INFORMATION SYSTEMS AUDIT AND CONTROL ISSUES FOR ENTERPRISE MANAGEMENT SYSTEMS: SOME QUALITATIVE EVIDENCE

Abstract:

Today, organisations may have production applications running on multiple servers, spread geographically throughout the organization. In such circumstances, organisations will look to software assistance through packages collectively known as Enterprise Management Systems (EMS). This paper shows how the introduction of such software creates a new set of IS audit and control problems for such environments. Five sites were interviewed and case studied. While many audit issues were identified, the following problems were clearly highlighted in the cases: a lack of backup in terms of critical human resources; change controls are often non-existent; possible malfunction of scripts causing various impacts including loss of data integrity; and, pre-emption of the execution of critical production systems crippling the entire production environment. Moreover, while the academic and practice literatures were found to be comprehensive regarding the audit and control issues peculiar to the EMS environment, the study identified issues that are not covered in the literature.

Introduction

In an Information Systems (IS) audit, an important area of review for the auditor is the operations centre (or the production servers room(s)) from which the production systems of the organisation are usually run. A review of the adequacy of the general controls in these areas is a well-accepted step in any comprehensive Information

Systems (IS) audit, irrespective of whether the production centre is operated by the organisation itself or by an outsourcing firm (Weber, 1999; King, 1990).

Such a review is important to external and internal auditors alike. External auditors in fulfilling their attest objectives would focus on controls being present in the centre operations to safeguard assets and ensure data integrity. For example, adequate fire prevention, water detection, and physical security controls would safeguard expensive computing assets while controls that monitored the recording of system error messages and the restarting of *abended* (abnormally ended) programs would contribute to the maintenance of data integrity. Internal auditors are not only concerned with attest objectives but more usually with efficiency and effectiveness objectives. In relation to the corporate data centre for example, existence of a sound, well-balanced production schedule and well-established procedures for restarting systems and producing system backups exemplify such controls.

Traditionally, when reviewing the operations area, auditors have looked for manual controls such as separation of duties between operators, production schedulers, programmers, data entry operators, network administrators, and the like; effective supervision of operator activities; and, rotation of duties amongst operations staff. Over the last few years in Australia, computer centres have moved to *automated (or **lights out**) operations facilities (AOF)* in varying degrees. Such facilities can range from automatic loading and unloading of storage media such as tapes and cartridges to the starting and stopping of programs according to a predetermined schedule, making backups, responding to system messages, restarting failed systems, etc. (Weber, 1999). Accordingly, human intervention is rarely needed. Moreover, today, it is not unusual for organizations to have their production systems running across ten's, even hundred's of servers and networks. In such a complex environment,

automated assistance in the monitoring and management of the production components would appear necessary and cost-effective (Ayers & Fentress, 2000; Kreger, 2001; Driml, 2003). Today, such monitoring and management systems are categorised as ***Enterprise Management Systems (EMS)***

The usefulness of AOF/EMS operations has been apparent in North American sites since the late 80's (Miller, 1988; King, 1990; Greenstein, 1992; Mullen, 1993; Sprague & McNurlin, 1993; Marlin, 1999; Gisinger *et al.*, 2001). The cost-effectiveness, and hence the take-up, of technological innovations in Australian sites tends to lag its North American counterparts by some five to seven years usually. Factors such as proven productivity gains, increased labour award flexibility allowing significant labour reductions in the operations area, a significant increase in the number of EMS products on the market and a commensurate drop in the cost of EMS hardware and software have all combined to bring about a marked increase in the use of EMS operations (to varying degrees) in Australian computer centres. To date, however, there does not appear to be any evidence on the degree of pervasion and the major products used in Australia.

Accordingly, this study was performed to gain preliminary insight on the following research questions:

1. What functional capabilities of the EMS are being popularly utilised?
2. What critical audit issues arise when an organization uses an EMS?
3. What controls *are* currently exercised over the EMS?
4. Is there a critical (significant) difference between the audit issues and controls specified in the IS Audit literature and those used/needed in EMS environments in practice?

This paper describes the results of a qualitative study into these research questions. Five (5) large organizations were case studied in terms of their use (to varying degrees) of AOF/EMS software for systems management. We performed this work because of three motivations principally:

1. To inform/extend the literature on the critical audit and control issues that may arise when an AOF/EMS is introduced into an organization;
2. To obtain insight into the types/extent of controls that organisations have actually implemented over the use of AOF/EMS systems; and
3. To provide some guidance to the community of Information Systems Audit practitioners on the types of controls that need to be in place for AOF/EMS systems, and where the most likely exposures in the control of such systems will be found.

Accordingly, this paper unfolds in the following manner. The next section explains briefly what Enterprise Management Systems are and what functionality they provide to an organization. Then, from a review of the literature, the specific audit issues that arise from the use of an EMS and the controls that are suggested to be in place are identified. Next, the case study research methodology and a summary of the results of each of the five cases are provided. The following section discusses the results particularly in the context of the research questions set for this work. Finally, the last section summarises the work in this study and explains briefly how further work into the area will be progressed.

What Are Enterprise Management Systems?

