NEbraskaCERT

Cybersecurity Forum
August 19, 2015
COBIT 5
Lets Play 50 Questions
(more or less)

- Michael T Hoesing 402 981-7747
- CISSP, CISA, CCP, ACDA, CIA, CFSA, CMA, CPA
- mhoesing@unomaha.edu
- (broke faculty, do not sue me)

University of Nebraska Omaha

a CAE IAE institution

COBIT 5 Background

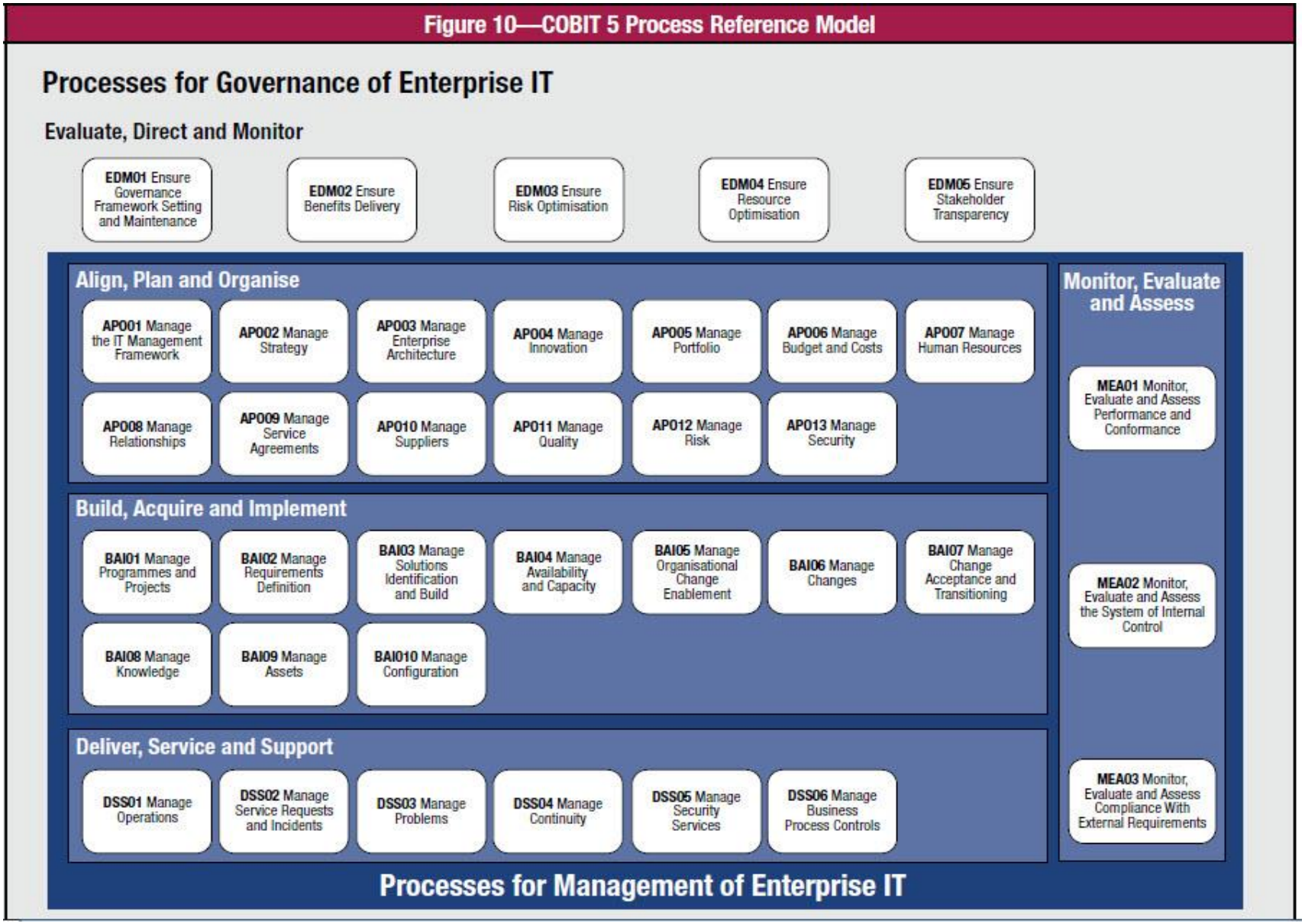
COBIT 5 Parts and Pieces

- **Enabling Processes** – 234 pages, explains the 37 process categories that used to be the 34 process categories in 4.1 ($135 non-members)
- Framework – 94 pages, explaining the goals background and structure of the new multi component COBIT 5 , ($50 non-members)
- COBIT 5 for Information Security – 220 pages ($175 non-members)
- Implementation – 78 pages now to deploy COBIT5 ($150 non-members)
- For Assurance – 318 pages how to run an IS audit shop ($80 non-members)

Process Groups

COBIT 5	CobiT 4.1
Evaluate, Direct, Monitor (Governance, RiskIT)	n/a
Align, Plan , Organize (ValIT)	Plan and Organize
Build, Acquire, Implement	Acquire and Implement
Deliver, Service, Support	Deliver & Support
Monitor, Evaluate, Assess (Management)	Monitor & Evaluate

COBIT 5 37 Processes



Source ISACA/ITGI COBIT 5 page 33

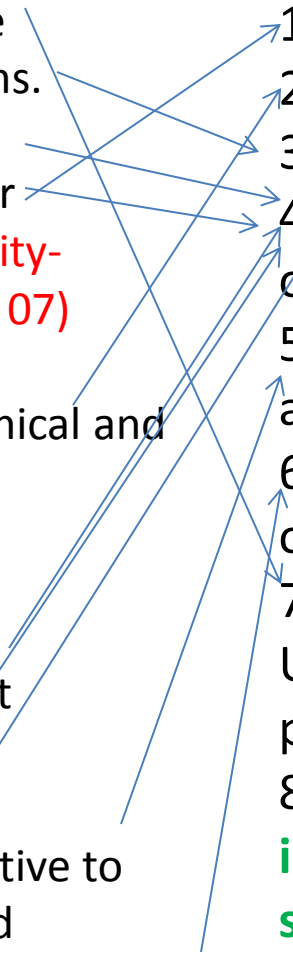
DS 5.3 and 5.4 - Are Now DSS 05.04 Identity Management & User Account Management

DS 5.3 Identity Management

1. Users uniquely identifiable
2. Authentication mechanisms.
3. Confirm user access rights
4. Approved by system owner
5. Implemented by the security-responsible person (see APO 07)
6. Use a central repository
7. Deploy cost-effective technical and procedural measures

DS 5.4 User Account Management

1. User account management procedures
2. Approval procedure
3. Rights and obligations relative to access contractually arranged
4. Perform regular management review



DSS 05.04 Identity Management

1. Maintain aligned user access rights
2. Uniquely identify roles
3. Authenticate all access
4. Administer all changes timely, based only on approvals
5. Segregate and manage privileged user accounts.
6. Perform regular management review of all accounts and related privileges.
7. Users are uniquely identifiable. Uniquely identify all information processing activities by user.
8. **Maintain an audit trail of access to information classified as highly sensitive**.

COBIT 5 Show What you Know

Goal Cascade & Alignment

IT related goals:

a) Flow from stakeholder needs
b) Flow from Enterprise goals
c) Need to be aligned with Enterprise goals
d) All of the above

D All of the above
This is the COBIT theme of Cascading Goals, IT does not work in a vacuum, everything IT does must flow from above. “Alignment” is one of the most frequently used words in COBIT5, taken from the deprecated ValIT.

