's cases and delivers the prior weeks case. The cases are sequentially numbered to reflect the day of the week and alternatively inbound and outbound status. An "A-B" scheme is used which provides for the two week cycle rotation i.e. a – is week one and b – is week two and then it starts over again. Each workday, the prior night's tapes are logged and inventoried as part of the case packing process.

CONTROL BR-2
Logs and inventory records of the tapes are reviewed for completeness and accuracy before the metal case is closed and locked.

RS stores the metal case in their secure facility for one week and then returns it to GIACE. GIACE operators unpack the case and shelve the tapes in the appropriate designated area. The tapes are kept for another two (2) weeks and then re-cycled by over-writing them with a new backup. The storage facility is a safe, secure and confidential environment, totally enclosed in secure fencing with electronically controlled access gates, 24hr internal and external CCTV, equipped with automatic fire suppression and is fully climate controlled.

Daily collection and delivery service for media storage. Couriers are RS staff; all vehicles are unmarked, carry mobile communications and are fitted with tracker systems. Paper records of collection & deliveries are obtained each day and retained by Operations for a minimum of 12 months. Emergency recovery of media is within 2 hours of being requested by operations. Tapes are inventoried as part of the case packing process and checked upon receipt from the RS courier and the tape placed in the designated racks

CONTROL BR-3
Production backup jobs are reviewed as a part of the daily checks conducted by Data Centre operators and Management

4.5.5.2 SAP Production Backup and Recovery Testing

Periodic tests are conducted to help ensure stored backup data can be used successfully for recovery.

CONTROL BR-4
A Periodic test, approximately every 6 months is conducted.

4.6 Testing Summaries

The test workpaper set documents the tests of the controls that are identified in Sections 4.5.1 through 4.5.5. These workpapers are provided in Appendix D and are summarized in this section, below. These summaries are also an important part of the overall audit workpaper package as can also be seen in Table 4-5, Workpaper Index, provided in Section 4.7.

4.6.1 Operations Testing Summary

CONTROL ID	CONTROL	SAMPLE SIZE	TEST PURPOSE	RESULTS OF TESTING PERFORMED	EFFECTIVE?	ACTION PLAN
OP-1	Standard Monitoring and Control documents are regularly used to standardize and document processes and activities.	1	Obtain evidence of Monitoring and Control documents	The monthly management meeting is documented by the monthly technical report. The Minutes of these monthly meetings are prepared and distributed to attendees and authorized distribution list. The chair of the meeting is the Owner of the distribution list.	Y	None Required No Exceptions Noted
OP-2	The GIACE facility is a registered BS7799/ISO 9001:2000 site.	1	Obtain evidence of current and valid registration	BS7799/ISO 9001:2000 site status is documented	Y	None Required No Exceptions Noted
OP-3	SAP R3 Scheduling tools are used for the production of schedules.	1	Obtain evidence that R3 Scheduling tools are used for the production schedules. Confirm for a successful job completion.	Confirmed evidence of R3 Scheduling tools in use for the production schedules and confirmed a successful job completion.	Y	None Required No Exceptions Noted
OP-4	SAP date/time stamp all job modification transaction and records the job properties	1	Review the properties tab for one job in the R3 scheduler and obtain evidence of modification history	Confirmed the properties tab for one job in the R3 scheduler and obtained evidence of modification history.	Y	None Required No Exceptions Noted
OP-5	A limited number of manual jobs can be initiated by end users in SAP	1	Verify Internal SAP control over job modification is working as designed	Verified that Internal SAP control over job modification is working as designed	Y	None Required No Exceptions Noted
OP-6	Job changes (add or modify) are made and tested in a test environment separate from production.	1	Sample job changes and validate that proper testing prior to introduction into production occurred.	Verified job changes (add or modify) are made and tested in a test environment separate from production.	Y	None Required No Exceptions Noted

OP-7	For new R3 job plans, a test of the program and parameter is performed in QA ensure proper combination	1	Sample of recent R3 job changes, obtain evidence of testing in QA.	Evidence of testing in QA found and verified	Y	None Required No Exceptions Noted
OP-8	For production systems, a manual daily check is carried out. This identifies any problems that have occurred since the last check.	1	Verify that a manual daily check identifies any problems that have occurred since the last check including any job "abends."	A manual daily check occurs and identifies any problems	Y	None Required No Exceptions Noted
OP-9	Calls made to the Help Desk and the GIACE response statistics are reviewed in the quarterly Desk Top Service Contract review meetings.	1	Verify that a manual check of the response statistics are reviewed in the quarterly Desk Top Service Contract review meetings	Verified that the response statistics reviewed in the quarterly Desk Top Service Contract are reviewed in the quarterly review meetings	Y	None Required No Exceptions Noted
OP-10	The monthly Service Level/Expected Availability Level report warns of potential outages, capacity and other problems along with anticipated remedial actions.	3	Confirm that Octopus receives a monthly report listing Service Levels or Expected Availability Levels.	Documented by the monthly technical report. The monthly reports are prepared and distributed to authorized distribution list. The chair of the meeting is the Owner of the distribution list.	Y	None Required No Exceptions Noted

4.6.2 Physical Security Testing Summary

CONTROL ID	CONTROL	SAMPLE SIZE	TEST PURPOSE	RESULTS OF TESTING PERFORMED	EFFECTIVE?	ACTION PLAN

PS-1	Appropriate physical security access control and monitoring policy, procedures, and mechanisms for the Data Centre are in place.	1	Validate the physical security access control and monitoring policy, procedures, and mechanisms	Site enclosed within a perimeter 2 meter fence barriers on road access fitted with cameras and activated by cardkey. 24 hour security guard presence on site external cameras with remote monitoring service. Windows are fitted with toughened glass fitted with "Crime Shield steel mesh" all fire exit doors are alarmed. Fire exits doors are additionally protected outside normal hours with steel shutters perimeter fence and barriers are locked outside normal hours. Access to the building and the Data Centre is controlled with the use of cardkey and zones allocated as required to authorized staff only. There are 6 control zones with computer machine rooms being a unique zone and the communications room also being a unique zone.	Y	None Required No Exceptions Noted
PS-2	Access for employees and contractors is controlled by physical access control mechanisms at all access points of the facility	AL L	Validate the access control and monitoring elements by conducting interviews, record inspections, and testing.	Procedures exist for authorizing access to secured areas, computer room and prevent unauthorized access. Employee's manager collects access cards and keys and forwards them to the Property Mgmt. at the time of termination. New employee must attend an orientation meeting and sign an agreement of understanding of the facilities policies and d procedures Access request have to be approve by line manger. Procedures exist for providing access to the data centre to third parties	Y	None Required No Exceptions Noted
PS-3	Access for terminated and new employees is controlled by HR that notifications are sent to management and security personnel.	AL L	Confirm that an access list of employees is controlled by Human Resources and that appropriate notification of new employees and departing employees is sent to management and security personnel.	Human Resources provides a list of terminated employees and access is reviewed on a periodic basis. The Data Centre Manger reviews the access log looking for violation patterns.	Y	None Required No Exceptions Noted

PS-4	Temperature, humidity, fire detection and water protection environmental security controls are implemented and monitored within computing machine rooms of the Data Centre.	1	Confirm that temperature, humidity, fire detection and water protection environmental security controls are implemented and monitored within computing machine rooms of the Data Centre.	The rooms are configured with internal movement sensors and cameras installed structured cabling pre-laid under floor power distribution points strategically positioned around the rooms. Water sensors are in place in the sub floor. All plumbing is located central to the workspace and not overhead of any machine room resources. Conventional fire detectors installed with visual & audible alarm for immediate response. Fire extinguishers are readily available. Temperature & humidity controlled	Y	None Required No Exceptions Noted
PS-5	Electrical power supply is both protected in terms of its quality and availability.	1	Validate servers in data centre are connected to UPS and backup generator is available 24x7x365	The machine rooms are divided into two wings South and Power is supplied from national grid to transformer into 2 supplies to data centre with automatic cutover UPS installed backup generator installed A backup generator is run up to operating temperature & speed once each week, and a full load once per year for 30 minutes.	Y	None Required No Exceptions Noted
PS-6	GIACE installed centralized building management system that controls and monitors environmental, power, fire detection devices.	1	Validate the installed automated building control, management and monitoring system for power, fire and water detection, and air conditioning.	Confirmed that GIACE has installed an automated building control, management and monitoring system for power, fire and water detection, and air conditioning.	Y	None Required No Exceptions Noted

4.6.3 Logical Access Testing Summary

CONTROL ID	CONTROL	SAMPLE SIZE	TEST PURPOSE	RESULTS OF TESTING PERFORMED	EFFECTIVE?	ACTION PLAN
LA-1,	A well defined security administration process is in place that includes appropriate approvals and an audit trail of user access approval and authorization.	All	Review for reasonableness the security administration process for Octopus network access.	Security administration process for Octopus network access is in place that includes appropriate approvals and an audit trail of user access approval and authorization.	Y	None Required No Exceptions Noted
LA-2	Segregation of duties exists between those needing/wanting, approving accesses, and setting up/configuring access.	All	Validate for a sample of employees with network access that segregation of duties was maintained in the setup process.	Segregation of duties exists and is maintained between those approving accesses, and setting up/configuring access.	Y	None Required No Exceptions Noted
LA-3,	Password rules, structure, and usage are enforced and apply to all users in the environment, regardless of their role.	25 or 25	Validate password parameters are enforced and obtain documentation showing where those options are configured for systematic enforcement upon new account setup	Review all key transaction identified and noted only two exceptions and two with reasonable business requirements for the access to key transaction that appear to be incompatible.	Y	None Required No Exceptions Noted
LA-4	All users are assigned their own unique ID and password and user accounts follow a consistent naming convention per the functionality of active directory.	25 or 25	Obtain listing of all employees with network accounts. Select sample and validate unique ID and standard naming convention.	Active directory precludes the reuse of a user id No exception noted	Y	None Required No Exceptions Noted
LA-5	The network perimeter architecture consists of a layered defense of routers and firewalls	All	Review network architecture diagram for reasonableness.	Network perimeter architecture includes: Router passwords are encrypted, External firewalls are configured to support automatic failover, Firewall configuration is performed using encryption protocols.	Y	None Required No Exceptions Noted
LA-6	A access request memo is created by the user's supervisor or department manager requesting and approving the access	All	Verify that an access request memo is created by the user's supervisor or department manager for all new access requests	Access request memos are created for all new users	Y	None Required No Exceptions Noted

LA-7	Audit logs are maintained for network logons and log offs and certain sensitive folders. The Network Administrator monitors and reviews these audit logs on a weekly basis.	All	Obtain examples of each type of audit log. Determine how review is performed and what evidence is maintained on the review.	Audit logs of events are reviewed.	Y	None Required No Exceptions Noted
LA-8	There are only two persons in the IT department who has Administrator access on the network	All	Obtain listing of all employees with SAP access. Validate that only two employees have administrator rights.	Listing of all employees with SAP access validated that only two employees have administrator rights.	Y	None Required No Exceptions Noted
LA-9	The Systems Administrator removes the access for terminated users A bi weekly termination report is received by the IT group from HR	All	Obtain 6 months of copies of HR reports to validate existence. Select sample of terminated employees and validate that each terminated employee's user's account was deactivated.	SAP users have access to data only through the SAP application. All other access is restricted at the root level through AIX and Oracle where only system administrators have access	Y	None Required No Exceptions Noted
LA-10	Changes to the configuration or hardware must go through the standard Change Management process by opening a help desk ticket and getting the appropriate approval from the service manager	All	Verify that a Help Desk ticket is generated and that the Service Manager contacts the client for approval as part of the standard Change Management process.	Help Desk ticket is generated per Change Management process	Y	None Required No Exceptions Noted
LA-11	The passwords parameters are on the network are set at the operating system level and are also enforced by default in SAP system	25 or 25	Verify that the password parameters are on the network are set at the operating system level and are also enforced by default in SAP system	Password parameters are on the network are set at the operating system level and are also enforced by default in SAP system.	Y	None Required No Exceptions Noted
LA-12	Oracle and SAP audit logging is implemented	25 or 25	Verify that Oracle and SAP audit logging is implemented	Oracle and SAP audit logging are implemented	Y	None Required No Exceptions Noted