A wide range of enterprise management software (EMS) products is available for automating various aspects of the management of an organisation's information

systems. These products may be designed for the mainframe or client/server environments, and may represent solutions for specific tasks, *e.g.,* storage management, or provide "end-to-end" solutions incorporating the vendor's own specialised products and/or those of other vendors. Examples of specialised products are Legato Storage Manager, Axent Software's OmniGuard™ security management software and Seagate's Backup Exec™ software management solution. Examples of end-to-end solutions are IBM's Tivoli Management Environment (TME) ® 10, Computer Associates' Unicenter TNG ®, Hewlett-Packard's OpenView ®, BMC's Patrol ®, Aprisma's (Cabletron's) Spectrum ®, Candle Corporation's MQ Series and BullSoft's EMS package (Ayers & Fentress , 2000).

Garvey (1999), Hagendorf-Follett (2001), Lais (2000a), Lais (2000b), Middlemiss (2000), Saunders (1999), Songini (2000), and Yasin (1999) explain that the key capabilities provided by EMS products include:

- Automatic detection of applications, databases and hardware environment, including desktops, network computers, hubs, routers and internet gateways.
- Graphical presentation of topology, business process views and floor plans.
- Standardised reporting including system performance metrics.
- Automating production setup, scheduling, execution and monitoring of processes.
- Job restart. Job restart systems can analyse why jobs terminate abnormally and automate restart and recovery processes.
- User notification system to provide an alert notification facility that notifies users of anomalous events.

- Active server-based virus scanning at the point of entry for e-mails and their attachments, and the monitoring of shared folders.
- EMS products can monitor a range of database availability issues, including backup server, table spaces, logs, locks, cache, file backup status and transaction queues.
- Operating system management that includes automatic discovery and continuous monitoring support for the operating system across a LAN or WAN, monitoring key components – CPU, memory, disks, network communications, processes, users, disk I/O, and queues.
- Application management that involves central monitoring and management of applications and services for peak performance and availability. Organisations spend millions of dollars on enterprise resource planning (ERP) systems like SAP R/3, services and infrastructure. An EMS product can utilise various components to monitor the ERP system, execute certain tasks in response to system alerts, and deploy the graphical user interface (*e.g.*, SAPGUI) to large numbers of desktops.
- Automated monitoring and management of internet services for UNIX and Windows NT.
- Job flow and workload management.
- Network management that includes event, fault, configuration, and performance management of networks. This service ensures the LANs run smoothly, with minimal network downtime. The EMS monitors and analyses WAN traffic, and manages interfaces between local and backbone networks.

- EMS products may provide comprehensive security management through authentication, access control, encryption, and audit trail analyses across multiple platforms.
- Storage management that includes backup, encryption, compression, version and time control, vaulting, and robotics; and
- Resource accounting and charging based on the tracking of usage of resources by user and cost centre, and determine charges.

Recent developments in EMS's incorporate predictive analysis modelling capabilities. For example, Computer Associates' Neugents ™ software used in Unicenter TNG monitor systems for unusual patterns and behaviour in real time and can analyse historical performance data to provide the ability to create a model of a system's patterns and predict future activity. BMC's Patrol ™ incorporates predictive analysis and capacity planning software for advanced modelling and analysis of changes in hardware, applications and transaction rates (see for example, Johnston, 2001, and Yasin, 2000).

Internal Control and IS Control.

The internal control system and its structure for an organisation has been explained by many authors. For example, Arens *et al.* (1996, p. 329) explain that, "the system consists of many specific policies and procedures designed to provide management with reasonable assurance that the goals and objectives it believes important to the entity will be met." The system is operationalised by a set of organisation-specific internal controls or control procedures designed to address internal control objectives such as safeguarding assets; compliance with corporate policies and/or legal requirements; authorisation, validity, completeness, valuation, classification, timing,

and posting of transactions; and, efficiency and effectiveness of operations (Arens *et al.*, 1996; CISA Review Manual, 2004). When an information system is a prominent part of an organisation's internal control environment, Auditing Standard AUS 214 (.02) and its American equivalent, SAS 94 (20), clearly dictate that the auditor should consider how the IS environment affects the audit. Accordingly, the control objectives and control procedures have to be translated into IS-specific control objectives and procedures.

This task has been done comprehensively over the years by the auditing standard setters, academic, and practitioner literatures (see for example, AUS 412 (.14); AUS 402 (.19 (e)); SAS (19); Weber, 1999; Bae *et al.*, 2003; CISA Review Manual, 2004). In particular, Weber (1999) and the CISA Review Manual (2004) give good guidance on the IS control procedures required in an IS environment. They categorise them as general management controls and application specific controls. The general management controls include controls over general organization and management, access to data and programs, systems development methodologies and change control, data processing operations, systems programming and technical support, data processing quality assurance procedures, physical access, back-up, and recovery planning. The application specific controls look at controls over input, processing, output, network communications, and databases for each major application system.

In particular, in programmed environments, authors such as Weber (1999) and Bae *et al.* (2003) point out that the highly pertinent general controls are separation of duties, security over access to the source and object code versions of the programs and their parameters, development standards (*i.e.*, programs developed in an authorised manner), change control for the programs, back-up and recovery procedures.

IS Audit and Control Issues Specific to EMS.

To date, there does not appear to be any evidence on the general audit and control issues introduced by the use of the EMS/AOF systems in Australia.

