SAP: How Risk Savvy Are You?

5 March 2012

SAP User Group – NSW Public Sector Special Interest Group

audit office
OF NEW SOUTH WALES

Why is this important?

audit office
OF NEW SOUTH WALES

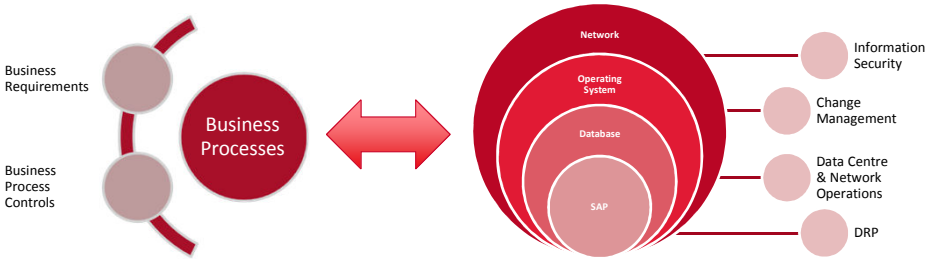
Session Objectives

Understanding some of the key risks associated with SAP.

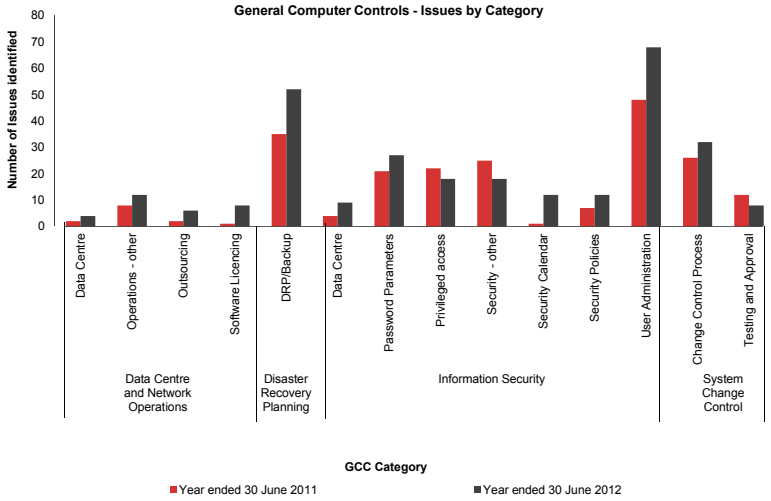
Understanding what tools are available to assist.

Understanding the common approaches on how these risks are addressed.

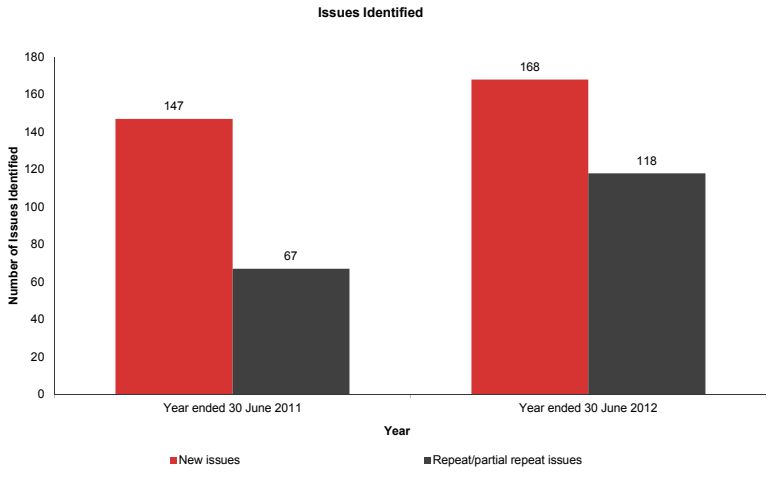
The Big Picture



Overview of Audit Issues Raised



Overview of Audit Issues Raised



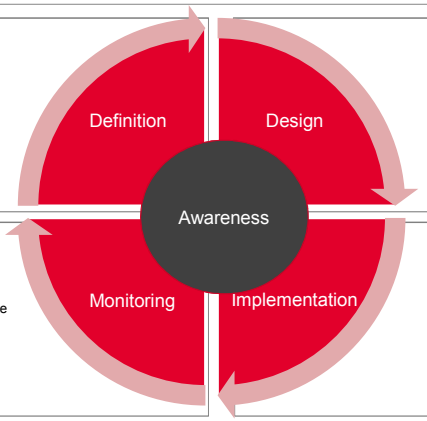
Risk Area:
SAP User Access Management

- General User Accounts Management
  - Creation, modification & termination
- Generic user accounts management
  - Access types
  - Custodianship management
- Default user accounts management
  - Access types
  - Custodianship management
- Users with access capability to:
  - Perform table maintenance
  - SAP_ALL & SAP_NEW equivalent
  - Administrative capabilities (including creation of user accounts capability)

Risk Area:
Segregation of Duties (SoD)

• Agencies showed a lack of awareness with regards to designing and implementing appropriate Segregation of Duties controls and processes.