4.6.4 Applications Testing Summary

CONTROL ID	CONTROL	SAMPLE SIZE	TEST PURPOSE	RESULTS OF TESTING PERFORMED	EFFECTIVE?	ACTION PLAN

ASIM-1	Steering Committees guide project work and timelines	25 or 25	For each major project in sample, validate that a Steering Committee exists and meets regularly. Document members and frequency of meeting schedule. Obtain as evidence last agenda and/or meeting minutes.	None during audit period, however, Other periods have R/3 upgrade minutes and approval memos	Y	None Required No Exceptions Noted
ASIM-2	Approval is required on all decisions to purchase or develop application systems	25 or 25	Select sample of new purchases or developments between 1/1/04 and 7/31/04. Validate that for each formal management approval evidence is available	None during audit period Other periods have R/3 approval memos.	Y	None Required No Exceptions Noted
ASIM-3	Access to the production environment is restricted (given only to the IT resources supporting the application) and a separation of test and production environments exists, including separation at the server level.	25 or 25	Obtain listing of all users with PROD access for both and SAP applications. Validate that production access is restricted appropriately. For each Oracle instance, validate test instance resides on separate server from production instance	Cross Reference – Logical Security	Y	None Required No Exceptions Noted
ASIM-4	Project plans are developed for all major releases.	25 or 25	Using same sample, validate project plans exist. Review for completeness.	Cross Reference – "Controlling Enhancements" Test Matrix	Y	None Required No Exceptions Noted
ASIM-5	An appropriate standardized methodology is used for major application system installments or upgrades.	25 or 25	Using same sample, validate standard methodology used on project.	Cross Reference – "Controlling Enhancements" Test Matrix	Y	None Required No Exceptions Noted
ASIM-6	A standard migration path exists and is used for all configuration/ program changes for SAP.	25 or 25	For sample of changes, validate that each followed migration path.	ASIM Test Matrix	Y	None Required No Exceptions Noted
ASIM 7	Cost/ benefit analysis is performed on all routine change requests prior to beginning any work	25 or 25	Determine if cost/ benefit documentation exists for a sample of routine changes drawn from report(s) of all changes made to operating environments	Obtained listing and validated that Help Desk ticket was logged for all active projects.	Y	None Required No Exceptions Noted
ASIM-8	Approved projects are logged into the tracking software and updated throughout their lifecycle	25 or 25	Determine if a Help Desk ticket was logged for all active projects	Obtained listing and validated that Help Desk ticket was logged for all active projects.	Y	None Required No Exceptions Noted
ASIM-9	Changes requests are logged and tracked to completion in the tracking system	25 or 25	For sample of changes, validate that each has a corresponding Help Desk ticket.	Validated that Help Desk ticket logs are generated	Y	None Required No Exceptions Noted

ASIM-10	A standard testing methodology is used in all SAP application upgrades	25 or 25	Obtain documented tested methodology. For sub section of project in original sample, validate that testing methodology is evident in corresponding project plan.	Cross Reference – "Controlling Enhancements"	Y	None Required No Exceptions Noted
ASIM-11	All SAP program changes are user acceptance tested and approved prior to implementation into production	25 or 25	Obtain report of all changes made to and SAP environment between 1/1/04 and 7/31/04. Validate that for each: Evidence of user acceptance testing prior to move to production. Standard migration path was used (dev/test, QA, Prod), and Corresponding Help Desk ticket exists	Cross Reference – Test Matrix		None Required No Exceptions Noted
ASIM-12	Test scripts used in SAP application upgrades are documented	25 or 25	Obtain documented test scripts for both applications. Select sample and review for reasonableness.	No evidence of for enhancement; tdid use as part of upgrade		Not Key, None
ASIM-13	End user, operations, and technical documentation is updated as part of large application upgrade	25 or 25	Select sample of all three types of documentation for projects that have occurred this year. Review and determine that it is accurate.	Cross Reference - Operations	Y	None Required No Exceptions Noted
ASIM-14	CTS numbers are automatically generated when a configuration or program change is made in SAP	25 or 25	Walkthrough the change of one program. Validate that the CTS number is automatically generated	No evidence found		Not Key, None
ASIM-15	Post implementation, all technical documentation relating to emergency changes is updated	25 or 25	Obtain copy of change control procedures. Validate that there is a "checklist" for emergency changes and that updating appropriately documentation is included in that list.	No evidence found *NOT KEY*:		Not Key, None

4.6.5 Back-Up and Recovery Testing Summary

CONTROL ID	CONTROL	SAMPLE SIZE	TEST PURPOSE	RESULTS OF TESTING PERFORMED	EFFECTIVE?	ACTION PLAN

BR 1	Written procedures governing the back up tape handling policy are included in the Work Instruction: Dispatch of Magnetic Media to the Off Site Store, Work Instruction: Octopus Corp. SAP/NT RNH2KBU1 Tape Changing and Work Instruction: Receipt of Magnetic Media From The Off-Site Store	All	Obtain copy of document retention policy and/or procedures and review and validate for reasonableness and completeness.	Procedure was Appropriate Tape Inventory had no exceptions. Noted no exceptions	Y	None Required No Exceptions Noted
BR 2	Logs and inventory records of the tapes are reviewed for completeness and accuracy before the metal case is closed and locked.	All	Obtain evidence of logs, review and validate.	Procedure was Appropriate. Noted no exceptions	Y	None Required No Exceptions Noted
BR 3	Production backup jobs are reviewed as a part of the daily checks conducted by Data Centre operators and Management	All	Obtain evidence of backup & recovery taps are delivered to the tape vault. Validate the tape logging, packing and case locking prior to pick up by the courier.	Obtained e-mails that evidenced the checks were done and that that day's backups were successful. Procedure was Appropriate. Noted no exceptions	Y	None Required No Exceptions Noted
BR 4	A Periodic test, approximately every 6 months is conducted.	All	Obtain evidence of backup & recovery tests performed in last year and validate that a sufficient sampling of locations, applications and supporting platforms have been recovered successfully	Obtained evidence that backup tests would provide a successful recovery.	Y	None Required No Exceptions Noted

4.7 Report To Management

The SOX-404 workpaper contributions that the IT Auditor would make to the overall SOX audit are summarized by the workpaper index in Table 4-5 – Workpaper Index. The workpaper reference number (#) in the index refers to the paragraph number in section 4.0 or to the paragraph number in Appendix- D, "Test Workpaper." Appendix E provides several selected screenshots (etc.) from the audit that could be sanitized and retain their purpose.

OPERATIONS	
WP Ref #	**Workpaper**
4.5.1	Operations Narrative with Controls
4.6.1	Operations Test Summary and Results
D-1.1	OS Test Sheet 1 Results
D-1.1a	Monthly Report
D-1.1b	Service Review Meeting Minutes
D-1.2	OS Test Sheet 2
D-1.3	OS Test Sheet 3, 4
D-1.4	OS Test Sheet 5, 6, 7, 8
D-1.5	OS Test Sheet 9
D-1.5a	Checks report log
D-1.5b	Checks report screenshot
D-1.5c	System checks information
D-1.6	OS Test Sheet 10
D-1.6a	Monthly Support Calls Report
PHYSICAL SECURITY	
WP Ref #	**Workpaper**
4.5.2.	Physical Security Narrative with Controls
4.6.2	Physical Security Test Summary and Results
D-2.1	PS Test Sheet 1
D-2.1a	Procedure for Gaining Access to Machine Rooms
D-2.1b	Cardkey Access Doors
D-2.1c	Data Center Access Procedure
D-2.1d	Acknowledge Data Center Access Procedure certification
D-2.2	PS Test Sheet 2, 3
D-2.2a	Data Center Access Control Log Sheet
D-2.2b	New Hire Memo, Induction Process
D-2.2c	Terminated Access Memo

D-2.2d	HR Administration process for recruitment
D-2.2e	Annual Review of access reports
D-2.3	PS Test Sheet 4, 5
D-2.3a	Personnel with Access Change List Test
D-2.3b	Audit List
D-2.3c	Cardholder Records by Access Level
D-2.4	PS Test Sheet 6

LOGICAL ACCESS

WP Ref #	Workpaper
4.5.3.	Logical Access Narrative with Controls
4.6.3	Logical Access Test Summary and Results
D-3.1	LA Test Sheet 1, 2
D-3.1a	Security Policy
D-3.1b	Segregation of Duties
D-3.2	LS Test Sheet 3, 4
D-3.2a	System settings for passwords
D-3.3	LS Test Sheet 5, 6, 7
D-3.4	LS Test Sheet 8, 9, 10
D-3.5	LS Test Sheet 11, 12

APPLICATIONS (ASIM) ACCESS

WP Ref #	Workpaper
4.5.4.	Applications (ASIM) Narrative with Controls
4.6.4	Applications (ASIM) Test Summary and Results
D-4.1	ASIM Test Sheet 1, 2
D-4.1a	Security Policy
D-4.1b	Segregation of Duties
D-4.2	ASIM Test Sheet 3, 4, 5, 6
D-4.2a	System settings for passwords
D-4.3	ASIM Test Sheet 7, 8, 9
D-4.4	ASIM Test Sheet 10, 11
D-4.5	ASIM Test Sheet 12, 13, 14, 15

BACKUP AND RECOVERY

WP Ref #	Workpaper
4.5.5.	Logical Access Narrative with Controls
4.6.5	Logical Access Test Summary and Results
D-5.1	BR Test Sheet 1

D-5.1a	Work Instruction: Dispatch of Magnetic Media to the Off Site Store
D-5.1b	Work Instruction: Terra SAP/NT RNH2KBU1 Tape Changing
D-5.1c	Work Instruction: Receipt of Magnetic Media From The Off-Site Storage
D-5.2	BR Test Sheet 2, 3
D-5.2a	Tape Inventory Sheet ("UNIX BOXES") Test results
D-5.2b	SAP/NT RNH2KBU1 SAP Job Check Screen Shots
D-5.2c	System Checks screenshots and checks report
D-5.3	BR Test Sheet 4

Table 4-5 – Workpaper Index

Any memoranda on any deficiencies, remediation or recommended actions are beyond the scope of this report since they would require incorporating material that was removed during sanitization process. Additionally, management decided not to use a SAS 70 report.

The final outcome of the SOX-404 audit was Octopus was properly prepared for the arrival of its outside, independent financial auditors.

END NOTES

[1] This site: *Sarbanes-Oxley Public Company Accounting Reform and Investor Protection Act of 2002*, provides an extensive, although not exhaustive, set of links and other references and to a variety of Sarbanes-Oxley information. The stated purpose of the site is to help "…firms to stay abreast of the proposed and final rules and regulations issued by the SEC to implement the Act (SOX)" by providing an "index of SEC filers, audit firms, offices, CPAs, services, fees, SEC enforcement actions and other critical disclosure information."

[2] Both Octopus Corporation and GIAC Enterprises are real company. Their identities are disguised for inclusion in this paper. Certain facts about them have also been modified to maintain the disguise although these changes do not materially change the basic issues presented in this paper.