Where the extent of human intervention by operators and local network administrators has been significantly minimised (or even eliminated) by EMS/AOF operations, the nature of the auditor's general control review of the operations area has necessarily changed dramatically. However, much of the training literature for auditors and information systems auditors still refers heavily to controls over human operators such as a review of operator manuals and instructions (see for example, CISA Review Technical Information Manual 2000, 2002, 2004). In effect though, by implementing EMS/AOF operations, organisations effectively are replacing predominantly human-controlled environments with programmed environments as the EMS/AOF systems consist of hardware controlled by program scripts written using languages specific to the products. Accordingly, the control procedures specific to programmed environments, tailored to the characteristics of EMS/AOF systems, become more relevant.

Only little guidance, however, has been provided to auditors to date on the nature and extent of the controls needed over EMS/AOF operations. Weber (1999) and King (1990) provide a review of the controls thought to be needed in this area, at least according to the prescriptive academic IS audit literature. These researchers prescribe that the important audit issues that need to be investigated, clarified, and detailed are:

1. Authorisation of the design, implementation, and maintenance of EMS/AOF programs (procedures or parameters).

2. Separation of duties between the people who write the EMS/AOF procedures and those people who install the procedures in the EMS/AOF hardware.

3. Storage of the EMS/AOF procedures and the security over that storage.

4. The extent to which the EMS/AOF procedures can interfere with the running of production application systems; for example, being able to suppress, not allow to be logged, or ignore application system error messages.

5. Documentation of EMS/AOF procedures.

6. Back-up and off-site storage of EMS/AOF programs, parameters.

7. Contingency plans for the failure of EMS/AOF hardware and/or software.

The Certified Information Systems Auditor (CISA) qualification offered by the Information Systems Audit and Control Association (ISACA) is the worldwide pre-eminent practice qualification for IS auditors. The Certified Information Systems Auditor (CISA) review manual (2004, p. 166) identifies briefly some concerns that arise in an automated systems management environment. "These include:

1. Remote access to a master console is often granted to stand-by operators for contingency purposes such as automated software failure. Therefore, communication access is opened to allow for very risky, high-power, console commands. Communication access security must be extensive. This would include using leased lines and dial-back capabilities.

2. Contingency plans must allow for the proper identification of a disaster in the unattended facility. In addition, the EMS/AOF controlling software or manual contingency procedures must be adequately documented and tested at the recovery site.

3. The application of proper program change controls and access controls, because vital IS operations are performed by software systems. Also, tests of software should be performed on a periodic basis especially after changes or updates are applied.

4. Assurance that errors are not hidden by the software and that all errors result in operator/network administrator notification."

It is interesting to note that items 1-4 in the CISA list are essentially covered in the literature. However, the literature does not directly allude to the CISA audit issue 1. We believe that the empirical case studies will uncover other important audit and control issues surrounding EMS/AOF operations that have not been identified and documented in the literature as yet. The general control issues currently identified in the literature are shown in Figure 1.

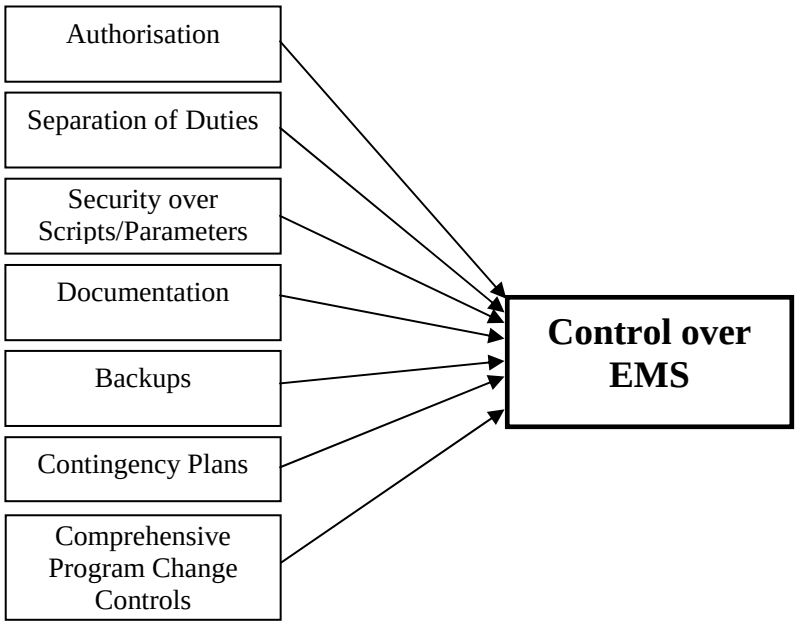

Figure 1. Control issues currently identified in literature.

Case Studies

As stated earlier, this study was performed to gain preliminary insight on the following research questions:

1. What functional capabilities of the EMS are being popularly utilised?
2. What critical audit issues arise when an organization uses an EMS?
3. What controls *are* currently exercised over the EMS?
4. Is there a critical (significant) difference between the audit issues and controls specified in the IS Audit literature and those used/needed in EMS environments in practice?

