MOORE ClearComm

IT Assurance and Best Practice

Today`s Schedule

- IT Assurance
- Sectors and Personas
- Measuring Risk
- Positive Impact
- SOC2 and ISO 27001
- Questions

MOORE ClearComm

Guests:

Maritz Cloete
Director of IT Assurance Services

Benjie Ocquaye
IT Assurance Senior Manager

maritz.cloete@mooreclear.com
benjamin.ocquaye@mooreclear.com

IT Assurance Defined

A promise given to users of an IT infrastructure, to inspire (reasonable) confidence that (said) IT system performs in the way intended or claimed, within levels of acceptable risk.

Users can include customers, clients, stakeholders or suppliers.

IT Audit Defined

An examination of the IT infrastructure, policies and operations of an organization – supported by an evaluation, to suggest improvements:

- ✓ Evaluation of an organisations technology and systems
- ✓ Collecting and evaluating evidence of IT management and controls
- ✓ Reduces all / any existing or future risks
- ✓ Takes / recommends necessary steps and measures to ensure reliability and ongoing protection
- ✓ Focuses on: Strategy, Policy, Security and Technical Architecture

Purpose and Objectives

IT Assurance aims to ensure that IT systems are:

- ✓ Functioning properly and securely
- ✓ Protecting corporate assets
- ✓ Maintaining data integrity
- ✓ Aligning with the business's overall goals and objectives

Evaluation of the IT environment to identify areas of risk (using a framework such as COBIT) is fundamental.

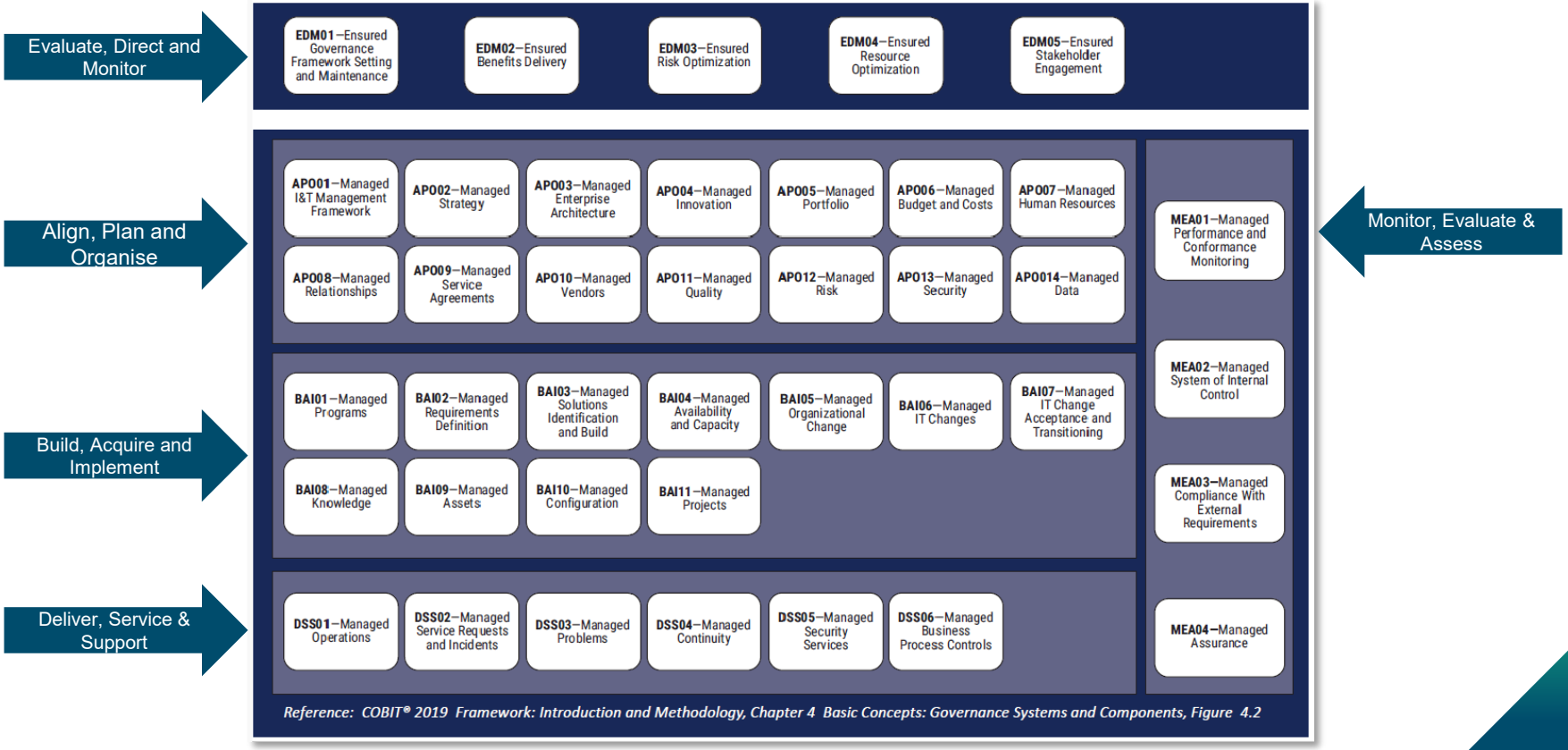
COBIT Framework

- ✓ Developed by the ISACA (http://isaca.org)
- ✓ Helps to organise IT function and to drive maturity in key processes – can work hand in hand with ITIT and ISO20000
- ✓ Sets out ‘control objectives’ – at a process level it defines what you should look to achieve
- ✓ Helps to align IT goals with business goals
- ✓ Great basis for IT Assurance programme of work – regardless of company size