[3] Bartos, James M., "*Sorting the Wheat From the Chaff*," the European Lawyer, pg22-23, September 2002

[4] *"U.S. Corporate-Disclosure Law Confuses Lawyers Outside U.S."*, News Release, *LexisNexis and* International Bar Association (IBA), September 15, 2003

[5] Lawrence A. Cunningham, "*Sarbanes-Oxley and All That: Impact Beyond America's Shores,"* Boston College Law School Lectures and Presentations, Boston College Law School, June 2003 (Speech delivered to the Federation of European Securities Exchanges' 7th European Financial Markets Convention in London)

[6] Multiple BS-7799 information citations are available. These two are typical*: "How 7799 Works,"* http://www.gammassl.co.uk/bs7799/works.html and "The ISO 17799 Directory," http://www.iso-17799.com/.

[7] A Summary of the Section Titles of Sarbanes-Oxley Act of 2002, as provided by the AICPA, is included in Appendix A. It is Section 404 that is of particular interest to IT Security and IT Audit Professionals.

[8] Worthen, Ben, "*Your Risks and Responsibilities*," CIO Magazine, May 15, 2003

[9] Logan, Debra, Mogull, Rich, "*Sarbanes-Oxley: The Role of Technology*," CIO Magazine, J*une 22, 2004*

[10] Hoffman, Thomas. "*The Sarb-Ox Shift*," COMPUTERWORLD, January 31, 2005

[11] Summary of Sarbanes-Oxley Act of 2002, published by The American Institute of Certified Public Accountants, http://www.aicpa.org

[12] American Institute of Certified Public Accountants (AICPA), *Audit Risk and Materiality in Conducting an Audit (SAS 47),*1983.

[13] Ibid, "*Communication of Internal Control Structure Related Matters Noted in an Audit (SAS 60)*." 1988.

[14] op cit, "*Consideration of the Internal Control Structure in a Financial Statement Audit (SAS 55),"* 1988

[15] op cit, "*Consideration of the Internal Control Structure in a Financial Statement Audit (Audit Guide for SAS 55)*," 1990.

[16] op cit, *"Reporting on an Entity's Internal Control Structure over Financial Reporting (Statement on Standards for Attestation Engagements 2),"* 1993.

[17] op cit, *"Consideration of Internal Control in a Financial Statement Audit: An Amendment to SAS No. 55"* (SAS 78)," 1995.

[18] Institute of Internal Auditors, Global Technology Audit Guide (GTAG). See its site at: http://www.theiia.org/index.cfm?doc_id=4706

[19] The GAO focuses on governmental issues. See its site at: *www.gao.gov*

[20] Information Systems Audit and Control Association (ISACA). *COBIT: Control Objectives for Information and related Technology*. 1995.

[21] U.S. Public Company Accounting Oversight Board (PCAOB). See its site at: http://www.pcaob.com/index.php

[22] Institute of Internal Auditors Research Foundation (IIARF), *Systems Auditability and Control*, 1991, revised 1994.

[23] COSO, or "The Committee of Sponsoring Organizations of the Treadway Commission" states its mission on its homepage as being "… a voluntary private sector organization dedicated to improving the quality of financial reporting through business ethics, effective internal controls and corporate governance." http://www.coso.org/

[24] IT Governance Institute (*www.itgi.org*)

[25] *IT Control Objectives For Sarbanes-Oxley*, ISACA, April 2004, http://www.isaca.org/Content/ContentGroups/Research1/Deliverables/IT_Control_Objectives_for_Sarbanes-Oxley_7july04.pdf

[26] Ibid, pg 17.

[27] op cit, pg. 57

[28] There are a number of NIST publications that are of particular interest to IT auditors in general and SOX 404 auditors in particular. See the library index at http://csrc.nist.gov/publications/index.html

[29] The ISO 17799 Directory, See their web page at: http://www.iso-17799.com/index.htm

[30] International Organization for Standardization. See their web page at: www.iso.org/

[31] *"IT Control Objectives for Sarbanes Oxley*," ITGI, July, 2004, Pg. 6, http://www.isaca.org/Content/ContentGroups/Research1/Deliverables/IT_Control_Objectives_for_Sarbanes-Oxley_7july04.pdf

[32] Colbert, Janet L, Ph.D., and Bowen, Paul L., Ph.D., "*A Comparison of Internal Controls: COBIT, SAC, COSO and SAS 55/78,"* Information Systems Audit and Control Association, July 2004, Pg. 1-2, http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=8174&TEMPLATE=/ContentManagement/ContentDisplay.cfm,

[33] Webster's 9Th New Collegiate Dictionary, Merriam-Webster, Springfield, MA 1991

[34] Morris, William Thomas, Engineering Economic Analysis, 1976, Reston

Publishing Co. Reston, Va.

[35] Ibid, *"Evaluating Outcomes – Multiple Criteria*," pp 154 - 179

[36] op cit, "*Risk Analysis,"*. pp 235-263Morris provides a more robust mathematical structure to variety of decision analyses.

[37] Topmiller, D. A., "*Methods: Past Approaches, Current Trends, and Future Requirements*," Manned System Design, Moraal, J. & Kraiss, K., ed., 1981, Plenum Press, NY,NY, pp. 3 - 32,

[38] "*COSO Releases New ERM Framework,*" The Institute of Internal Auditors, Inc., http://www.theiia.org/?doc_id=4907

[39] COSO site, www.coso.org

[40] Scalet, Sarah D., "*A New Guide to Risk,*" CIO Magazine, Nov. 15, 2004, http://www.cio.com/archive/111504/tl_risk.html

[41] Berinato, Scott, "*Risk's Rewards,*" CIO Magazine, Nov 1, 2004, http://www.cio.com/archive/110104/risk.html

[42] Seider, Daniel, "*Decision Assistance Techniques For System Development*," Conference Proceedings, AFCEA, 1985, pp. 2-5

[43] Ibid, p. 6

[44] op cit , p.10

[45] Ostrofsky, Benjamin, Design, Planning and Development Methodology, Prentice Hall, Englewood Cliffs, NJ., 1977

OTHER REFERENCES

1. The COSO Internal Control Integrated Framework, AICPA product order number 990012kk at *www.cpa2biz.com*
2. SEC Rules on Section 404, *www.sec.gov/rules/final/33-8238.htm*
3. PCAOB Standard No. 2, *www.pcaobus.org/rules/Release-20040308-1.pdf*
4. Sarbanes-Oxley Act of 2002, The United States Congress (2002), The Sarbanes-Oxley Act (H.R. 3763). *http://www.law.uc.edu/CCL/SOact/toc.html*
5. AICPA Antifraud & Corporate Responsibility Center, *www.aicpa.org/antifraud/*
6. AICPA Audit Committee Effectiveness Center, *http://www.aicpa.org/audcommctr/homepage.htm*

APPENDIX - A, Summary of Sarbanes-Oxley Act of 2002

Section 101	Establishment; Duties Of The Board.
Section 103	Auditing, Quality Control, And Independence Standards And Rules.
Section 102(a)	Mandatory Registration
Section 102(f)	Registration And Annual Fees.
Section 109(d)	Funding; Annual Accounting Support Fee For The Board.
Section 104	Inspections of Registered Public Accounting Firms
Section 105(b)(5)	Investigation And Disciplinary Proceedings; Investigations; Use Of Documents.
Section 105(c)(2)	Investigations And Disciplinary Proceedings; Disciplinary Procedures; Public Hearings.
Section 105(c)(4)	Investigations And Disciplinary Proceedings; Sanctions.
Section 105(d)	Investigations And Disciplinary Proceedings; Reporting of Sanctions.
Section 106	Foreign Public Accounting Firms.
Section 107(a)	Commission Oversight Of The Board; General Oversight Responsibility.
Section 107(b)	Rules Of The Board.
Section 107(d)	Censure Of The Board And Other Sanctions.
Section 107(c)	Commission Review Of Disciplinary Action Taken By The Board.
Section 108	Accounting Standards.
Section 201	Services Outside The Scope Of Practice Of Auditors; Prohibited Activities.
Section 203	Audit Partner Rotation.
Section 204	Auditor Reports to Audit Committees.
Section 206	Conflicts of Interest.
Section 207	Study of Mandatory Rotation of Registered Public Accountants.
Section 209	Consideration by Appropriate State Regulatory Authorities.
Section 301	Public Company Audit Committees.
Section 302	Corporate Responsibility For Financial Reports.
Section 303	Improper Influence on Conduct of Audits
Section 304	Forfeiture Of Certain Bonuses And Profits.
Section 305	Officer And Director Bars And Penalties; Equitable Relief.
Section 305	Officer And Director Bars And Penalties.
Section 306	Insider Trades During Pension Fund Black-Out Periods Prohibited.
Section 401(a)	Disclosures In Periodic Reports; Disclosures Required.
Section 401 (c)	Study and Report on Special Purpose Entities.
Section 402(a)	Prohibition on Personal Loans to Executives.
Section 403	Disclosures Of Transactions Involving Management And Principal Stockholders.
Section 404	Management Assessment Of Internal Controls.
Section 407	Disclosure of Audit Committee Financial Expert.
Section 409	Real Time Disclosure.
Section 501	Treatment of Securities Analysts by Registered securities Associations.
Section 601	SEC Resources and Authority.
Section 602(a)	Appearance and Practice Before the Commission.
Section 602(c)	Study and Report.
Section 602(d)	Rules of Professional Responsibility for Attorneys.
Section 701	GAO Study and Report Regarding Consolidation of Public Accounting Firms.
Title VIII	Corporate and Criminal Fraud Accountability Act of 2002.
Title IX	White Collar Crime Penalty Enhancements
Section 1001	Sense of Congress Regarding Corporate Tax Returns
Section 1102	Tampering With a Record or Otherwise Impeding an Official Proceeding
Section 1103	Temporary Freeze Authority

APPENDIX - B, Components of Enterprise Risk Management

Enterprise risk management consists of eight interrelated components. These are derived from the way management runs an enterprise and are integrated with the management process. These components are:

- *Internal Environment* – The internal environment encompasses the tone of an organization, and sets the basis for how risk is viewed and addressed by an entity's people, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate.
- *Objective Setting* – Objectives must exist before management can identify potential events affecting their achievement. Enterprise risk management ensures that management has in place a process to set objectives and that the chosen objectives support and align with the entity's mission and are consistent with its risk appetite.
- *Event Identification* – Internal and external events affecting achievement of an entity's objectives must be identified, distinguishing between risks and opportunities. Opportunities are channeled back to management's strategy or objective-setting processes.
- *Risk Assessment* – Risks are analyzed, considering likelihood and impact, as a basis for determining how they should be managed. Risks are assessed on an inherent and a residual basis.
- *Risk Response* – Management selects risk responses – avoiding, accepting, reducing, or sharing risk – developing a set of actions to align risks with the entity's risk tolerances and risk appetite.
- *Control Activities* – Policies and procedures are established and implemented to help ensure the risk responses are effectively carried out.
- *Information and Communication* – Relevant information is identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities. Effective communication also occurs in a broader sense, flowing down, across, and up the entity.
- *Monitoring* – The entirety of enterprise risk management is monitored and modifications made as necessary. Monitoring is accomplished through ongoing management activities, separate evaluations, or both.
- Enterprise risk management is not strictly a serial process, where one component affects only the next. It is a multidirectional, iterative process in which almost any component can and does influence another.