In order to obtain data to address these research questions, several large organisations that have implemented EMS/AOF were approached and five (5) of them agreed to participate in case studies. These case studies were conducted in late 2000/early 2001 to obtain in-depth knowledge of the issues associated with using EMS that is more readily obtained through an interview. Participants in case studies are more likely to provide information that would not be made available in response to a survey, and so they allow the researcher to obtain a richer understanding of the nature and complexity of the phenomena under investigation (Benbasat *et al.*, 1987; Yin , 1994).

Research Instrument

The case study/interview protocol used as the basis for the case study research was constructed on the basis of the issues identified in the academic and practice literatures[1]. The interviewees in the organisations consisted of those Information

[1] A copy of the request letter, consent form, and the protocol used by the interviewers can be obtained from the corresponding author on request.

Services staff who were directly involved in the installation, running, and maintenance of the EMS/AOF systems for the organisation. In order to ensure impartiality and completeness of the collection and analysis of data collected in this study, a methodology was adapted from Lillis (1999). The interview protocol was designed in order to minimise interviewer bias, which can significantly affect the results derived from the data. The prescriptive nature of the interview protocol ensured that each case was subjected to the same level of questioning. Additionally, the interview protocol, and the feedback sought prior to the implementation of the interviews, helped ensure that the interview protocol consisted of probing non-directive questions – further reducing the possibility of bias.

The protocol was pilot tested at the first case study site (Case Study A). The Case A participant (herein referred to as "Participant A") was provided with a copy of the protocol that would be used as the basis for the interview and to document the responses. Participant A was asked to provide feedback on the instrument instructions, clarity, etc. to reduce potential problems when used for the survey. Appropriate modifications on the instrument were made based on this feedback.

The protocol was structured with two main sections. Section A was intended to collect demographic data about the site to provide an understanding of the environment to be controlled using the EMS/AOF. The data to be collected included hardware make and model, major operating systems used, database products, types of local area networks, major application systems (*e.g.*, Oracle Financials, SAP R/3), numbers of workstations and on-line users, annual revenue, number of personnel, type of industry, private or public sector, and a copy of the organisation chart for the information systems group.

Section B collected data on the EMS/AOF product(s) used and capabilities implemented by the organisation. The data to be collected included EMS/AOF product(s), major application systems controlled using the product(s), level of privilege afforded to the EMS/AOF (*e.g.*, a high level of privilege would allow the EMS/AOF to terminate application systems), capabilities implemented, responsibility for and control of input parameter settings and script languages, change controls implemented (*e.g.*, authorisation and testing of changes to scripts), backup and recovery procedures, and other control issues.

Data Analysis

The analysis of the interview transcript data utilised a combination of theory-testing and grounded theory methodologies. The interview protocol was defined with two purposes in mind. First, to confirm the extent to which the control issues that are identified in literature feature in organisations utilising EMS/AOF functionality. Second, to identify any additional control issues present in practice but not present in the current literature, *i.e.*, to derive new control issues from the data.

The interview transcript data was analysed by one researcher, without the use of data analysis packages, in phase one of the analysis. The transcripts were then codified and analysed by another researcher using the NUD.IST Vivo 2.0 package in phase two of the analysis. The researchers then met to discuss the results of the analysis. The approach was seen as a means of reducing any subjectivity that may be present in the analysis.

Phase One Case Study Results

Five case studies were conducted involving large organisations known to have implemented EMS/AOF. These organisations (herein referred to as Cases A – E) each employed at least 2000 personnel, with Case E having approximately 12000 personnel. Huge investments had been made by these organisations in their IT systems; however, they each had only one or two staff responsible for the operation of their EMS/AOF. The data gathered from each case study is summarised and discussed below[2]. The results presented immediately below summarise the phase one manual analysis of the transcript data. Each table of results is followed by a set of critical comments derived from the interview transcripts that give support to the relevant evaluations made in the table.

Case A		
Demographics	*Hardware/software environment:*	Fujitsu with MSPLEX operating system
	Database products:	SYMPHOWARE, AIM, MDB
	Major application systems:	Rating and billing
	Workstations:	2001-3000
	Industry:	Local government utility
EMS/AOF Operations		
EMS Environment	*EMS/AOF products:*	Fujitsu AOF
	Batch applications controlled:	Meter readings, billing, cash receipts, credit control, backup
	On-line applications controlled:	Rating, property, accounting
Level of privilege and utilised capabilities	*Level of privilege:*	Very high
	Capabilities used:	Automatic detection, production monitoring, user notification, database management, operating system management, application management, job flow and workload management, network management, storage management
Authorisation	*Standards applied to scripts*	No
Separation of Duties	*Who maintains input parameters:*	Systems support
	Who maintains scripts:	Systems support, operations support, job schedulers
Security over	*Access control for parameters:*	RACF, ACF2 security software

[2] A copy of the typed transcripts of the five case study/interviews can be obtained from the corresponding author on request.

Scripts/Parameters	*Access control for scripts:*	Operating system or third party security software
Documentation	*Scripts documented:*	No
	Recovery Procedures documented:	Adequate
Backups	*Backup for scripts:*	With regular system backup
Contingency Plans	*Recovery procedures:*	With system recovery procedures
	Testing of recovery procedures:	No
Comprehensive Program Change Controls	*Change controls:*	Changes made in production environment using GEM change management software. Independent review of changes with limited testing.