ISACA Information Systems Audit and Control Association

MOORE ClearComm

COBIT Framework: Core Model



MOORE ClearComm

Sectors and Personas

Sectors and Industries

Sectors for whom IT Assurance should be particularly in focus:

- ✓ Financial Services
- ✓ Energy, Mining and Renewables
- ✓ Professional Services
- ✓ Manufacturing and Distribution
- ✓ Charity and Non-Profit
- ✓ Education
- ✓ Technology
- ✓ Healthcare
- ✓ Automotive
- ✓ Engineering

Reasons and Requirements

- ✓ Demand for 3rd party assurance – SOC1/2, ISO, etc
- ✓ SA315 for External Financial Audit
- ✓ Corporate governance requirement for independent assessment (ESG)
- ✓ Oversight requirements (e.g. within 3rd sector, schools, etc)
- ✓ Heightened awareness of Technology Risk within organisations:
  - Use of Hybrid/Cloud services
  - Business Resilience
  - Cyber Resilience

MOORE ClearComm

Managing IT Risk

Managing IT Risk

- ✓ Understand the organisations core objectives and purpose
- ✓ Understand the role the IT environment plays in achieving these objectives
- ✓ Define the organisations “IT Risk Surface”
- ✓ Factors in third-party service delivery
- ✓ Identifies risks that require management action
- ✓ Carry out actions, and re-evaluate

What is “Risk Surface”?

Any “location” where an organization’s reputation, assets, legal obligations, regulatory compliance, or ability to operate is at risk:

- ✓ Not limited to technical or digital infrastructure under your direct control
- ✓ Extends to areas where your assets are managed by third parties
- ✓ Supply chain risk is often overlooked
- ✓ Many organisations ignore (or are unaware) of their extended risk surface
- ✓ Technical, IT and Cyber Security risk management should protect the entirety of your risk surface

MOORE ClearComm

Case Study:
Internal Scrutiny

Case Study: MAT Cyber Security and Resilience Review

Trustees were concerned about the state of Cyber Security across the Multi Academy Trust's 10 primary schools. Instructed MCC to carry out independent review as part of annual internal scrutiny programme.

What We Did:
Carried out an assessment across all 10 schools, measured against good practice.

What We Found:
Highlighted significant variation in measures, due to

- Reliance on several different IT Service Providers across schools
- Cyber security requirements not included in contracts or SLAs
- Lack of Trust-wide security policies and procedures

Review Outcome:
Schools were quantifiably at risk of Cyber Attack, the audit brought specific risk areas to light, along with clear steps to address the risks identified.

MOORE ClearComm

IT Risk and Financial Reporting Audits

Audit Standards now demand IT Risk evaluation

1

Management & Auditors rely on Data

Explicitly or implicitly place reliance on the:

- Completeness
- Consistency
- Accuracy
- Validity and
- Timeliness

of data for significant classes of transactions

but

2

IT Systems

IT systems can be:

- Complex
- Poorly designed
- Incorporate poor practice or
- Abused in a manner not originally designed or intended for

therefore

3

ISA (UK) 315

ISA (UK) 315 mandates the evaluation of the Risk of Material Misstatement through the client's use of IT for each Significant Class of Transaction (SCOT)

Risks Auditors Worry About

Access

Access to systems are poorly managed, segregation of duties not enforced, accessible by unauthorised users

System Change

Changes to systems are not controlled, processing integrity could be under question

Cyber Security

Poor cyber security hygiene, system access and/or integrity could already be compromised

Data Interfaces

Shoddy data interfaces between systems, reliability of data moved between systems can be undermined

Disaster Recovery

Weak disaster recovery planning, questions over data quality post recovery

Migrations

System migrations in the year, questions over effectiveness of data migration

Case Study in Finance Reporting Audit

A global business consisting of multiple entities, a large proportion of which are international:

- Largest entity has turnover of circa £60.8m (53% of group turnover)
- All entities are recruitment businesses

What We Did:

- Required mapping of data flows specific to financial reporting process
- Identify key risks that could lead to material misstatement (Change Controls, Access Controls)
- Tested controls to confirm these operated effectively over the reporting period

Review outcome:

- Provided audit team with assurance that the information from the key systems can be relied upon
- Identified opportunities for improvement in client control environment

MOORE ClearComm

Positive Impact

Tangible Impact

- ✓ Proactive approach to identifying and treating IT risks before they materialise
- ✓ Mitigation of impact(s) should the risk(s) materialise
- ✓ Improvements to overall organisational resilience
- ✓ Demonstration of IT risk awareness / proactiveness to partners, suppliers and customers, and security culture
- ✓ Findings typically feed into IT strategy
- ✓ Meeting of compliance requirements

MOORE ClearComm

Questions

maritz.cloete@mooreclear.com
benjamin.ocquaye@mooreclear.com
richard.jackson@mooreclear.com

Our Next Webinar

Data Protection: Are You Compliant?

Date: Wednesday 22nd May

Time: 10.00am-11.00am

Panel:

- Rich Jackson, Strategic Business Manager (Moore ClearComm)
- Meagan Mirza, Senior Data Protection Officer (Moore ClearComm)

Location: Zoom

MOORE ClearComm

Moore ClearComm
9 Appold Street
London
EC2A 2AP
t: +44 (0)20 45821983

www.mooreclear.com

MOORE ClearComm