APPENDIX – C, SOX Testing Template

Overall Process Name
Process Owner Name:

Business Activities: (Names provided in the "Principal Business Activity" column of the Control Matrix)

Tester Name and Title:

Purpose/Control Objectives: The control objectives for which this test program was designed include the following:

1 Control Objective as stated in the Risk Matrix (Control Matrix Ref#)
2 Control Objective as stated in the Risk Matrix (Control Matrix Ref#)
3 Control Objective as stated in the Risk Matrix (Control Matrix Ref#)
4 Control Objective as stated in the Risk Matrix (Control Matrix Ref#)
5 Control Objective as stated in the Risk Matrix (Control Matrix Ref#)

Key Sources: The below contacts, systems and/or documentation were used in testing each control activity noted above:

1 Title of employee, name of document
2 Name of system report, resource documents used
3 Resource documents used, title of employee

Control Activities: The following are control activities which need to be tested for effectiveness:

1 Control activity and reference to the appropriate objectives above (i.e. 1,3 and 4)
2 Control activity and reference to the appropriate objectives above (i.e. 2 and 3)
3 Control activity and reference to the appropriate objectives above (i.e. 4 and 5)

Test Procedures: Describe the test method (i.e. vouching, interviews, observations, etc.) and detailed procedures for the tests to be performed, and the reasons for doing so. Include the sample selection criteria, sampling method, period sampled and a description of the population

1 We tested this control activity by ***Inquiry***, ***Observation***, or ***Vouching***. Describe the test procedure.
2 We tested this control activity by ***Inquiry***, ***Observation***, or ***Vouching***. Describe the test procedure.
3 We tested this control activity by ***Inquiry***, ***Observation***, or ***Vouching***. Describe the test procedure.

Test Results: Document the results of the tests, the supporting documentation, and any findings.

		Testing Attributes			
Sample	Description	A	B	C	Notes
1					
2					
3					
4					

Tick Mark Explanation:		Testing Attributes	
X =	Attribute was satisfied	A =	Describe the attributes of the control tested.
(1) =	Exception explanation	B =	Describe the attributes of the control tested.
(2) =	Exception explanation	C =	Describe the attributes of the control tested.
(3) =	Exception explanation		

Conclusion: Provide an overall conclusion as to the effectiveness of each control activity based on the error rates noted as well as other support noted.

1 Effective/Ineffective
2 Effective/Ineffective
3 Effective/Ineffective

Recommendation (if applicable): Recommend corrective action to mitigate the exposure relating to the ineffective control. Identify the related disposition/action plan, person responsible for remediating the control gap, and expected date of full remediation. Number the recommendation in relation to the ineffective control noted above.

1 ***Action Plan Description:***
Name of Person Responsible:
Expected Date of Implementation:

APPENDIX – D, Test Results Workpaper

1 Operations

1.1 Operations Monitoring and Control

MAJOR PROCESS:	Operations
SUB - PROCESS:	Operations Monitoring and Control
CONTROL NUMBER:	OP-1
CONTROL DESCRIPTION:	Standard Monitoring and Control documents are regularly used to standardize and document processes and activities.
TEST PURPOSE:	Obtain evidence of Monitoring and Control documents
FREQUENCY OF CONTROL:	Monthly
TYPE OF TRANSACTION:	Manual
SAMPLE SIZE:	1
REPORT USED:	Monitoring and Control Monthly Report
TIME PERIOD:	3 months
TESTING APPROACH:	Interviewed process owners, Observed and reviewed reports with process owners
RESULTS OF TESTING PERFORMED	The monthly management meeting is documented by the monthly technical report. The Minutes of these monthly meetings are prepared and distributed to attendees and authorized distribution list. The chair of the meeting is the Owner of the distribution list.
REMEADTION ACTION TAKEN	None required

Source Documents Used	Test Results
Monthly Report 1	A
Monthly Report 2	A
Monthly Report 3	A

Key	Attribute
A	Attribute met without exception
B	Tested Attribute is acceptable, limited and appropriate
C	Attribute has exceptions
D	Attribute has deficiencies

1.2 Operations Certification

MAJOR PROCESS:	Operations
SUB - PROCESS:	Operations Certification
CONTROL NUMBER:	OP-2

CONTROL DESCRIPTION:	The GIACE facility is a registered BS7799/ISO 9001:2000 site.
TEST PURPOSE:	Obtain evidence of current and valid registration
FREQUENCY OF CONTROL:	Monthly
TYPE OF TRANSACTION:	Manual
SAMPLE SIZE:	1
REPORT USED:	Periodic BS7799/ISO 9001:2000Report
TIME PERIOD:	12 months
TESTING APPROACH:	Interviewed process owners, Observed and reviewed certificate and reports with process owners.
RESULTS OF TESTING PERFORMED	BS7799/ISO 9001:2000 site status is documented
REMEADTION ACTION TAKEN	None Required

Source Documents Used	Test Results
BS7799/ISO 9001:2000certification and report	A

Key	Attribute
A	Attribute met without exception
B	Tested Attribute is acceptable, limited and appropriate
C	Attribute has exceptions
D	Attribute has deficiencies

1.3 SAP Job Initiation, Approval & Scheduling

MAJOR PROCESS:	Operations
SUB - PROCESS:	SAP Job Initiation, Approval & Scheduling
CONTROL NUMBER:	OP-3, OP-4,
CONTROL DESCRIPTION:	OP-3 SAP R3 Scheduling tools are used for the production of schedules. OP-4 SAP date/time stamp all job modification transaction and records the job properties
TEST PURPOSE:	OP-3 Obtain evidence that R3 Scheduling tools are used for the production schedules. Confirm for a successful job completion. OP-4 Review the properties tab for one job in the R3 scheduler and obtain evidence of modification history.
FREQUENCY OF CONTROL:	Monthly
TYPE OF TRANSACTION:	Manual
SAMPLE SIZE:	1
REPORT USED:	Process Audit Reports

TIME PERIOD:	3 months
TESTING APPROACH:	Interviewed process owners, Observed and reviewed reports with process owners
RESULTS OF TESTING PERFORMED	OP-3 Confirmed evidence of R3 Scheduling tools in use for the production schedules and confirmed a successful job completion. OP-4 Confirmed the properties tab for one job in the R3 scheduler and obtained evidence of modification history.
REMEADTION ACTION TAKEN	None Required

Source Documents Used	Test Results
Process Audit Reports	A

Key	Attribute
A	Attribute met without exception
B	Tested Attribute is acceptable, limited and appropriate
C	Attribute has exceptions
D	Attribute has deficiencies

1.4 Change Management

MAJOR PROCESS:	Operations
SUB - PROCESS:	Change Management
CONTROL NUMBER:	OP-5, OP-6, OP-7, OP-8
CONTROL DESCRIPTION:	OP-5 A limited number of manual jobs can be initiated by end users in SAP OP-6 Job changes (add or modify) are made and tested in a test environment separate from production. OP-7 For new R3 job plans, a test of the program and parameter is performed in QA ensure proper combination OP-8 For production systems, a manual daily check is carried out. This identifies any problems that have occurred since the last check.
TEST PURPOSE:	OP-5 Verify Internal SAP control over job modification is working as designed OP-6 Sample job changes and validate that proper testing prior to introduction into production occurred. OP-7 Sample of recent R3 job changes, obtain evidence of testing in QA. OP-8 Verify that a manual daily check identifies any problems that have occurred since the last check including any job “abends.”
FREQUENCY OF CONTROL:	Daily
TYPE OF TRANSACTION:	Manual
SAMPLE SIZE:	1 or n/a
REPORT USED:	Report
TIME PERIOD:	3 months
TESTING APPROACH:	Interviewed process owners, Observed and reviewed reports

RESULTS OF TESTING PERFORMED	OP-5 Verified that Internal SAP control over job modification is working as designed OP-6 Verified job changes (add or modify) are made and tested in a test environment separate from production. OP-7 Evidence of testing in QA found and verified OP-8 A manual daily check occurs and identifies any problems
REMEADTION ACTION TAKEN	

Source Documents Used	Test Results
Job Control audit report	A
Basis Moves Report	A
Exceptions Report	A

Key	Attribute
A	Attribute met without exception
B	Tested Attribute is acceptable, limited and appropriate
C	Attribute has exceptions
D	Attribute has deficiencies

1.5 Help Desk

MAJOR PROCESS:	Operations
SUB - PROCESS:	Help Desk
CONTROL NUMBER:	OP-9
CONTROL DESCRIPTION:	Calls made to the Help Desk and the GIACE response statistics are reviewed in the quarterly Desk Top Service Contract review meetings.
TEST PURPOSE:	Verify that a manual check of the response statistics are reviewed in the quarterly Desk Top Service Contract review meetings
FREQUENCY OF CONTROL:	Monthly
TYPE OF TRANSACTION:	Manual
SAMPLE SIZE:	1
REPORT USED:	Desk Top Service Contract Report
TIME PERIOD:	1 month
TESTING APPROACH:	Reviewed reports with process owners
RESULTS OF TESTING PERFORMED	Verified that the response statistics reviewed in the quarterly Desk Top Service Contract are reviewed in the quarterly review meetings
REMEADTION ACTION TAKEN	None Required

Source Documents Used	Test Results
Monthly Report	A

Key	Attribute
A	Attribute met without exception
B	Tested Attribute is acceptable, limited and appropriate

C	Attribute has exceptions
D	Attribute has deficiencies

1.6 Control Monitoring and Reporting

MAJOR PROCESS:	Operations
SUB - PROCESS:	Control Monitoring and Reporting
CONTROL NUMBER:	OP-10
CONTROL DESCRIPTION:	The monthly Service Level/Expected Availability Level report warns of potential outages, capacity and other problems along with anticipated remedial actions.
TEST PURPOSE:	Confirm that Octopus receives a monthly report listing Service Levels or Expected Availability Levels.
FREQUENCY OF CONTROL:	Monthly
TYPE OF TRANSACTION:	Manual
SAMPLE SIZE:	3
REPORT USED:	Service Level/Expected Availability Level Monthly Report
TIME PERIOD:	3 months
TESTING APPROACH:	Reviewed reports with process owners
RESULTS OF TESTING PERFORMED	Documented by the monthly technical report. The monthly reports are prepared and distributed to authorized distribution list. The chair of the meeting is the Owner of the distribution list.
REMEADTION ACTION TAKEN	None Required

Source Documents Used	Test Results
Monthly Report 1	A
Monthly Report 2	A
Monthly Report 3	A

Key	Attribute
A	Attribute met without exception
B	Tested Attribute is acceptable, limited and appropriate
C	Attribute has exceptions
D	Attribute has deficiencies

2 Physical Security

2.1 Physical Security Monitoring and Control

MAJOR PROCESS:	Physical Security
SUB - PROCESS:	Physical Security Monitoring and Control
CONTROL NUMBER:	PS-1
CONTROL DESCRIPTION:	Appropriate physical security access control and monitoring policy, procedures, and mechanisms for the Data Centre are in place.

TEST PURPOSE:	Validate the physical security access control and monitoring policy, procedures, and mechanisms
FREQUENCY OF CONTROL:	Quarterly
TYPE OF TRANSACTION:	Manual
SAMPLE SIZE:	1
REPORT USED:	Physical Security Policy for the Data Center
TIME PERIOD:	3 months
TESTING APPROACH:	Physical “walk-through” inspections at the Data Centre. Inspection, Interviews with process owners.
RESULTS OF TESTING PERFORMED	Site enclosed within a perimeter 2 meter fence barriers on road access fitted with cameras and activated by cardkey. 24 hour security guard presence on site external cameras with remote monitoring service. Windows are fitted with toughened glass fitted with "Crime Shield steel mesh" all fire exit doors are alarmed. Fire exits doors are additionally protected outside normal hours with steel shutters perimeter fence and barriers are locked outside normal hours. Access to the building and the Data Centre is controlled with the use of cardkey and zones allocated as required to authorized staff only. There are 6 control zones with computer machine rooms being a unique zone and the communications room also being a unique zone.
REMEADTION ACTION TAKEN	None required

Source Documents Used	Test Results
Physical Security Policy for the Data Center	A

Key	Attribute
A	Attribute met without exception
B	Tested Attribute is acceptable, limited and appropriate
C	Attribute has exceptions
D	Attribute has deficiencies

2.2 Employee, Visitor, Contractor Access Control and Monitoring

MAJOR PROCESS:	Physical Security
SUB - PROCESS:	Employee, Visitor, Contractor Access Control and Monitoring
CONTROL NUMBER:	PS-2, PS-3
CONTROL DESCRIPTION:	PS-2 Access for employees and contractors is controlled by physical access control mechanisms at all access points of the facility PS-3 Access for terminated and new employees is controlled by HR that notifications are sent to management and security personnel.
TEST PURPOSE:	PS-2 Validate the access control and monitoring elements by conducting interviews, record inspections, and testing. PS-3 Confirm that an access lists of employees is controlled by Human Resources and that appropriate notification of new employees and departing employees is sent to management and security personnel.