Comments

Security over the input parameters and scripts was strong with the use of third–party security packages to control access to the libraries that held these critical components. The AOF product controls a range of applications in the production environment. Accordingly, there is no development environment in which to perform changes and testing. AOF operates at a very high level of privilege. In addition to monitoring the systems and providing alerts, AOF can perform automated functions that may include executing programs and terminating application systems. Accordingly, there is a risk that scripts may malfunction and cause various impacts including loss of data integrity. Few staff members have the expertise to manage this product properly. There is also the potential for maliciousness by staff.

Case B		
Demographics	*Hardware/software environment:*	Compaq Alpha with UNIX and VMS operating system
	Database products:	ORACLE
	Major application systems:	ORACLE Financials, CONCEPT Payroll
	Workstations:	> 4000
	Industry:	Tertiary institution
EMS/AOF Operations		
EMS Environment	*EMS/AOF products:*	BMC Patrol, Networker, Legato Storage Manager, SMS
	Batch applications controlled:	Payroll
	On-line applications controlled:	Finance, personnel
Level of privilege	*Level of privilege:*	Very high

and utilised capabilities	*Capabilities used:*	Automatic detection, graphical presentation, standardised reporting, user notification, database management, operating system management, internet monitoring
Authorisation	*Standards applied to scripts*	No
Separation of Duties	*Who maintains input parameters:*	Systems specialist
	Who maintains scripts:	Systems specialist
Security over Scripts/Parameters	*Access control for parameters:*	Operating system
	Access control for scripts:	Operating system or third party security software
Documentation	*Scripts documented:*	No
	Recovery Procedures documented:	No
Backups	*Backup for scripts:*	With regular system backup
Contingency Plans	*Recovery procedures:*	With system recovery procedures
	Testing of recovery procedures:	Yes
Comprehensive Program Change Controls	*Change controls:*	None

Comments

This organization is at an early stage in implementing BMC Patrol, but it intends using this product to control all application systems. Strong security over the input parameters and scripts is maintained by the file permission settings of the operating system. Change controls are non-existent however. Accordingly, there is no development environment in which to perform changes and testing. This product operates at a very high level of privilege and can perform automated functions that may include executing programs and terminating application systems. Accordingly, there is a risk that scripts may malfunction and cause various impacts including loss of data integrity. Few staff members have the expertise to manage this product properly. Additional control issues raised by staff include remote control of workstations by systems personnel and “piggybacking” on user ORACLE Financials sessions via the Software Management System (SMS).

Case C		
Demographics	*Hardware/software environment:*	HP with HP UX operating system
	Database products:	ORACLE
	Major application systems:	Inhouse applications, HR, Network Facilities Management, Roster Status
	Workstations:	2001-3000
	Industry:	Energy utility
EMS/AOF Operations		
EMS Environment	*EMS/AOF products:*	BMC Patrol
	Batch applications controlled:	Nil
	On-line applications controlled:	All applications, including database operations
Level of privilege and utilised capabilities	*Level of privilege:*	Only monitoring
	Capabilities used:	Automatic detection, standardised reporting, database management, operating system management
Authorisation	*Standards applied to scripts*	No
Separation of Duties	*Who maintains input parameters:*	Database administrator
	Who maintains scripts:	Database administrator
Security over Scripts/Parameters	*Access control for parameters:*	Operating system
	Access control for scripts:	Operating system
Documentation	*Scripts documented:*	No
	Recovery Procedures documented:	No
Backups	*Backup for scripts:*	With regular system backup
Contingency Plans	*Recovery procedures:*	None
	Testing of recovery procedures:	No
Comprehensive Program Change Controls	*Change controls:*	None

Comments

This organization suffers from a lack of management commitment to implementing BMC Patrol. Hewlett Packard (HP) provides standard scripts. Strong security over the input parameters and scripts is maintained by the file permission settings of the operating system. Change controls are non-existent. Accordingly, there is no development environment in which to perform changes and testing. This product can operate at a very high level of privilege, but is currently used only for monitoring. Despite this, the risk remains that scripts may malfunction and cause various impacts

including loss of data integrity. Few staff members have the expertise to manage this product properly.

Case D		
Demographics	*Hardware/software environment:*	Sun, Alpha, Compaq, HP with Sun OS, UNIX and HP UX operating systems
	Database products:	ORACLE
	Major application systems:	ORACLE Financials
	Workstations:	> 4000
	Industry:	Local government
EMS/AOF Operations		
EMS Environment	*EMS/AOF products:*	CA Uni-Center, BMC Patrol, Control M, Datametrics, ViewPoint
	Batch applications controlled:	Revenue
	On-line applications controlled:	ORACLE
Level of privilege and utilised capabilities	*Level of privilege:*	Only monitoring
	Capabilities used:	Automatic detection, graphical presentation, standardised reporting, production monitoring, user notification, database management, operating system management, internet monitoring, job flow and workload management, storage management
Authorisation	*Standards applied to scripts*	No
Separation of Duties	*Who maintains input parameters:*	Desktop support, operations manager
	Who maintains scripts:	Desktop support, operations manager
Security over Scripts/Parameters	*Access control for parameters:*	Operating system
	Access control for scripts:	Database management system
Documentation	*Scripts documented:*	Yes
	Recovery Procedures documented:	No
Backups	*Backup for scripts:*	Separate backup
Contingency Plans	*Recovery procedures:*	Separate recovery
	Testing of recovery procedures:	No
Comprehensive Program Change Controls	*Change controls:*	Authorisation, separate development environment, unit testing, some changes in production

Comments

Strong security over the input parameters is maintained by the file permission settings of the operating system while security over the scripts is maintained through the

access controls of the database management system. Separate development, testing, and production libraries are maintained for the maintenance of the EMS/AOF scripts. Accordingly, change controls are deemed to be adequate. These products are currently used only for monitoring applications.

