

Keynote

ITAL Library

Background and History

Most organisations are likely to have a wide range of different technology environments from desktop operating systems such as Windows and Unix to applications using databases such as SQL Server and Oracle. Many audit plans will include reviews of the controls over these technology environments. This is one of the most complex IT audit topics often requiring scarce and expensive specialist advice. The PAWS IT Audit Library provides a risks and controls library, together with audit tests and tools to collect audit evidence for a range of popular environments. The IT Audit Library uses a common approach to all technology platform audits, and aims to simplify this complex topic and reduce the need for specialist assistance.

Audit Scope

We should first consider the purpose of the audit. This is to provide an opinion on the controls in place to manage the associated risks. Does it matter whether the platform under review is Windows or Unix based, indeed does it matter whether it is an operating system or a database environment under review? By concentrating on the fundamental components of the audit review, namely processes, risks and controls, we can develop a common scope that can be applied to all of our audits. Imagine the time that can be saved in avoiding the need to design audit programmes for each new technology platform audit.

Most IT auditors will be familiar with COBIT, this is the most widely adopted framework throughout the IT auditing community, and is also available as a PAWS risks and controls library. We will use this framework to help structure our technology platform audits. To begin, we must identify which control processes and objectives are relevant to our technology platform audits. We initially note as relevant the process, 'DS5 Ensure System Security', and in particular the associated objectives:

- DS5.3 Identity Management

- DS5.4 User Account Management

- DS5.5 Security Testing, Surveillance and Monitoring

- DS5.6 Security Incident Definition

- DS5.7 Protection of Security Technology

- DS5.9 Malicious Software Prevention, Detection and Correction

- DS5.10 Network Security

On further investigation, we discover that a number of other processes and objectives are also relevant to the technology platform audit. Consider, 'DS3 Manage Performance and Capacity', 'AI6 Manage Changes', 'DS9 Manage the Configuration', 'DS11 Manage Data', 'DS12 Manage the Physical Environment', 'PO2 Define the Information Architecture', and even elements of 'PO4 Define the IT Processes, Organisation and Relationships' in the review of roles and responsibilities, segregation of duties, and reliance on key IT personnel. We are now able to define an outline COBIT compliant process and objective, scope for all our technology audits.

Keynote

Risks and Controls

The next step is to define the specific risks and controls. The risks and controls for any system are common across all systems, irrespective of the detailed nature of how the controls are implemented. Consider for example the risks associated with identity management. These will include unauthorised access, inappropriate access and lack of accountability.

Taking unauthorised access, this is normally managed through the implementation of authentication controls. While there have been huge advances in alternative mechanisms, such as biometrics, authentication controls remain primarily as passwords. Even passwords themselves are similar across a range of technology environments. Password controls often enforce a minimum password length and require a mixture of upper and lower case characters or the inclusion of numerical digits. They may also include checks against a dictionary of common words and a history of previous passwords to prevent the re-use of recently used passwords.

It does not matter whether we are looking at a Windows or Unix environment, or even whether we are looking at a SQL Server or Oracle database environment, the identity management process is relevant, the risk of unauthorised access is relevant, and authentication controls in the form of passwords are relevant. By expanding this concept to all of the COBIT processes and objectives included in our audit scope we can define a common set of risks and controls that can be applied to all our technology audits.

Audit tests

We must now determine the detailed audit testing to help us ascertain whether the controls have been implemented and operated as intended. The design and operation of controls will vary from technology environment to technology environment. This is where the IT Audit Library really takes things forward. We have designed the audit tests for each of the controls for a number of different environments. Therefore the IT auditor can use a common approach to all their technology environment audits armed with the toolset they need to carry out the assignment.

Extract Scripts

The review of configuration settings for each technology environment requires the use of system tools or system commands. The tools, commands and programming languages are specific to each individual environment and this is where the need for specialist advice is once again normally required.

However, the IT Audit Library contains extract scripts to automate the collection of audit evidence. The scripts are totally passive and written in clear text that can be read and verified by the system administrator. There is no requirement for the auditor to research and develop routines to extract information or take up the valuable time of the system administrators. They can simply request the extract scripts to be run, and then review the output reports. The auditor can reduce the time spent collecting evidence and concentrate on interpreting the results.

Keynote

How Pentana Can Help

The IT Audit Library is a set of risks, controls and audit tests, aligned to the popular COBIT framework which can be loaded into your PAWS package. The next time you carry out a technology platform audit you only need select the platform type, and PAWS will automatically create your audit programmes and test schedules. You then request the system administrator to run the supplied extract script and follow the instructions in the audit tests to complete your audit fieldwork.

The PAWS IT Audit Libraries can be used independently, but for maximum benefit they should be used in conjunction with the PAWS COBIT library which provides an overall structure for the detailed IT tests. PAWS IT Audit Libraries are available as SQL scripts that are run against the PAWS database to add library items. They are priced separately for Unix, Windows, Oracle and SQL Server. In addition, you will receive extract scripts to run against the relevant database or operating system log files that will produce reports as the basis for your detailed testing.

The PAWS IT Audit Library is easy to load and use, however should you require assistance we can help liaise with your IT teams to run the extract scripts, or even help you with completion of the field work, preparation of audit recommendations and presentation to IT management.