FREQUENCY OF CONTROL:	Quarterly
TYPE OF TRANSACTION:	Manual
SAMPLE SIZE:	All
REPORT USED:	Monitoring and Control Report
TIME PERIOD:	3 months
TESTING APPROACH:	Interviewed process owners, Observed and reviewed reports with process owners. Employee, Visitor, Contractor access control and monitoring elements were tested as part of the interviews, record inspections, and testing at the Data Centre.
RESULTS OF TESTING PERFORMED	PS-2 Procedures are in place for authorizing access secured areas and the computer room and prevent unauthorized access. The employee's manager collects the access cards and keys and forwards them to the Properties Management at the time of termination. Upon approval the employee must attend an orientation meeting and sign an agreement of understanding of the facilities policies and d procedures Access request have to be approve by line manger. Procedures exist for providing access to the data center to third parties PS-3 Human Resources provides a list of terminated employees and access is reviewed on a periodic basis. The Data Centre Manger reviews the access log looking for violation patterns.
REMEADTION ACTION TAKEN	None required

Source Documents Used	Test Results
Monitoring and Control Report	A
HR notifications	A
Access Security Logs	A

Key	Attribute
A	Attribute met without exception
B	Tested Attribute is acceptable, limited and appropriate
C	Attribute has exceptions
D	Attribute has deficiencies

2.3 Environmental Controls

MAJOR PROCESS:	Physical Security
SUB - PROCESS:	Environmental Controls
CONTROL NUMBER:	PS-4, PS-5
CONTROL DESCRIPTION:	PS-4 Temperature, humidity, fire detection and water protection environmental security controls are implemented and monitored within computing machine rooms of the Data Centre. PS-5 Electrical power supply is both protected in terms of its quality and availability.

TEST PURPOSE:	PS-4 Confirm that temperature, humidity, fire detection and water protection environmental security controls are implemented and monitored within computing machine rooms of the Data Centre. PS-5 Validate servers in data centre are connected to UPS and backup generator is available 24x7x365
FREQUENCY OF CONTROL:	Quarterly
TYPE OF TRANSACTION:	Manual
SAMPLE SIZE:	1
REPORT USED:	Monitoring and Control Monthly Report
TIME PERIOD:	3 months
TESTING APPROACH:	Interviewed process owners, Observed and reviewed reports with process owners. Observed, Interviewed, and reviewed reports with process owners.
RESULTS OF TESTING PERFORMED	PS-4 The rooms are configured with internal movement sensors and cameras installed structured cabling pre-laid under floor power distribution points strategically positioned around the rooms. Water sensors are in place in the sub floor. All plumbing is located central to the workspace and not overhead of any machine room resources. Conventional fire detectors installed with visual & audible alarm for immediate response. Fire extinguishers are readily available. Temperature & humidity controlled PS-5 Power is supplied from national grid to transformer into 2 supplies to data centre with automatic cutover UPS installed backup generator installed A backup generator is run up to operating temperature & speed once each week, and a full load once per year for 30 minutes.
REMEADTION ACTION TAKEN	None required

Source Documents Used	Test Results
Monitoring and Control Monthly Report	A

Key	Attribute
A	Attribute met without exception
B	Tested Attribute is acceptable, limited and appropriate
C	Attribute has exceptions
D	Attribute has deficiencies

2.4 Automatic Reporting and Monitoring

MAJOR PROCESS:	Physical Security
SUB - PROCESS:	Automatic Reporting and Monitoring
CONTROL NUMBER:	PS-6
CONTROL DESCRIPTION:	GIACE installed centralized building management system that controls and monitors environmental, power, fire detection devices.
TEST PURPOSE:	Validate the installed automated building control, management and monitoring system for power, fire and water detection, and air conditioning.

FREQUENCY OF CONTROL:	Monthly
TYPE OF TRANSACTION:	Manual
SAMPLE SIZE:	1
REPORT USED:	Monitoring and Control Monthly Report
TIME PERIOD:	3 months
TESTING APPROACH:	Interviewed process owners, Observed and reviewed reports with process owners. Observed, Interviewed, and reviewed reports with process owners.
RESULTS OF TESTING PERFORMED	Confirmed that GIACE has installed an automated building control, management and monitoring system for power, fire and water detection, and air conditioning.
REMEADTION ACTION TAKEN	None required

Source Documents Used	Test Results
Monitoring and Control Monthly Report	A

Key	Attribute
A	Attribute met without exception
B	Tested Attribute is acceptable, limited and appropriate
C	Attribute has exceptions
D	Attribute has deficiencies

3 Logical Access

3.1 End User Access – Internet and Remote Access

MAJOR PROCESS:	Logical Access
SUB - PROCESS:	End User Access – Internet and Remote Access
CONTROL NUMBER:	LA-1, LA-2
CONTROL DESCRIPTION:	LA-1 A well defined security administration process is in place that includes appropriate approvals and an audit trail of user access approval and authorization. LA-2 Segregation of duties exists between those needing/wanting, approving accesses, and setting up/configuring access.
TEST PURPOSE:	LA-1 Review for reasonableness the security administration process for Octopus network access. LA-2 Validate for a sample of employees with network access that segregation of duties was maintained in the setup process.
FREQUENCY OF CONTROL:	Quarterly
TYPE OF TRANSACTION:	Manual
SAMPLE SIZE:	All
REPORT USED:	Security Policy
TIME PERIOD:	3 months

TESTING APPROACH:	Interviewed process owners, Observed and reviewed reports with process owners
RESULTS OF TESTING PERFORMED	LA-1 Security administration process for Octopus network access is in place that includes appropriate approvals and an audit trail of user access approval and authorization. LA-2 Segregation of duties exists and is maintained between those approving accesses, and setting up/configuring access.
REMEADTION ACTION TAKEN	None required

Source Documents Used	Test Results
Security Administration Policy and Procedures	A
Segregation of Duties Policy and Procedures	A
Segregation of Duties audit and control reports	A

Key	Attribute
A	Attribute met without exception
B	Tested Attribute is acceptable, limited and appropriate
C	Attribute has exceptions
D	Attribute has deficiencies

3.2 Passwords

MAJOR PROCESS:	Logical Access
SUB - PROCESS:	Passwords
CONTROL NUMBER:	LA-3, LA-4
CONTROL DESCRIPTION:	LA-3 Password rules, structure, and usage are enforced and apply to all users in the environment, regardless of their role. LA-4 All users are assigned their own unique ID and password and user accounts follow a consistent naming convention per the functionality of active directory.
TEST PURPOSE:	LA-3 Validate password parameters are enforced and obtain documentation showing where those options are configured for systematic enforcement upon new account setup. LA-4 Obtain listing of all employees with network accounts. Select sample and validate unique ID and standard naming convention.
FREQUENCY OF CONTROL:	Monthly
TYPE OF TRANSACTION:	Manual
SAMPLE SIZE:	25% of population or 25
REPORT USED:	New User email, Outlook End User testing and Active Directory functionality
TIME PERIOD:	3 months
TESTING APPROACH:	Interviewed process owners, Observed and reviewed reports with process owners
RESULTS OF TESTING PERFORMED	LA-3 Review all key transaction identified and noted only two exceptions and two with reasonable business requirements for the access to key transaction that appear to be incompatible. LA-4 Active directory precludes the reuse of a user id No exception noted

REMEADTION ACTION TAKEN	LA-3 Management has implemented the appropriate changes LA-4 None Required

Source Documents Used	Test Results
New user requests	A
Email verifying setup	A
New user requests form	A
New User notification memo	A

Key	Attribute
A	Attribute met without exception
B	Tested Attribute is acceptable, limited and appropriate
C	Attribute has exceptions
D	Attribute has deficiencies

Password rules structure and usage are enforced and apply to all users in the environment, regardless of their role. Appropriate password structure and usage is enforced by the system and are, at least:

- Password Life Span = 90 days. Users have to change the password at first logon and then every 90 days.
- Minimum Password Length = N characters with alphanumeric values
- Password Alpha/Numeric = At least 8 letter character, 1 number
- Case Sensitive = Upper/lower case sensitive
- Password Uniqueness = 1 passwords
- Account Lockout = the account gets locked out after 3 invalid attempts.
- Lockout Duration = until unlocked by Employee support

3.3 Network Access

MAJOR PROCESS:	Logical Access
SUB - PROCESS:	Network Access
CONTROL NUMBER:	LA-5, LA-6, LA-7
CONTROL DESCRIPTION:	LA-5 The network perimeter architecture consists of a layered defense of routers and firewalls LA-6 A access request memo is created by the user's supervisor or department manager requesting and approving the access. LA-7 Audit logs are maintained for network logons and log offs and certain sensitive folders. The Network Administrator monitors and reviews these audit logs on a weekly basis.
TEST PURPOSE:	LA-5 Review network architecture diagram for reasonableness. LA-6 Verify that an access request memo is created by the user's supervisor or department manager for all new access requests. LA-7 Obtain examples of each type of audit log. Determine how review is performed and what evidence is maintained on the review.
FREQUENCY OF CONTROL:	Monthly
TYPE OF TRANSACTION:	Manual

SAMPLE SIZE:	All
REPORT USED:	Monitoring and Control Monthly Report
TIME PERIOD:	3 months
TESTING APPROACH:	Interviewed process owners, Observed and reviewed reports with process owners
RESULTS OF TESTING PERFORMED	LA-5 Network perimeter architecture includes: Router passwords are encrypted, External firewalls are configured to support automatic failover, Firewall configuration is performed using encryption protocols. LA-6 Access request memos are created for all new users LA-7 Audit logs of events are reviewed.
REMEADTION ACTION TAKEN	None required

Source Documents Used	Test Results
Network perimeter architecture audit logs	A
Access request memos	A

Key	Attribute
A	Attribute met without exception
B	Tested Attribute is acceptable, limited and appropriate
C	Attribute has exceptions
D	Attribute has deficiencies

3.4. Operating System

MAJOR PROCESS:	Logical Access
SUB - PROCESS:	Operating System
CONTROL NUMBER:	LA-8, LA-9, LA-10
CONTROL DESCRIPTION:	LA-8 There are only two persons in the IT department who has Administrator access on the network LA-9 The Systems Administrator removes the access for terminated users A bi weekly termination report is received by the IT group from HR LA-10 Changes to the configuration or hardware must go through the standard Change Management process by opening a help desk ticket and getting the appropriate approval from the service manager
TEST PURPOSE:	LA-8 Obtain listing of all employees with SAP access. Validate that only two employees have administrator rights. LA-9 Obtain 6 months of copies of HR reports to validate existence. Select sample of terminated employees and validate that each terminated employee's user's account was deactivated. LA-10 Verify that a Help Desk ticket is generated and that the Service Manager contacts the client for approval as part of the standard Change Management process.
FREQUENCY OF CONTROL:	Monthly
TYPE OF TRANSACTION:	Manual

SAMPLE SIZE:	all
REPORT USED:	Audit Logs and Control Report
TIME PERIOD:	3 months
TESTING APPROACH:	Interviewed process owners, Observed and reviewed reports with process owners
RESULTS OF TESTING PERFORMED	LA-8 Listing of all employees with SAP access validated that only two employees have administrator rights. LA-9 SAP users have access to data only through the SAP application. All other access is restricted at the root level through AIX and Oracle where only system administrators have access LA-10 Help Desk ticket is generated per Change Management process.
REMEADTION ACTION TAKEN	None required