Case E		
Demographics	*Hardware/software environment:*	Fujitsu, HP with BME and HP UX operating systems
	Database products:	INGRIS
	Major application systems:	POLARIS
	Workstations:	> 4000
	Industry:	State government
EMS/AOF Operations		
EMS Environment	*EMS/AOF products:*	ITO, Vigilant, HP Operations Centre, Maestro, Helmsman
	Batch applications controlled:	None
	On-line applications controlled:	POLARIS, property, weapons
Level of privilege and utilised capabilities	*Level of privilege:*	Only monitoring
	Capabilities used:	Automatic detection, graphical presentation, production monitoring, database management, operating system management, job flow and workload management, network management
Authorisation	*Standards applied to scripts*	No
Separation of Duties	*Who maintains input parameters:*	Systems administration
	Who maintains scripts:	Systems administration
Security over Scripts/Parameters	*Access control for parameters:*	Operating system
	Access control for scripts:	Operating system
Documentation	*Scripts documented:*	No
	Recovery Procedures documented:	Yes
Backups	*Backup for scripts:*	With regular system backup
Contingency Plans	*Recovery procedures:*	None
	Testing of recovery procedures:	No
Comprehensive Program Change Controls	*Change controls:*	Authorisation, separate development environment, unit testing, some changes in production, independent testing, some documentation

Comments

Strong security over the input parameters and scripts is maintained by the file permission settings of the operating system. Change controls exist but they could be improved by not allowing changes to be made directly to "production" scripts. There is no disaster management plan for IT. These products are currently used only for monitoring applications. Without full testing, malfunctions could occur resulting in lost data integrity.

Phase Two Analysis Results

The case study interview transcripts were coded and analysed using NUD.IST Vivo 2.0 software for textual data analysis. The NVivo package has been long regarded as one of the leading qualitative data analysis packages (Lewis 1998). The package was chosen for its powerful data codification and data searching capabilities.

Raw interview transcripts were coded with the use of NVivo, associating transcript sentences with nodes. In order to reduce bias in the analysis of the data, the hierarchical coding structure was designed based on the semi-structured interview questions. Any additional nodes in the hierarchy that did not correspond to the initial coding structure were added as additional issues emerging from the interview data.

The results of the NVivo analysis are presented in Table 1.

Issue		**Number of cases (out of five possible) in which the issue was raised**
Level of privilege and utilised capabilities	*Level of Privilege*	
	High	2
	Monitoring Only	3
	Utilised capability	
	Automatic detection	5
	Graphical presentation	3
	Standardised reporting	4

	Production monitoring	2
	Standardised text editor	0
	Job restart	0
	User notification system	3
	Virus scanning	0
	Database management	5
	Operating system management	5
	Application management	1
	Internet monitoring	2
	Job flow and workload management	2
	Network management	1
	Security management	0
	Storage management	2
	Output management	0
	Resource accounting and charging	0
Authorisation	Standards applied to scripts	0
Security over Scripts/Parameters	*Access control for scripts*	
	Operating System	3
	Third party security software	1
	Database Management System	1
	Access control for parameters	
	Operating System	4
	Third party security software	
Documentation	Scripts documented	1
	Recovery Procedures documented	2
Separation of Duties	*Who maintains input parameters:*	
	Systems Administrator	2
	Database Administrator	1
	Systems Specialist	1
	Operational Support	2
	Who maintains scripts:	
	Systems Administrator	2
	Database Administrator	1
	Systems Specialist	1
	Operational Support	1
Comprehensive Program Change Controls	*Change controls*	
	Authorisation	2
	Separate development environment	2
	Unit testing	2
	Independent testing	1
	Updating script documentation	1
	Controlled release to production	1
Backups	*Backup procedures*	
	Regular system backups	4
	Separate backups	1
	Documented	2
Contingency Plans	*Recovery procedures*	
	System recovery procedures	2
	Separate recovery procedures	1
	None	2
	Tested periodically	1

Other issues raised:	lack of expertise of staff in the products in question (3 cases), lack of experienced backup staff (2 cases), lack of confidence in the products' system performance metrics reporting (1 case), product not utilized to best of monitoring capabilities (1 case), remote access to master console (1 case)

Table 1. Summary of Nvivo case analysis.

The results from phase one and phase two analyses of the case studies can be summarised as follows.

