



IBM Global Services Security

Security in IT Outsourcing Whose Responsibility ?

Andy Ho, CISM, CISA, CISSP
Manager of Security, Asia Pacific, IBM Global Services

Information Systems Audit and Control Association
Hong Kong Chapter Professional Development Seminar, Apr/2004

© 2004 IBM Corporation

IGS



Agenda

- **Recent Trends of Outsourcing**
- **The Security Consideration**
- **The Suggested Way to Address the Security Issue**

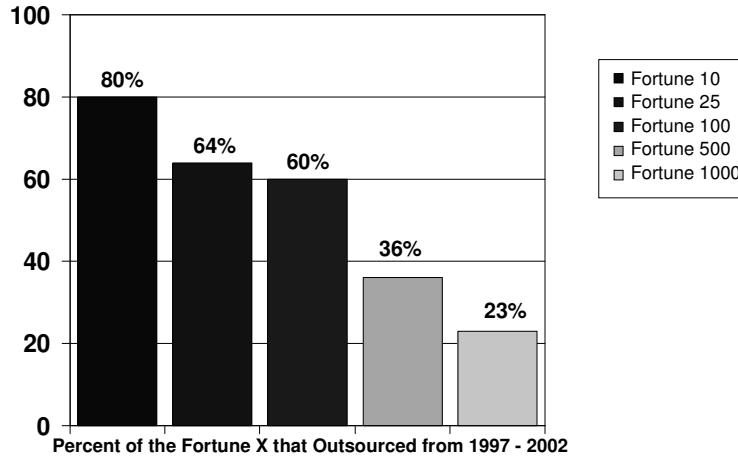


2

© 2004 IBM Corporation

Outsourcing has become a common business strategy

60% of Fortune 100 firms have their outsourcing business strategies in place



Source: IDC Contracts Database 1997-2002

Firms Using Outsourcing Services



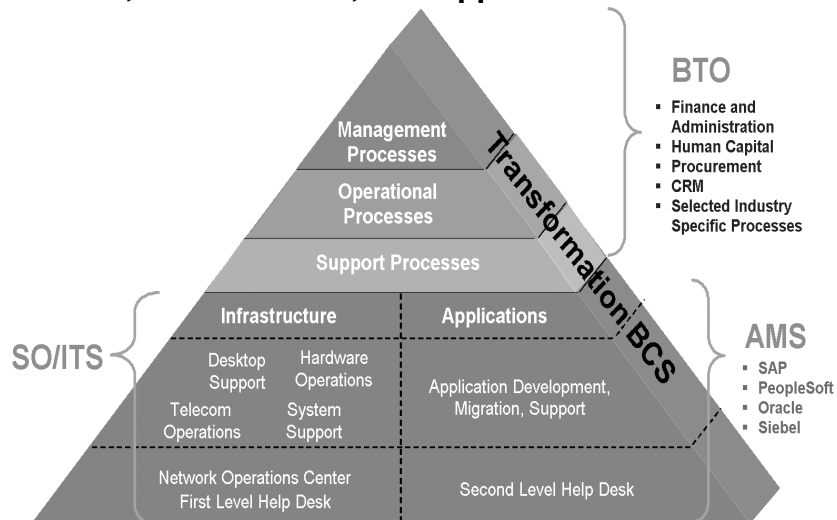
Strategic Outsourcing : What is the Value for the Client ?

- Cost reduction
- Ability to focus on core competencies
- Increase availability of specific skills and resources
- Improve stability, effectiveness and service levels of IT
- Enable rapid business change / expansion
- Obtain access to advanced technologies & research, and to industry, business and technology experts
- Predictable expense management
- Gain contractually committed service levels
- Flexibility to transition to the next generation of infrastructure and applications
- Build a long term strategic relationship ... for competitive advantage