Source Documents Used	Test Results
Administrator privileges audit trail	A
Change Management policy and procedures	A

Key	Attribute
A	Attribute met without exception
B	Tested Attribute is acceptable, limited and appropriate
C	Attribute has exceptions
D	Attribute has deficiencies

3.5. BASIS Support

MAJOR PROCESS:	Logical Access
SUB - PROCESS:	BASIS Support
CONTROL NUMBER:	LA-11, LA-12
CONTROL DESCRIPTION:	LA-11 The passwords parameters are on the network are set at the operating system level and are also enforced by default in SAP system. LA-12 Oracle and SAP audit logging is implemented
TEST PURPOSE:	LA-11 Verify that the password parameters are on the network are set at the operating system level and are also enforced by default in SAP system. LA-12 Verify that Oracle and SAP audit logging is implemented
FREQUENCY OF CONTROL:	Monthly
TYPE OF TRANSACTION:	Manual
SAMPLE SIZE:	25% of pop or 25
REPORT USED:	Monitoring and Control Monthly Report
TIME PERIOD:	3 months
TESTING APPROACH:	Interviewed process owners, Observed and reviewed reports with process owners

RESULTS OF TESTING PERFORMED	LA-11 Password parameters are on the network are set at the operating system level and are also enforced by default in SAP system. LA-12 Oracle and SAP audit logging are implemented
REMEADTION ACTION TAKEN	None required

Source Documents Used	Test Results
Password parameter logs	A
Oracle and SAP audit logs	A

Key	Attribute
A	Attribute met without exception
B	Tested Attribute is acceptable, limited and appropriate
C	Attribute has exceptions
D	Attribute has deficiencies

4 Application Implementation and Maintenance

4.1 Application Implementation

MAJOR PROCESS:	Application Implementation and Maintenance
SUB - PROCESS:	Application Implementation and Maintenance
CONTROL NUMBER:	ASIM-1, ASIM-2
CONTROL DESCRIPTION:	ASIM-1 Steering Committees guide project work and timelines ASIM-2 Approval is required on all decisions to purchase or develop application systems
TEST PURPOSE:	ASIM-1 For each major project in sample, validate that a Steering Committee exists and meets regularly. Document members and frequency of meeting schedule. Obtain as evidence last agenda and/or meeting minutes. ASIM-2 Select sample of new purchases or developments between 1/1/04 and 7/31/04. Validate that for each formal management approval evidence is available
FREQUENCY OF CONTROL:	Daily
TYPE OF TRANSACTION:	Manual
SAMPLE SIZE:	25% of population or 25
REPORT USED:	Monitoring and Control Reports
TIME PERIOD:	3 months
TESTING APPROACH:	Interviewed process owners, Observed and reviewed reports with process owners
RESULTS OF TESTING PERFORMED	ASIM-1 None during audit period, however, Other periods have R/3 upgrade minutes and approval memos ASIM-2 None during audit period Other periods have R/3 approval memos.
REMEADTION ACTION TAKEN	None required

Source Documents Used	Test Results
Control Reports	A
R/3 upgrade minutes	A
Approval memos	A

Key	Attribute
A	Attribute met without exception
B	Tested Attribute is acceptable, limited and appropriate
C	Attribute has exceptions
D	Attribute has deficiencies

4.2 Process

MAJOR PROCESS:	Application Implementation and Maintenance
SUB - PROCESS:	Process
CONTROL NUMBER:	ASIM-3, ASIM-4, ASIM-5, ASIM-6
CONTROL DESCRIPTION:	ASIM-3 Access to the production environment is restricted (given only to the IT resources supporting the application) and a separation of test and production environments exists, including separation at the server level. ASIM-4 Project plans are developed for all major releases. ASIM-5 An appropriate standardized methodology is used for major application system installments or upgrades. ASIM-6 A standard migration path exists and is used for all configuration/ program changes for SAP.
TEST PURPOSE:	ASIM-3 Obtain listing of all users with PROD access for both and SAP applications. Validate that production access is restricted appropriately. For each Oracle instance, validate test instance resides on separate server from production instance. ASIM-4 Using same sample, validate project plans exist. Review for completeness. ASIM-5 Using same sample, validate standard methodology used on project. ASIM-6 For sample of changes, validate that each followed migration path.
FREQUENCY OF CONTROL:	Monthly
TYPE OF TRANSACTION:	Manual
SAMPLE SIZE:	25% of population or 25
REPORT USED:	Monitoring and Control Monthly Report
TIME PERIOD:	3 months
TESTING APPROACH:	Interviewed process owners, Observed and reviewed reports with process owners
RESULTS OF TESTING PERFORMED	ASIM-3 Cross Reference – Logical Security ASIM-4 Cross Reference – “Controlling Enhancements” Test Matrix ASIM-5 Cross Reference – “Controlling Enhancements” Test Matrix ASIM-6 ASIM Test Matrix

REMEADTION ACTION TAKEN	None required

Source Documents Used	Test Results
	A
	A

Key	Attribute
A	Attribute met without exception
B	Tested Attribute is acceptable, limited and appropriate
C	Attribute has exceptions
D	Attribute has deficiencies

4.3 Change Categories

MAJOR PROCESS:	Application Implementation and Maintenance
SUB - PROCESS:	Change Categories
CONTROL NUMBER:	ASIM-7, ASIM-8, ASIM-9
CONTROL DESCRIPTION:	ASIM-7 Cost/ benefit analysis is performed on all routine change requests prior to beginning any work ASIM-8 Approved projects are logged into the tracking software and updated throughout their lifecycle ASIM-9 Changes requests are logged and tracked to completion in the tracking system
TEST PURPOSE:	ASIM-7 Determine if cost/ benefit documentation exists for a sample of routine changes drawn from report(s) of all changes made to operating environments ASIM-8 Determine if a Help Desk ticket was logged for all active projects ASIM-9 For sample of changes, validate that each has a corresponding Help Desk ticket.
FREQUENCY OF CONTROL:	Monthly
TYPE OF TRANSACTION:	Manual
SAMPLE SIZE:	25% of population or 25
REPORT USED:	Monitoring and Control Report
TIME PERIOD:	3 months
TESTING APPROACH:	Interviewed process owners, Observed and reviewed reports with process owners
RESULTS OF TESTING PERFORMED	ASIM-7 Test Matrix ASIM-8 Obtained listing and validated that Help Desk ticket was logged for all active projects. ASIM-9 Help Desk ticket review and validated by logs
REMEADTION ACTION TAKEN	None required

Source Documents Used	Test Results

Help Desk ticket logs and reports	A
Cost/ benefit documentation	A

Key	Attribute
A	Attribute met without exception
B	Tested Attribute is acceptable, limited and appropriate
C	Attribute has exceptions
D	Attribute has deficiencies

4.4 Testing

MAJOR PROCESS:	Application Implementation and Maintenance
SUB - PROCESS:	Testing
CONTROL NUMBER:	ASIM-10 ASIM-11
CONTROL DESCRIPTION:	ASIM-10 A standard testing methodology is used in all SAP application upgrades ASIM-11 All SAP program changes are user acceptance tested and approved prior to implementation into production
TEST PURPOSE:	ASIM-10 Obtain documented tested methodology. For sub section of project in original sample, validate that testing methodology is evident in corresponding project plan. ASIM-11 Obtain report of all changes made to and SAP environment between 1/1/04 and 7/31/04. Validate that for each: Evidence of user acceptance testing prior to move to production. Standard migration path was used (dev/test, QA, Prod), and Corresponding Help Desk ticket exists
FREQUENCY OF CONTROL:	Monthly
TYPE OF TRANSACTION:	Manual
SAMPLE SIZE:	25% of population or 25
REPORT USED:	Monitoring and Control Monthly Report
TIME PERIOD:	3 months
TESTING APPROACH:	Interviewed process owners, Observed and reviewed reports with process owners
RESULTS OF TESTING PERFORMED	ASIM-10 Cross Reference – "Controlling Enhancements" ASIM-11 Test Matrix
REMEADTION ACTION TAKEN	None required

Source Documents Used	Test Results
Test Matrix	A
	A

Key	Attribute
A	Attribute met without exception
B	Tested Attribute is acceptable, limited and appropriate
C	Attribute has exceptions

D	Attribute has deficiencies

4.5 Enhancement Change Process

MAJOR PROCESS:	Application Implementation and Maintenance
SUB - PROCESS:	Enhancement Change Process
CONTROL NUMBER:	ASIM-12, ASIM-13, ASIM-14, ASIM-15
CONTROL DESCRIPTION:	ASIM-12 Test scripts used in SAP application upgrades are documented ASIM-13 End user, operations, and technical documentation is updated as part of large application upgrade ASIM-14 CTS numbers are automatically generated when a configuration or program change is made in SAP ASIM-15 Post implementation, all technical documentation relating to emergency changes is updated
TEST PURPOSE:	ASIM-12 Obtain documented test scripts for both applications. Select sample and review for reasonableness. ASIM-13 Select sample of all three types of documentation for projects that have occurred this year. Review and determine that it is accurate. ASIM-14 Walkthrough the change of one program. Validate that the CTS number is automatically generated ASIM-15 Obtain copy of change control procedures. Validate that there is a "checklist" for emergency changes and that updating appropriately documentation is included in that list.
FREQUENCY OF CONTROL:	Monthly
TYPE OF TRANSACTION:	Manual
SAMPLE SIZE:	25% of population or 25
REPORT USED:	Monitoring and Control Monthly Report
TIME PERIOD:	3 months
TESTING APPROACH:	Interviewed process owners, Observed and reviewed reports with process owners
RESULTS OF TESTING PERFORMED	ASIM-12 No evidence of for enhancement; they did use as part of upgrade ASIM-13 Cross Reference - Operations ASIM-14 No evidence found ASIM-15 No evidence found *NOT KEY*:
REMEADTION ACTION TAKEN	None required

Source Documents Used	Test Results
	A
	A

Key	Attribute
A	Attribute met without exception
B	Tested Attribute is acceptable, limited and appropriate
C	Attribute has exceptions

D	Attribute has deficiencies

5. Backup and Recovery

5.1 SAP Production Backup and Recovery

MAJOR PROCESS:	SAP Production Backup and Recovery
SUB - PROCESS:	SAP Production Backup and Recovery
CONTROL NUMBER:	BR 1
CONTROL DESCRIPTION:	Written procedures governing the back up tape handling policy are included in the Work Instruction: Dispatch of Magnetic Media to the Off Site Store, Work Instruction: Octopus Corp. SAP/NT RNH2KBU1 Tape Changing and Work Instruction: Receipt of Magnetic Media From The Off-Site Store
TEST PURPOSE:	Obtain copy of document retention policy and/or procedures and review and validate for reasonableness and completeness.
FREQUENCY OF CONTROL:	Monthly
TYPE OF TRANSACTION:	Manual
SAMPLE SIZE:	All
REPORT USED:	Monitoring and Control Report
TIME PERIOD:	3 months
TESTING APPROACH:	Interviewed process owners, Observed and reviewed reports with process owners
RESULTS OF TESTING PERFORMED	Procedure was Appropriate Tape Inventory had no exceptions. Noted no exceptions
REMEADTION ACTION TAKEN	None required

Source Documents Used	Test Results
Work Instruction: Dispatch of Magnetic Media to the Off Site Store	A
Work Instruction SAP/NT RNH2KBU1 Tape Changing	A
SAP/NT RNH2KBU1 SAP Job Check Screen Shots	A

Key	Attribute
A	Attribute met without exception
B	Tested Attribute is acceptable, limited and appropriate
C	Attribute has exceptions
D	Attribute has deficiencies