- There appears to be a strong priority on security over the input parameters and scripts. These components are maintained by a handful of persons with the required expertise.
- However, there is a lack of backup in terms of human resources.
- Change controls range from existing and operating properly, to existing and not operating properly, to non-existent. Change controls that exist but do not operate properly are characterised by many changes being performed in "production" without adequate testing and documentation.
- A separate development environment may not be maintained in many instances.
- In addition to monitoring the systems and providing alerts, these products can perform automated functions that may include executing programs and terminating application systems. Accordingly, there is a risk that scripts may malfunction and cause various impacts including loss of data integrity.
- This software needs to operate at such a high level of privilege with regard to the Operating System that, in some circumstances, it may pre-empt the execution of critical production systems and, effectively, cripple the entire production environment. In such circumstances, the entire system may need

to be re-started. Accordingly, recovery procedures and, in extreme situations of prolonged outage, disaster recovery procedures become critical.

It is interesting to review these results in light of the audit issues prescribed by the academic and practice literatures earlier. Table 2 summarises the results in light of these issues.

Audit Issue	**Mentioned in Cases***	**Addressed Adequately (On average across the 5 cases)****
1. Authorisation of design, implementation and maintenance		
1.1. Authorisation	Y	L
1.2. Standards	N	-
1.3. Ongoing monitoring & maintenance of scripts	Y	H
2. Separation of Duties	Y	L
3. Security over parameters/scripts	Y	H
3.1 Security over scripts	Y	H
3.2 Security over parameters	Y	H
3.3 Control over remote access to master console	Y	L
4. Documentation	Y	L
5. Backups	Y	H
6. Contingency plans		
6.1 Recovery Procedures	Y	M
6.2 Off site copies	N	-
7. Proper program change control		
7.1 Change controls	Y	L
7.2 Errors not hidden by software	N	-
Other audit issues identified in cases.		
9. Level of privilege of software operation	Y	L
10. Adequate level of expertise in	Y	M

software		
11. Adequate level of backup for human resources.	Y	L

Table 2. Summary of results against prescribed controls.

(* Y = Yes, N = No; ** L = 1-2 cases, M = 3 cases, H = 4-5 cases)

Table 2 shows that the prescriptive IS Audit academic and practitioner literatures are deficient still with regard to critical issues such as the level of operating system privilege at which this type of software operates, the presence of an adequate level of expertise in the software at the site, and the presence of an adequate level of backup for the critical human experts in this type of software. Moreover, even though sites are aware of many of the critical audit issues prescribed in the literature, they appear to pay no/little attention (on average) to several of these issues, *e.g.*, authorisation of the development/maintenance of scripts, separation of duties, remote access to master consoles, documentation of scripts and design decisions, and change controls. Furthermore, there were control issues of which the participants made no mention at all, *viz.*, developing scripts according to authorised standards, maintenance of current off-site copies of scripts, and ensuring errors are not hidden by the executing scripts. Indeed, only secure file storage of the parameters/scripts, and ongoing monitoring over the adequacy and completeness of EMS/AOF operations appear to attract high levels of attention at sites.

Summary and Further Work

This paper has detailed the work performed in a preliminary study that has investigated the IS audit and control issues surrounding the introduction and use of an Enterprise Management System (Automated Operation Facilities) into a computer-based site. It has explained how, today, organisations may have production

applications running on tens, even hundreds of servers and networks, spread geographically throughout the organization. In such an environment, organisations cannot rely entirely on human operators/administrators. Moreover, the organization needs centralised control over the operation of those corporate servers. In such circumstances, organisations will look to software assistance through packages collectively known as Enterprise Management Systems (EMS).

This paper goes on to show how the introduction of such software, and the resultant minimisation of reliance on human operators/administrators, creates a new set of IS audit and control problems for such environments. Five sites were interviewed and case studied. The results of this work are summarised in this study. While many audit issues were identified, the following problems were clearly highlighted in the cases:

- There is adequate security over input parameters and scripts. These are maintained by a handful of persons with the required expertise.
- However, there is a lack of backup in terms of human resources.
- Change controls range from adequate to non-existent. Many changes are performed in production without adequate testing and documentation.
- A separate development environment may not be maintained.
- In addition to monitoring the systems and providing alerts, these products can perform automated functions that may include executing programs and terminating application systems. Accordingly, there is a risk that scripts may malfunction and cause various impacts including loss of data integrity.
- This software needs to operate at such a high level of privilege with regard to the Operating System that, in some circumstances, it may pre-empt the

execution of critical production systems and, effectively, cripple the entire production environment. In such circumstances, the entire system may need to be re-started.

This paper then determined that while the academic and practice literatures were beginning to recognise the audit and control issues peculiar to the EMS/AOF environment, there were still issues that the literatures did not cover, *viz*., the level of operating system privilege at which this type of software operates, the presence of an adequate level of expertise in the software at the site, and the presence of an adequate level of backup for the critical human experts in this type of software. Moreover, even though sites are aware of many of the critical audit issues prescribed in the literature, they appear to pay little attention (on average) to several of these issues. Indeed, only secure file storage of the parameters/scripts and ongoing monitoring over the adequacy and completeness of EMS/AOF operations appear to attract high levels of attention at sites.