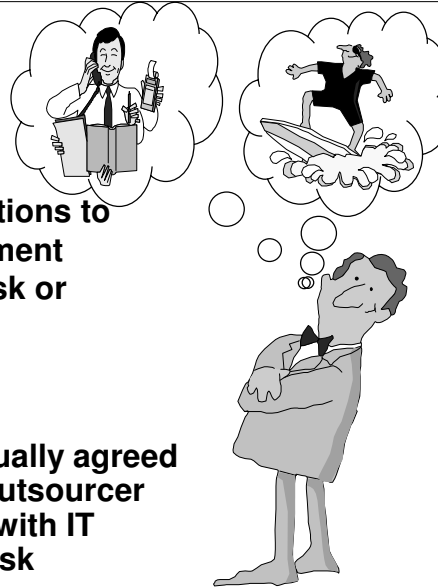
Increase shareholder value

Outsourcing Services Available: Processes, Infrastructure, and Applications



Security Consideration

- Does outsourcing of IT operations to an outsourcer mean management can transfer the IT security risk or accountability to a third party company?
- Failure to implement a mutually agreed security process with the outsourcer may expose organizations with IT outsourcers to untenable risk

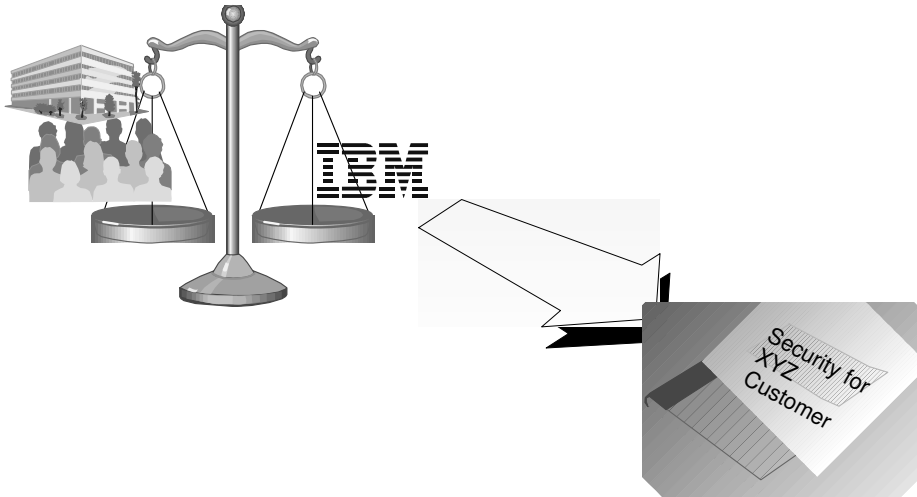


Meta Group – Need a Process to allocate responsibilities

- The client organization should retain primary execution responsibility for most of the analysis/design processes and functions. A key cornerstone of an adaptive approach to information security is the development and implementation of processes (i.e., policy management, risk management, etc.) that enable business discretion in security solution design. Given the intimate knowledge of the business that this implies, such processes do not lend themselves to being outsourced. However, technology-specific expertise (e.g., cryptography, network security) can be provided by the outsourcer (or other service providers).
- In addition to providing a model for allocating responsibilities between client and outsourcer, security processes also enable specific associated metrics. These metrics potentially form the foundation for effective security service levels to be negotiated and instituted as part of the outsourcing relationship. Furthermore, effective security auditing is crucial in an outsourced environment, and the nature of processes (i.e., a predefined set of actions executed in a predefined sequence, with consistent decision points) enables improved auditability.
- Bottom Line: Outsourcing IT does not transfer risk or accountability for information security. Organizations must use a process-based approach to delineate security responsibilities between themselves and their outsourcers.

Source: Organizing for security in an outsourced environment - By Tom Scholtz, 20 Jan 2004 | Meta Group,
http://searchcio.techtarget.com/originalContent/0,289142,sid19_gci945210,00.html

The Suggested Way to Address Security Responsibility Issue For Data Center Outsourcing

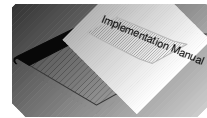
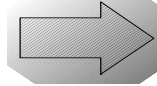


Client Security Document - Agenda

1. What is and why create an SO security document ?
2. What the SO security document covers ?
3. The creation process
4. Implementation

What is an SO Security Document?

- **A document that is used to capture the Security Policies that an outsourcing client wants an outsourcer to implement on their systems/servers and network**
 - Based on existing the outsourcer's IT security policies
- **Two documents are created for each client**
 1. SO Security Document (Client's Security Policy and Roles & Responsibilities)
 2. Implementation Manual (Controls to implement the security policy documented in the SO Security Document)



Why create an SO security document?

- **Ensure both the client and the supporting personnel understand all of the security responsibilities**
- **Ensure support teams knows how systems are to be set up and maintained**
- **Ensure that the security processes required are known**
- **Contract language is very high level and this document completes the requirements**



Why create it?

- **Document Client's Security Policies**
 - Many clients do not have a documented policy or it is out of date
 - Allows the outsourcer to recommend policy changes to the client to either strengthen it or save costs
- **Identifies security requirements for the outsourcer to implement and maintain**
 - Processes that need to be created/modified
 - Security control values to be set on the client's system/server platforms
- **Document controls for compliance reviews**
 - Used by the outsourcer's Audit Teams, IGS Business Controls, Client's Audit Teams and third party auditors to verify delivery of service for the client
 - If Client's Audit Teams or third party auditors think the controls should be different than documented, it lets them know that the discussion must be with the client

The Participants

- **From the Client**
 - The PO/DPE should discuss with the client who the representatives should be. They should be able to decide for the company the security policy that they want the outsourcer to maintain on their systems/servers.
- **From the Outsourcer**
 - Project Executive (PE) or PO representative (Owns the relationship with the client and the SO security document)
 - DPE (Owns the delivery of services from IGS to the client)
 - SO security process coordinator (Will manage the tasks involved with the SO security document creation)
 - Security Specialist/Security Delivery Specialist
 - Provider of Service for Logical and Physical Access Controls, Portable Media Management, and Network Security
- **From third party (if any)**
 - If any part of the service delivery is outsourced to another company, a representative must be involved to ensure that the company can deliver the required security. The representative can be from the company or an the outsourcer employee that the third party agrees can represent them.

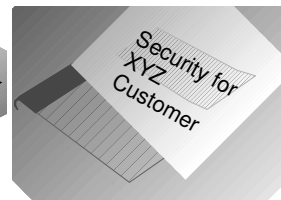
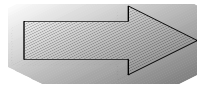
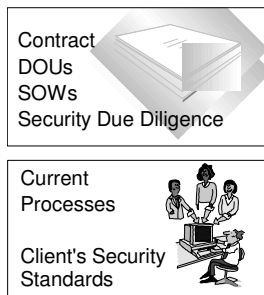
Importance of Participation



- Participation of all parties during the creation of the security document / Implementation Manual is critical.
- Failure to fully participate may lead to an audit failure and expose the client and the outsourcer.

Creation Process

The Outsourcer will create a draft and review it with the client



IBM Recommendations for all Policy tables will be filled in.

Roles defined in the contract will be filled in.

Security Document Contents

- Specifies who performs the security roles
- Documents the client's security policies that should be implemented on the outsourcing systems and servers
 - Physical Access Controls
 - Logical Access Controls
 - Security Status Checking
 - Portable Storage Media
 - Security Incident Management
 - Security/Integrity Advisory Process
 - Application/End User Security
 - Network Controls
 - Firewalls
 - Managed Security Services



A 'Roles Worksheet' is created

- This step documents per the contract whether the outsourcer or the Client will perform the security roles. These tables should be reviewed very carefully to ensure that the execution matches the contract. to assist with this.
- For example:

Userids Roles/Responsibilities (P = Primary, A = Assist)		IBM	Cust XYZ	N/A
Base	During the Transition period, perform a baseline inventory of userids for the systems for which IBM has security responsibility.	P	A	
	During the Transition Period, perform a review of system accesses for all employees transferring to IBM to confirm that same access is required and advise IBM of any change.	A	P	
	Establish, change, deactivate and remove userids and associated access authorities for IBM employees (userid administrator)	P		

Document the client's Security requirements

Example 1: (all the same)

System Value/Parameter	Recommended Setting	Current Setting	Agreed to Setting	Reference
Password history	4	4		2.1.2
Max password age	186 days	90 days		2.1.2
Min password length	6	5 characters		2.1.2

Example 2: (minor differences)

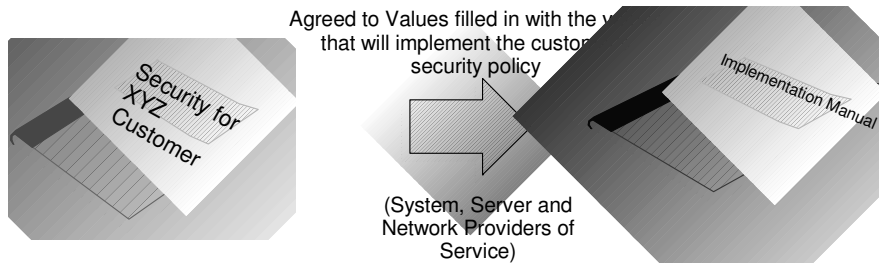
System Value/Parameter	Recommended Setting	Current Setting	Agreed to Setting	Reference
Password history	4	4		2.1.2
Max password age	186 days	90 days		2.1.2
Min password length	6	5 RNYSP01: 4 RNYSP05: 3		2.1.2

Example 3: (many differences, single tables)

System Value/Parameter	Recommended Setting	Current Setting	Agreed to Setting	Reference
Password history	4	RNYSP01: 4 RNYSP02: 3 RNYSP03: RNYSP05: RNYSP06: 5 RNYSP04: 4 RNYSP07: 0		2.1.2
Max password age	186 days	RNYSP01: RNYSP02: 90 days RNYSP03: 186 days RNYSP04: 365 days RNYSP05: RNYSP06: RNYSP07: 0 days		2.1.2
Min password length	6	RNYSP01, RNYSP03,		2.1.2

From Policy to Implementation

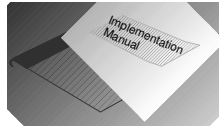
- Use the Client's security policy defined in the SO security document to determine what values would implement those policies
- Place those values in the Implementation Manual 'Agreed to Value' column



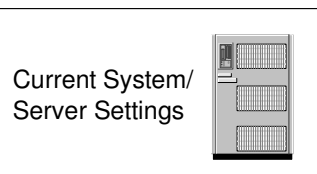
Implementation Manual Contents

- Documents the controls that need to be implemented on specific platforms / subsystems to be compliant with your security policy documented in the SO security document.
- The appendices specific to the systems and servers will be included. There are 50+ platform specific appendices available.
- The outsourcer will maintain this document for the purpose of knowing the controls to be implemented. You are welcome to review it.
- It will be updated if the SO security document is updated.

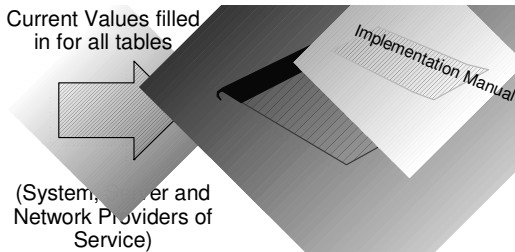
A1. OS/390 & MVS w/RACF	M. Novell Netware	X. Tandem
A2. OS/390 & MVS w/CA-TopSecret	N. TCP/IP	Y. DEC/VMS
A3. OS/390 & MVS w/CA-ACF2	N1. TCP/IP (AIX)	Z. Tivoli
B1. Host VM with RACF	N2. TCP/IP (Linux)	AA. HP/UX
B2. Host VM with ALERT/VM	N3. TCP/IP (OS/400)	AB. Sun/Solaris
B3. Host VM with VM:Secure	N4. TCP/IP (OS/390)	AC. Digital UNIX
B4. Host VM with ACF2	N5. TCP/IP (OS/2)	AD. Linux
C. OS/400 Platforms	N6. TCP/IP (Sun Solaris)	AE. Firewall
D. Network Infrastructure	O. DCAF	AF. Sybase
E. AIX Platforms	P. DCE Servers	AG. Oracle
F. AFS Servers	Q. DFS Servers	AH. SAP
G. AFS Client Subsystems on AIX	R. DCE/DFS Clients	AI. Microsoft Exchange
H. OS/2 LAN Servers	S. Netfinity	AJ. Microsoft Windows 2000
I. OS/2 Base Operating Systems	T. Netview DM/2	AK. Apache Webserver
J. Lotus Domino Servers	U. Microsoft Windows NT	AL. Domino Webserver
K. Universal DB	V. ADSM/TSM Servers	AM. Microsoft IIS
L. CMVC	W. Netview	AN. MQSeries



Implement Current System Values?



Current Values filled in for all tables



(System, Server and Network Providers of Service)

Include appendices for platforms managed by the Outsourcer for this client – Example IBM platforms

Appendix A1. z/OS, OS/390 and MVS Platforms with RACF

© Copyright IBM Corporation, 1997, 2002 - All Rights Reserved
Version 4.2 - November 18, 2002

A1.1 System Setup

A1.1.1 Initial System Setup

A1.1.1.1 System Settings

Note: System Standards for NetView, TCP/IP, Web Servers, MQSeries, etc. can be found in other Appendices.

System Settings	Recommended Setting	Current Setting	Agreed to Setting	Reference
RACF SETROPTS	IES(BATCHALLRACF)			2.1
RACF SETROPTS	PASSWORDINTERVAL (186) HISTORY(4) REVOKE(4) NORULES)			2.1
RACF SETROPTS	CLASSACT(DATASET GROUP USER TEMPDSN OPERCMDS TSOAUTH SDSF FACILITY TAPEVOL) RACLIST(OPERCMDS) GENERIC(DATASET) PROTECTALL(FAILURES) WHEN(PROGRAM) RVARYEW(SWITCH)			2.2

Include appendices for platforms managed by the Outsourcer for this client - Example non-IBM platforms

Appendix AD. Linux

Copyright IBM Corporation, 1997, 2002 - All Rights Reserved
Version 4.2 - November 18, 2002

Version - Release Levels:

RedHat Ver 6 Rel 1 RedHat Ver 6 Rel 2 RedHat Ver 7 Rel 1 RedHat Ver 7 Rel 2
RedHat Ver 7 Rel 3 SuSE Ver 7 Rel 3 SuSE Ver 8 Turbo Linux Ver.
7.0 Server Caldera eServer V2.3 Debian (preliminary only)

AD.1 System Setup

AD.1.1 Initial System Setup

AD.1.1.1 System Settings

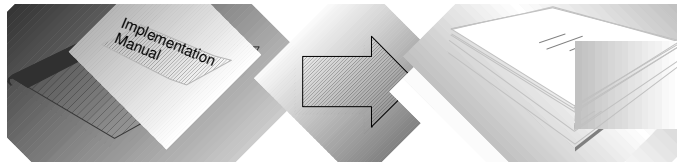
System Settings	Description	Recommended Setting	Current Setting	Agreed to Setting	Reference
/etc/pam.d/other	Enforce a default no access policy	auth required /lib/security/pam_deny.so account required /lib/security/pam_deny.so			3.6.1

AD.1.1.2 Network Settings

System Settings	Recommended Setting	Current Setting	Agreed to Setting	Reference
Anonymous FTP options	System Settings: If any directories will be made writable, the <code>u 027</code> option must be used. Note: this is a vsftpd specific requirement.			2.1.1
Configuration of the ftp account home directory	Must be owned by root and grant write access only to the owner			2.1.1
Configuration of the bin subdirectory of the ftp account home directory	Must be owned by root and grant write access only to the owner. File contained in this directory must have a mode of 0111.			2.1.1
Configuration of	Must be owned by root and			2.1.1

Creation Process (continued)

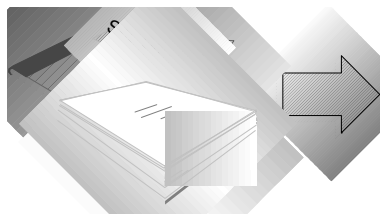
- the Outsourcer will create an exceptions document to show where the current security setting does not implement the security policy documented in the SO security document



A list of the Current Values that are different than the Agreed to Value.

Creation Process (continued)

- The client and The outsourcer will review the updated security document (changes from the last review meeting) and the exceptions document



The results will be a list of security controls that will be made compliant with the security policies and those that will remain exceptions to the client's policy

The exceptions will be added to the last chapter of the security document

Creation Process (continued)

Finalize the Document

- All updates completed and agreed to
- Document will be delivered to the client's representative with a cover letter
- SO security document / Implementation Manual made available to the outsourcer's Service Delivery Personnel



Implementation

- **Identify procedures / controls in SO security document / Implementation Manual that need to be implemented (if any)**
- **Create change records for all changes**
- **Implement Changes**



Summary of Schedule

- mm/dd Create initial draft for review
- mm/dd Kickoff meeting
- mm/dd Client XYZ review complete
- mm/dd Implementation Manual & exceptions document created
- mm/dd Review of SO security document /exceptions document
- mm/dd Final version of document complete
- mm/dd Implementation starts



Summary

- **Outsourcing IT does not transfer risk or accountability for information security**
- **A process-based approach to document security responsibilities between organizations and their outsourcers is suggested**

Questions