5.2 SAP Production Backup and Recovery Scheduling

MAJOR PROCESS:	SAP Production Backup and Recovery
SUB - PROCESS:	SAP Production Backup and Recovery Scheduling
CONTROL NUMBER:	BR-2, BR-3

CONTROL DESCRIPTION:	BR-2 Logs and inventory records of the tapes are reviewed for completeness and accuracy before the metal case is closed and locked. BR-3 Production backup jobs are reviewed as a part of the daily checks conducted by Data Centre operators and Management
TEST PURPOSE:	BR-2 Obtain evidence of logs, review and validate. BR-3 Obtain evidence of backup & recovery taps are delivered to the tape vault. Validate the tape logging, packing and case locking prior to pick up by the courier.
FREQUENCY OF CONTROL:	Monthly
TYPE OF TRANSACTION:	Manual
SAMPLE SIZE:	1
REPORT USED:	Monitoring and Control Report
TIME PERIOD:	3 months
TESTING APPROACH:	Interviewed process owners, Observed and reviewed reports with process owners
RESULTS OF TESTING PERFORMED	BR-2 Procedure was Appropriate. Noted no exceptions BR-3 Obtained e-mails that evidenced the checks were done and that that day's backups were successful. Procedure was Appropriate. Noted no exceptions
REMEADTION ACTION TAKEN	None required

Source Documents Used	Test Results
Tape Inventory Sheet ("UNIX BOXES")	A

Key	Attribute
A	Attribute met without exception
B	Tested Attribute is acceptable, limited and appropriate
C	Attribute has exceptions
D	Attribute has deficiencies

5.3 SAP Production Backup and Recovery Testing

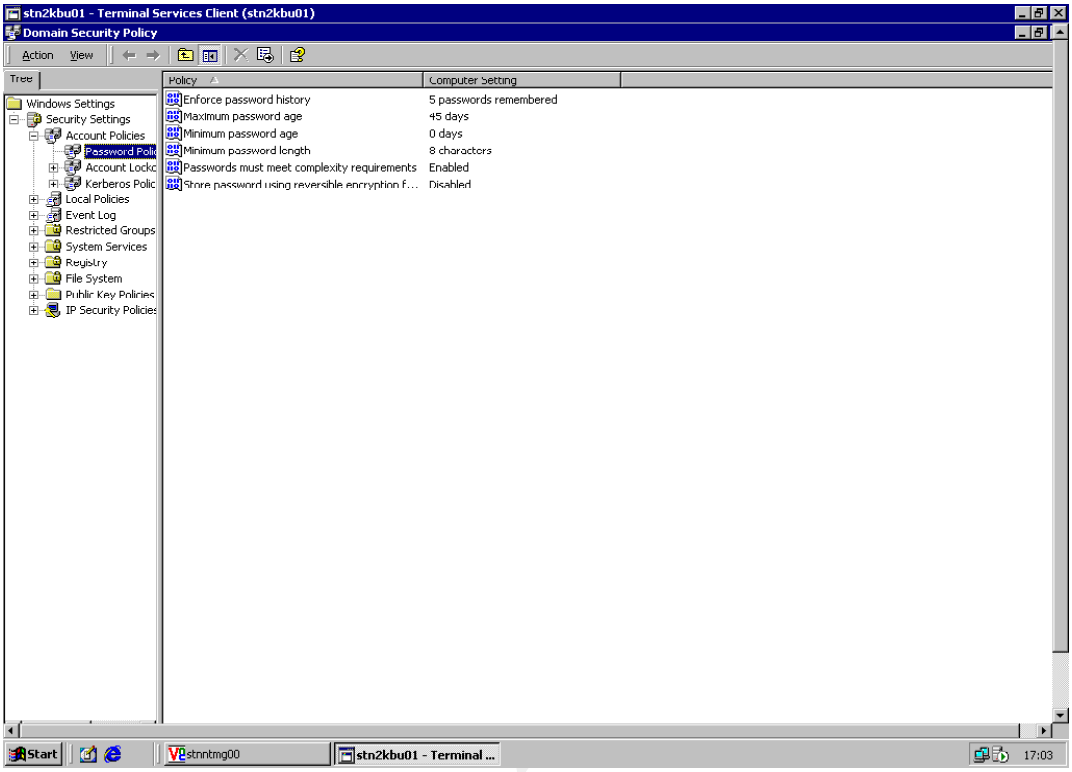
MAJOR PROCESS:	SAP Production Backup and Recovery
SUB - PROCESS:	SAP Production Backup and Recovery Testing
CONTROL NUMBER:	BR-4
CONTROL DESCRIPTION:	A Periodic test, approximately every 6 months is conducted.
TEST PURPOSE:	Obtain evidence of backup & recovery tests performed in last year and validate that a sufficient sampling of locations, applications and supporting platforms have been recovered successfully.
FREQUENCY OF CONTROL:	Monthly
TYPE OF TRANSACTION:	Manual
SAMPLE SIZE:	1

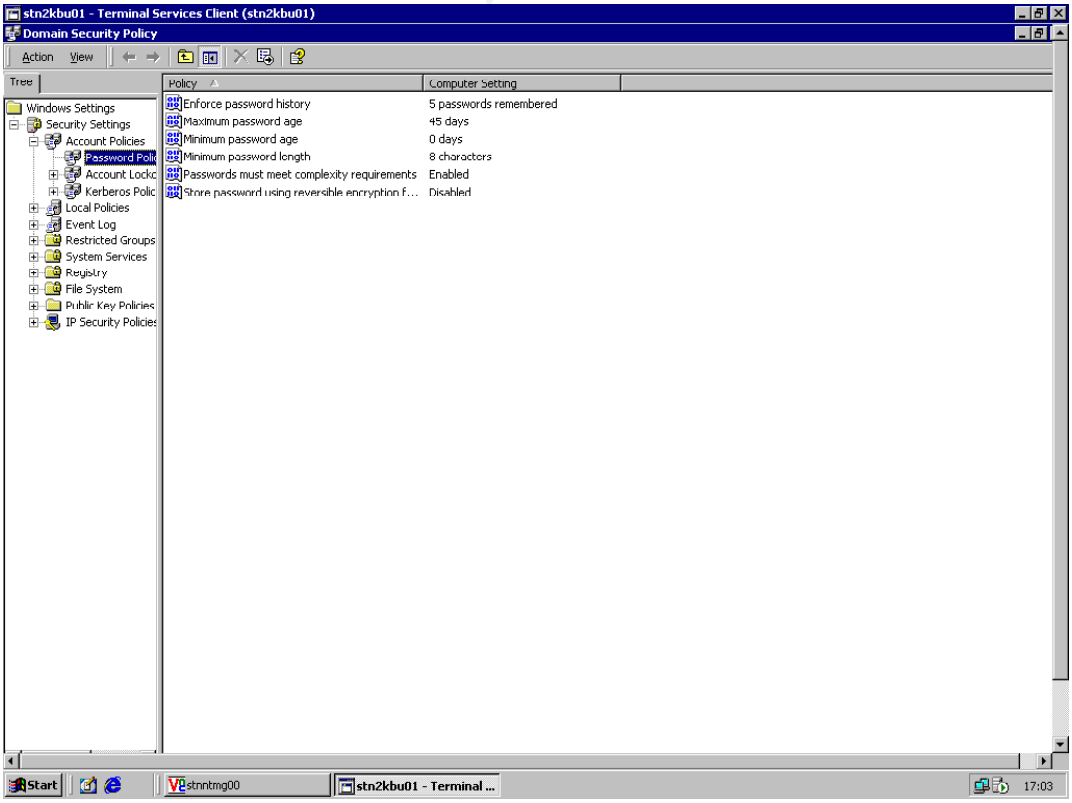
REPORT USED:	Monitoring and Control Report
TIME PERIOD:	3 months
TESTING APPROACH:	Interviewed process owners, Observed and reviewed reports with process owners
RESULTS OF TESTING PERFORMED	Obtained evidence that backup tests would provide a successful recovery.
REMEADTION ACTION TAKEN	None required