The work in this study was designed to accomplish three objectives:

1. Inform/extend the literature on the critical audit and control issues that may arise when an AOF/EMS is introduced into an organization;

2. Obtain insight into the types/extent of controls that organisations have actually implemented over the use of AOF/EMS systems; and

3. Provide some guidance to the community of Information Systems Audit practitioners on the types of controls that need to be in place for AOF/EMS systems, and where the most likely exposures in the control of such systems will be found.

Further work in this area is planned. On the basis of the results of the qualitative work reported here, a comprehensive survey instrument has been designed. It will be issued to in excess of 1,000 large sites in Australia and New Zealand. The results of this study and the subsequent comprehensive survey will attempt to give significant insight into the following research questions of interest:

1. To what extent are EMS's implemented in large organisations in Australia?
2. What functional capabilities of the EMS are being most popularly utilised?
3. What critical audit issues arise when an organization uses an EMS?
4. What controls should be exercised and what controls *are* currently exercised over the EMS?

Acknowledgements

This work is funded in part by a grant from the Institute of Chartered Accountants in Australia. The authors are indebted to participants and the discussant on an earlier version of this paper presented at AFAANZ 2003 in Brisbane.

REFERENCES

Arens, A., Best, P., Shailer, G., and J. Loebbecke, 1996, Auditing in Australia: An Integrated Approach, 3rd edn., Prentice-Hall:Sydney.

Ayers, S. and D. Fentress, 2000, "Enhancing IT Governance Through Enterprise Management Software Solutions", Information Systems Control Journal, Vol. 2, pp. 1-5.

Bae, B., Epps, R., and S. Gwathmey, 2003, "Internal Control Issues: The Case of Changes to Information Processes", Information Systems Control Journal, Vol. 4, pp. 44-46.

Certified Information Systems Auditor Review Manual, 2000, Information Systems Audit and Control Association (ISACA): Rolling Meadows.

Certified Information Systems Auditor Review Manual, 2002, Information Systems Audit and Control Association (ISACA): Rolling Meadows.

Certified Information Systems Auditor Review Manual, 2004, Information Systems Audit and Control Association (ISACA): Rolling Meadows.

Driml, S., 2003, "Enhancing Security with an IT Network Awareness Center", Information Systems Control Journal, Vol. 4, pp. 51-52.

Garvey, M., 1999, "Storage Gains Flexibility", Informationweek, No. 754, p. 30.

Gisinger, A., Shankaran, R. and P. Ray, 2001, "An evaluation process for enterprise management systems: a business perspective", Proceedings of 2001 Enterprise Networking, Applications, and Services Conference, pp. 9-16.

Greenstein, I., 1992, "Quit babysitting your LANs", Networking Management, No. 3, pp. 70-75.

Hagendorf-Follett, J., 2001, “Serving the Enterprise”, Computer Reseller News, No. 928, p. 100.

Johnston, M., 2001, “IBM Systems Management Software Predicts Server Failure”, InfoWorld, Vol 23, No. 5, p. 20.

King, J., 1990, “Auditing the lights-out facility”, EDPACS, Vol. 18, No. 3, pp. 1-8.

Kreger, H., 2001, “Java Management Extensions for Application management”, IBM Systems Journal, Vol. 40 No. 1, pp. 104-129.

Lais, S., 2000a, “BMC’s Patrol Targets B2B Management”, Computerworld, Vol. 34, No. 33, p. 52.

Lais, S., 2000b, “HP Launches OpenView Suite that offers Business View”, Computerworld, Vol. 34, No. 6, p. 10.

Lewis, R., 1998, ATLAS/ti and NUD*IST: A comparative review of two leading qualitative data analysis packages. Cultural Anthropology Methods, 10(3): 41-47.

Lillis, A.M., 1999, “A framework for the analysis of interview data from multiple field research sites”, Accounting and Finance, Vol. 39, No. 1, pp. 79-105.

Marlin, S., 1999, “Enterprise Systems Management: Banks look to get a grip on IT”, Bank Systems & Technology, Vol. 36, No. 11, pp. 42-48.

Middlemiss, J., 2000, “ABN AMRO taps Computer Associates’ Platform to Consolidate Disparate Systems”, Bank Systems & Technology, Vol. 37, No. 9, p. 24.

Miller, H.W., 1988, “Planning for unattended data center operation”, Mainframe Journal, Jan/Feb., pp. 10-15.

Mullen, J., 1993, “Auditing the Data Center: Setting audit test objectives”, EDP Auditing, Auerbach Publications, pp. 1-15.

Saunders, J., ,1999, “CA adds Storage Control to its Management Tools”, Computing Canada, Vol. 25, No. 28, p. 23.

Songini, M., 2000, “CA targets Quality of Service, Service-Level Management”, Network World, Vol. 17, No. 14, p. 10.

Sprague, R. and B. McNurlin, 1993, Information Systems Management in Practice, Prentice-Hall:Englewood-Cliffs.

Weber, R., 1999, EDP Auditing: Conceptual Foundation and Practice, 3rd edn., Prentice-Hall:New Jersey.

Yasin, R., 1999, “BullSoft combines Security, Management”, Internetweek, No. 766, p. 8.

Yasin, R., 2000, “Anticipate Problems, Map Changes – Software that Sees the Future”, Internetweek, No. 827, p. 1.

Yin, R.K., 1994, Case Study Research: Design and Methods. Sage:Thousand Oaks.