• Key functions and processes for which access should be segregated were often undefined.



• Inadequate design of Segregation of Duties prior to business re-organisation and system implementation/ upgrades.

• Segregation of Duties was often treated as an after-thought, resulting in high costs, inefficiencies and exposure to financial and reputational risk.

• Lack of formal periodic Segregation of Duties reviews.

• Reviews often fell short of the required level of detail to mitigate risks.

• Access was not assigned in accordance with the users' defined role.

• System developers at several agencies had unrestricted access to commit changes in the production system.

Risk Area: SAP Security Management

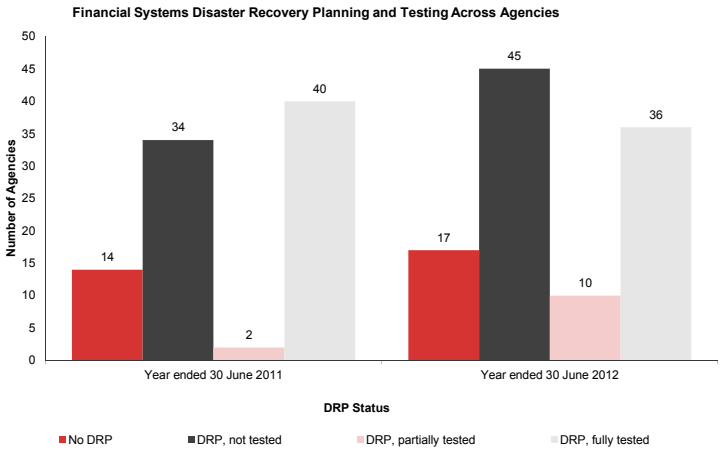
- Configuration Management
  - Production client
  - Password parameters
  - Workflow
  - SAP built-in configurations settings
  - Users with capabilities to perform all types of configuration management
- Audit Logging
  - Configuration
  - Reviews
  - Escalation & follow up

Risk Area: Change Management

- Application Changes
  - Documented types of application changes made in the financial year
  - Approvals
  - Testing
  - Comparison of approved request forms & changes in SAP
- Transport management
  - Users with capability to perform transports
  - Transport path

Risk Area: Disaster Recovery Management

- Issues Raised by Audit Office of NSW (for 2011 & 2012):



Risk Area: SAP Projects

- Many organisations see business transformations or process changes as not required with SAP implementations or major upgrades. Typically, it is viewed as just a technical upgrade.
- Security is usually an after-thought or overlooked during SAP implementations or major upgrades.
- Automated configurations are not fully explored as a criteria for SAP implementations or major upgrades.
- **As a result, typically seen would be manual workarounds or costly changes. Also, increased risk, unauthorised transactions & fraud.**

So What Can You Do? (An Auditor's Perspective)

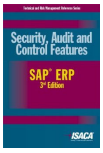
audit office OF NEW SOUTH WALES

- Establish or extend the organisation's risk management practices in managing SAP.
- Design and implement controls that addresses the high risk areas, common audit issues, common SAP weakness pitfalls and any compliance/ regulatory compliance requirements.
- Establish a program for the effectiveness of the controls over a period of time (and not just at implementation stages)

Helpful Tools and Resources

audit office OF NEW SOUTH WALES

- Tools:
  - GRC
  - Firefighter
- NSW government resources:
  - Auditor General's Report (http://www.audit.nsw.gov.au/Publications/Latest-reports)
  - DFS guidelines
  - NSW Treasurer's Directions (section 730 – Internal controls for computer-based financial systems)
  - M2012-15: Digital Information Security Policy (http://www.dpc.nsw.gov.au/announcements/ministerial_memoranda/2012/m2012-15_digital_information_security_policy)
- Audit guides:
  - ISACA Security, Audit and Control Features of SAP ERP 3rd Edition
  - ANAO Better Practice Guides



Q&A

audit office
OF NEW SOUTH WALES