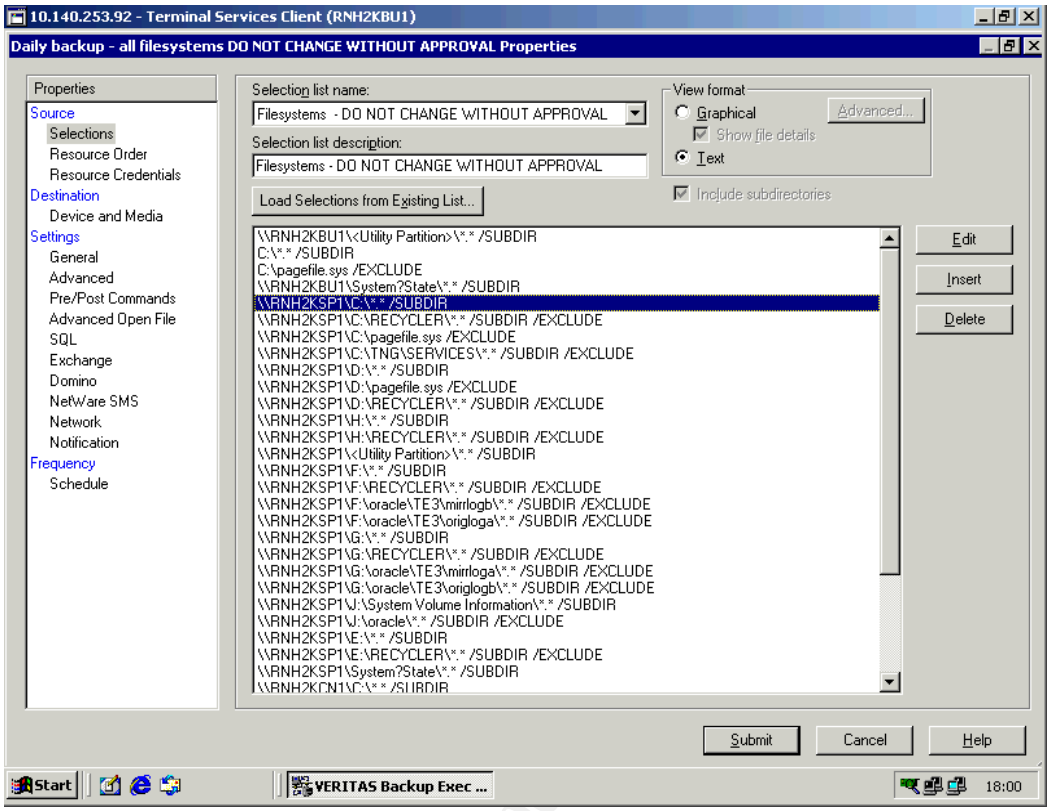
Source Documents Used	Test Results
	A

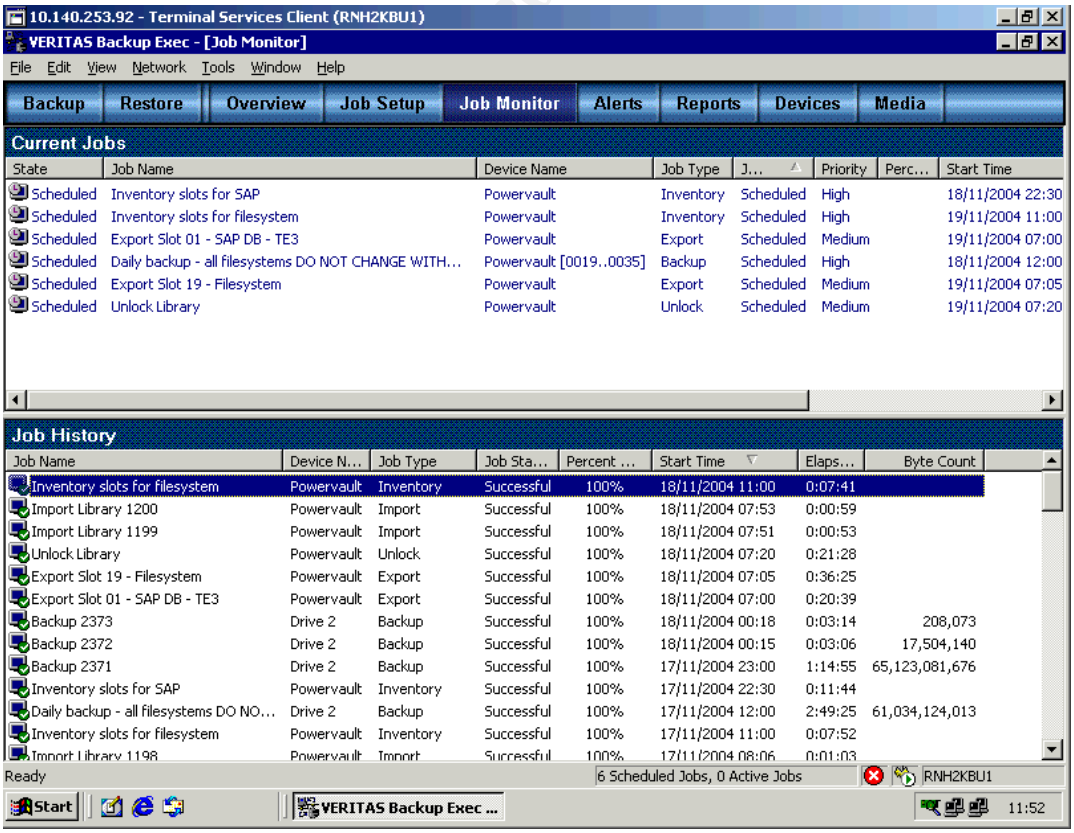
Key	Attribute
A	Attribute met without exception
B	Tested Attribute is acceptable, limited and appropriate
C	Attribute has exceptions
D	Attribute has deficiencies

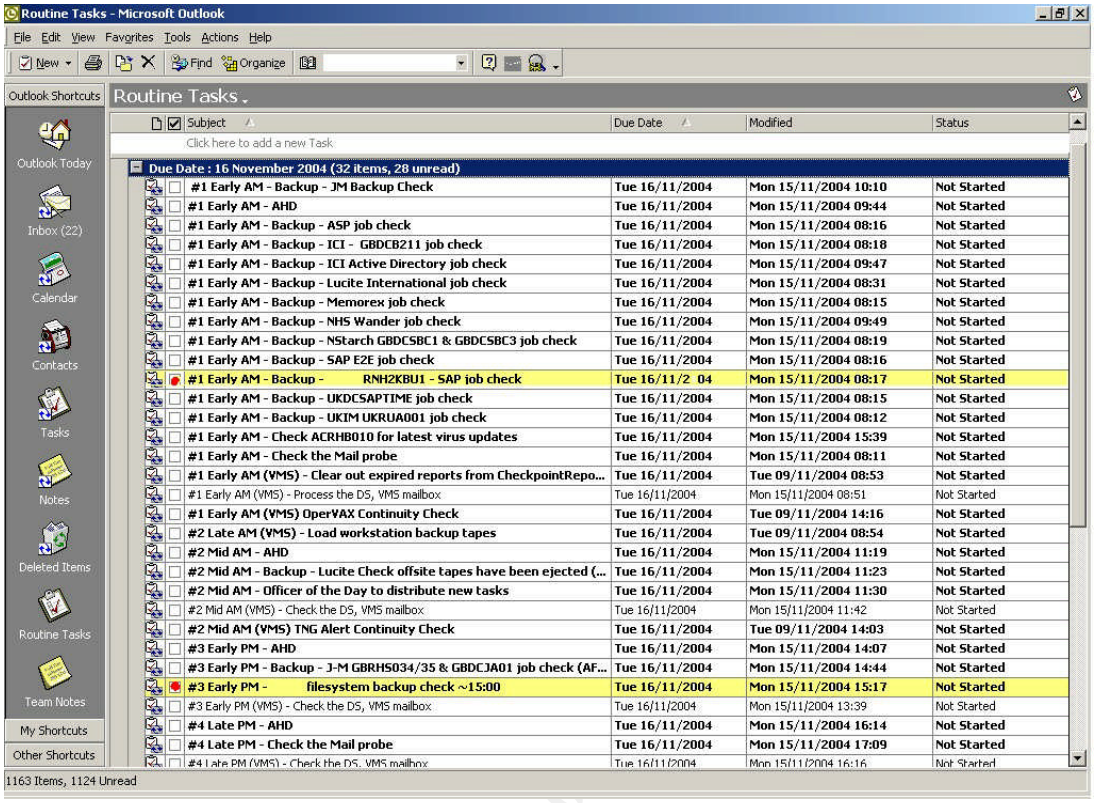
APPENDIX - E, Selected Audit Documentation

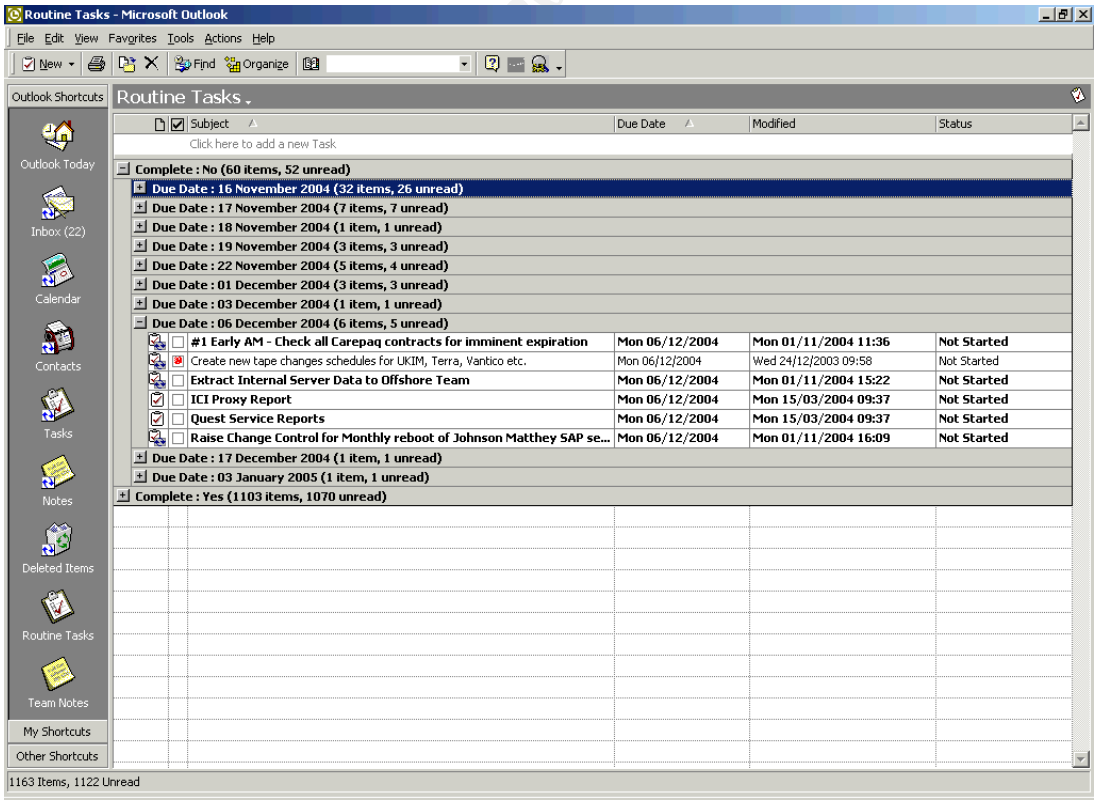












Last Updated: March 15th, 2019

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS Secure Canberra 2019	Canberra, AU	Mar 18, 2019 - Mar 29, 2019	Live Event
ICS Security Summit & Training 2019	Orlando, FLUS	Mar 18, 2019 - Mar 25, 2019	Live Event
SANS SEC504 Paris March 2019 (in French)	Paris, FR	Mar 18, 2019 - Mar 23, 2019	Live Event
SANS Munich March 2019	Munich, DE	Mar 18, 2019 - Mar 23, 2019	Live Event
SANS Jeddah March 2019	Jeddah, SA	Mar 23, 2019 - Mar 28, 2019	Live Event
SANS Doha March 2019	Doha, QA	Mar 23, 2019 - Mar 28, 2019	Live Event
SANS SEC560 Paris March 2019 (in French)	Paris, FR	Mar 25, 2019 - Mar 30, 2019	Live Event
SANS Madrid March 2019	Madrid, ES	Mar 25, 2019 - Mar 30, 2019	Live Event
SANS 2019	Orlando, FLUS	Apr 01, 2019 - Apr 08, 2019	Live Event
SANS Cyber Security Middle East Summit	Abu Dhabi, AE	Apr 04, 2019 - Apr 11, 2019	Live Event
SANS London April 2019	London, GB	Apr 08, 2019 - Apr 13, 2019	Live Event
Blue Team Summit & Training 2019	Louisville, KYUS	Apr 11, 2019 - Apr 18, 2019	Live Event
SANS Riyadh April 2019	Riyadh, SA	Apr 13, 2019 - Apr 18, 2019	Live Event
SANS Seattle Spring 2019	Seattle, WAUS	Apr 14, 2019 - Apr 19, 2019	Live Event
SANS Boston Spring 2019	Boston, MAUS	Apr 14, 2019 - Apr 19, 2019	Live Event
FOR498 Battlefield Forensics Beta 1	Arlington, VAUS	Apr 15, 2019 - Apr 20, 2019	Live Event
SANS FOR585 Madrid April 2019 (in Spanish)	Madrid, ES	Apr 22, 2019 - Apr 27, 2019	Live Event
SANS Northern Virginia- Alexandria 2019	Alexandria, VAUS	Apr 23, 2019 - Apr 28, 2019	Live Event
SANS Muscat April 2019	Muscat, OM	Apr 27, 2019 - May 02, 2019	Live Event
Cloud Security Summit & Training 2019	San Jose, CAUS	Apr 29, 2019 - May 06, 2019	Live Event
SANS Pen Test Austin 2019	Austin, TXUS	Apr 29, 2019 - May 04, 2019	Live Event
SANS Bucharest May 2019	Bucharest, RO	May 06, 2019 - May 11, 2019	Live Event
SANS Security West 2019	San Diego, CAUS	May 09, 2019 - May 16, 2019	Live Event
SANS Milan May 2019	Milan, IT	May 13, 2019 - May 18, 2019	Live Event
SANS Dublin May 2019	Dublin, IE	May 13, 2019 - May 18, 2019	Live Event
SANS Stockholm May 2019	Stockholm, SE	May 13, 2019 - May 18, 2019	Live Event
SANS Perth 2019	Perth, AU	May 13, 2019 - May 18, 2019	Live Event
SANS Northern VA Spring- Reston 2019	Reston, VAUS	May 19, 2019 - May 24, 2019	Live Event
SANS New Orleans 2019	New Orleans, LAUS	May 19, 2019 - May 24, 2019	Live Event
SANS Amsterdam May 2019	Amsterdam, NL	May 20, 2019 - May 25, 2019	Live Event
SANS Hong Kong 2019	Hong Kong, HK	May 20, 2019 - May 25, 2019	Live Event
SANS Autumn Sydney 2019	Sydney, AU	May 20, 2019 - May 25, 2019	Live Event
SANS Norfolk 2019	OnlineVAUS	Mar 18, 2019 - Mar 23, 2019	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced