

-
-
-

Agenda

Introduction and Objectives

- What are your Options
- Areas that must be covered, and how

How this presentation will go today -

- We encourage the session to be interactive. We want your opinions and comments.
- We will discuss each of the areas to review, the control objectives, go over some risks and then describe the basic controls.
- For each, area, we will then make suggestions as to how you might audit the area.
- We have provided some Web sites to go to for audit programs to assist you.

Message

- It's always been difficult to look at IT on your own. Today, because of growth, technical complexity and regulatory requirements, it's even more difficult. One answer is to outsource or co-source.
- If you cannot, we have a few recommendations that can help you and your organization understand how to proceed and maximize your coverage.
- No matter how complex or simple a system, there are some items that you must cover (e.g. , security, project management, business continuation planning, etc.).

•
•
•

Options

- **Outsource**
- **Co-source**
- **Do it yourself**
- **Guest Auditor**

Outsource

- **Completely outsource your IT audit function**
- **Pros –**
 - Right skills
- **Cons –**
 - Never build the skills internally
 - Difficult to manage at times
 - No staff continuity

Co-Source

- **Use a third party to assist you in technical audits**
- **Pros –**
 - Cost effective
 - Right skills
- **Cons –**
 - Difficult to manage at times
 - No staff continuity

Do It Yourself


- **Build the skills in house**
- **Train business/operational auditors**
- **Pros –**
 - Retain the skills
- **Cons –**
 - Cost
 - Time commitment
 - Once you train auditors, they become more valuable

•
•
•

Guest Auditor

- **Borrow technical skills**
- **Use internal resources**
- **Pros –**
 - Less costly
- **Cons –**
 - Independence
 - Lack of audit skills

-
-
-



**Then, of course, you could
employ a combination of the
options we just discussed.**

•
•
•

Significant Areas Needing Coverage

- **Security**
 - **Business Continuation Planning**
 - **Library Management**
 - **Change Management**
 - **Application Controls**
 - **Backup and Recovery**
 - **Project Management**
 - **Systems Development Life Cycle (SDLC)**
 - **Vendor Management**
- • • • • • • • • •

Security

Objective

- Identification, Authentication & Access
- Security surveillance/ Awareness
- Monitoring mechanisms

Risk

- Unauthorized access to sensitive and confidential information (Privacy is a big issue)
- Loss of processing capability (viruses, worms, etc.)
- Company reputation

Controls

- Policies and procedures, Security Agreement
- Violation and incident reporting
- Prevention, detection and correction

Security - cont'd

What to do

- Hire expertise if you don't have it
- Train "experts"
- Buy tools, it's easier than building them
- Monitor security "patches"/ Viruses/Health check
- Leverage your organization/partner (security organization, IT)

Business Continuation Planning

Objective

- Information systems and business processes are available as needed

Risk

- Lost revenue
- Customer dissatisfaction
- Impact on reputation

Controls

- Inventory and prioritize critical applications
- Establish recovery time objectives
- Document plans for business, locations and systems
- Test, test, test...

BCP - cont'd

What to do

- This is an area that can be done with operational auditors
- Determine who's accountable
- Review plans, Recovery Time Objectives, Test Time Questionnaires, overall strategy (big picture)
- Test, test, test...

Library Management - cont'd

What to do

- Still need test, production library separation, version control
- Documentation required, approvals, etc.
- Deal with more vendors means education for your staff

Change Management - cont'd

What to do

- Need to look over multiple platforms (NT, UNIX, routers, middleware, mainframe)

Application Controls

Objective

- Completeness and accuracy of input, processing & output

Risk

- Misappropriation of funds
- Unauthorized access
- Company reputation

Controls

- Balancing & reconciliation
- Transaction authorization
- Data integrity
- Confidentiality of information

Application Controls - cont'd

What to do

- Back to basics
- End to end testing
- Nothing falls through the cracks (which are many)

Backup and Recovery

Objective

- Restore processing timely

Risk

- Lost revenue
- Customer dissatisfaction
- Impact on reputation

Controls

- Records management policy and procedures
- Offsite storage

•
•
•

Backup and Recovery - cont'd

What to do

- Review process
- Ensure accountability
- Stay tuned with regulations

Project Management

Objective

- Standard process (from scope to conclusion)
- Projects delivered on time and on budget
- Projects meet user requirements

Risk

- Turnover/retention
- Cost overruns
- Workarounds

Controls

- Standard process and deliverables
- Accountability
- Monitoring

Project Management - cont'd

What to do

- Real time involvement, more dialogue
- Still need standard process, no matter what they say
- Need to train your auditors in the technologies employed
- Company needs to manage vendor relationships
- Accountability and monitoring still apply

SDLC

Objective

- **Standard and REPEATABLE process**
- **Clearly defined user needs and problem to be solved**
- **Right resources utilized**

Risk

- **Right resources not involved**
- **Requirements not defined**
- **Potential benefits not realized**

Controls

- **Methodology**
- **Accountability and approvals**
- **Monitoring**

SDLC - cont'd

What to do

- Still need structure, may be RAD, still must document
- Understand interfaces
- Involve your organization's Information Security, BC Office and Technology
- Accountability, monitoring, approvals still apply

Vendor Management

Objective

- **Select the right vendor for the job**
- **Negotiate a sound contract that protects your organization**
- **Manage the ongoing relationship**

Risk

- **Vendor doesn't meet expectations**
- **Hidden costs**
- **Disputes, etc.**

Vendor Management - cont'd

Controls

- Vendor selection, due diligence
- Right people negotiate contract
- Service level agreements (SLAs)

Vendor Management – Cont'd

What to do

- **Make sure you are involved in due diligence**
- **Understand project management**
- **Make sure that the proper people are involved**
 - Especially legal related to the contract, exit strategy
- **Help develop strong SLAs**
- **Help develop good monitoring processes**

•
•
•

Questions

- **Luis.fuertes@prudential.com**
- **Jack.malley@prudential.com**