The Process Model

- The correct Life Cycle sequence is :
  a) Design → Plan → Build → Dispose
  b) Plan → Design → Build → Dispose
  c) Plan → Design → Monitor → Use
  d) Plan → Design → Dispose → Monitor

B Plan → Design → Build → Dispose
Planning is about direction and strategy, Designing is about choosing from alternate paths to implement the Plan. Monitoring is how the Process Model is managed and is not part of the Process Model.

Governance vs Management

Governance provides guidance and Management plans, builds, runs and monitors activities aligned with the guidance.

TRUE Governance provides direction and policies at an enterprise level and IT management performs actions on their scope of work aligned (get used to that word) the organizations overarching governance.

COBIT Structure for the 37 Processes

- Each of the 37 Enabling Process documents has the components of:
  A. An identifier (EAMnn, DSSnn,…)
  B. Description
  C. Purpose
  D. Where the goals cascade from
  E. Goals of the process and associated measurement metrics
  F. Personnel roles (responsible, accountable, consulted, informed)
  G. Process description
  H. Related guidance
  I. All of the above

I All of the Above – this was more informative than a question, I do that sometimes in tests to baffle students

Governance Accountability vs Responsibility

The Accountable and Responsible parties for evaluating, directing and monitoring the IT governance program are, respectively

a) Board, CIO (Chief Information Officer)
b) CIO, Board
c) Board, Audit
d) Board, CRO (Chief Risk Officer)

A The Board is accountable to the stakeholders and the CIO is responsible for execution of, the IT governance program.

Auditing Benefits Delivery

Determining the level of stakeholder satisfaction with IT's optimization of benefits could involve which IS audit evidence gathering technique:

a) review, or generation, of questionnaires (surveys)
b) penetration testing
c) vulnerability scanning
d) reviewing configuration files

A COBIT 5, for several of the 37 processes, states a measurement of success (goal achievement) is stakeholder satisfaction, and stakeholder feedback should be solicited by IT Management and reviewed by the auditor.

Measuring IT Risk Management

In COBIT 5, the most frequently used factor in measuring IT risk goal attainment is related to:

a) Incidents
b) Staff Turnover
c) Share price
d) Management Turnover

A If IT management is effective managing risk incidents and breaches (insert hot sexy word "CyberSecurity" here) will be minimized.

Optimizing Asset Utilization

In EDM04, the IT architecture plan/strategy does not include safeguarding assets, that topic is covered in DSS05 only.

FALSE While safeguarding assets is an important factor in the Information Security process DSS05, unprotected assets are subject to waste which reduces asset optimization.

Stakeholder Transparency

Reporting should be:

a) Accurate
b) Timely
c) Based on service level agreements, both internal and external, where appropriate
d) All of the above

D All of the above – SLAs, are valuable internal management tools and not just reserved for external parties

Committees

The IT Strategy committee should be at the Board level while the IT Steering committee should be at the business executive level.

TRUE Verbatim from APO-01

Risk Management Scope

The IT asset inventory does not include processes performed by outside vendors.

FALSE you can outsource the execution of a process, but you can not outsource the accountability for the risk of the process.

IT Strategy & the Asset Life Cycle

The IT Strategy, an evolving document, should consider:

a) Existing technology
b) Emerging technology
c) Declining technology
d) All of the above

D All of the Above – is the current state effective at achieving SLAs? Could some newer technology be more effective? Are we using technology outside of the vendor's support window which increases risk?

Data Dictionary

A data dictionary should include:

a) A data owner
b) Security classification level
c) Retention guidelines
d) Destruction requirements
e) All of the above

E All of the Above – Data is one the most important information assets and, should have an accountable party, be risk assessed, have a determined life cycle and procedures for end of life

Innovation Accountability

It is business unit management's primary role to be aware of new IT developments and their applicability to furthering the organization's goals and it is IT management's primary goal with respect to innovation to support them with research and testing.

FALSE – IT should take the lead in being aware of new technologies and educate the business unit on what is available so the business unit can decide the applicability to operations and what are the next steps

Innovation Success Measurement

The measurement metric “Percent of implemented initiatives that realiz/se the envisioned benefits.” Implies:

a) all initiatives should be implemented.
b) all implemented initiatives will be successful.
c) It is difficult to predict the future accurately, but the degree to which targets are missed should be measured, trended, and compared with peer averages
d) None of the above

C – while 100% realization of benefits is ideal, the practical answer, usually driven by cost considerations, is that an overly optimistic plans seldom get implemented with all the features desired

Project Success Measurement

Two key success criteria of IT initiatives:

a) On time and within budget
b) Increased revenue and decreased costs
c) Decreased headcount and more local tax incentives
d) Decreased Compliance and increased Legal costs

A – IT should have project management techniques in place to monitor and control resource consumption aligned with progress toward the benefits achievement, revenue generated by a project is a business unit accountability, specific costs and cost reductions vary by project, timelines and budgets are common across all projects

IT Cost Allocations

IT Cost allocation models should be designed by IT management, the experts, without involvement of business unit management.

FALSE – IT provides services and the business unit decides how those services should be consumed and business unit should set the cost allocation rules to optimize utilization/consumption

IT Human Resource Management

Inability to hire specific critical long-term IT skills is an issue that can be best overcome with:

a) Engaging consultants
b) Hiring someone with almost all the skills then provide incremental training
c) Throw that technology away without consulting the business units
d) Relocate the position to the business unit

B – Consultants provide short-term solutions but seldom are cost effective as long term solutions, the technology may be critical to current business operations and be difficult to replace, kicking the can down the org chart just prolongs the problem

IT & Business Unit Relationships

Establishing a single point of contact within IT for each business unit:

a) Provides clarity in the communication channel
b) Can provide a consistent story is told by IT
c) Can provide efficiency if the appropriate person is placed in the role
d) All of the above

D – the key is getting the correct person in the liaison role, technically competent, but can explain technology to the business unit on their terms while knowing the business unit's operations

OLAs (Operating Level Agreements)

OLA's (Operating Level Agreements) specify technology oriented processes used to support one or more SLAs. For example, an OLA of applying critical, relevant, tested, vendor operating system patches within XX hours of release, which reduces the chance of viruses or malware on the operating system, this supports the SLA that any application running on that operating system have an uptime of YY%.

TRUE – OLA another favorite phrase in COBIT 5

IT Vendor Management

Vendor contracts should address terms such as:

a) Continuity procedures and timeframes
b) Use of substitute vendors or subcontractors
c) Days notice before termination by either party
d) Availability of data
e) All of the above

E All of the above – while not a complete list, all of the above should be considered

IT Quality Monitoring

APO-11 regarding quality monitoring does ***not*** include:

a) Frequent use of the word “Continuous”
b) Only measure events over $1 million
c) Determine root cause of issues
d) None of the above

B Materiality is not specifically mentioned in APO-11, relevance and risk-based are guiding terms, a lot of little issues can represent a larger problem

Risk Types

"Public comment or embarrassment" is best described as:

a) Inherent risk
b) Intrinsic risk
c) Extrinsic risk
d) Reputation Risk

D Public perception can put you out of business if it is negative

Realized Risk (Incident) Response

Incident response plans should not include steps to minimize the spread of the risk impact since the vulnerability is now a reality.

FALSE containment of the damage is definitely part of an incident response plan

ISMS Information Security Management System

The scope of an Information Security Management System (ISMS) may not include:

a) Being primarily accountable for a function such as Business Continuity if that is handled by a specifically designated group outside of IT. Any ISMS scope exclusions must be approved at an appropriate level.

b) Maintaining a list of security solutions as part of the IT architecture

c) Consider information security policy creation, training and awareness

d) Adjust solutions based on monitoring results

A while Information Security has a key role in BCP, BCP is usually an organization-wide activity and may be better managed as not just an IT thing (DR)

Management of IT Projects

- Project plan considerations include:
  a) The critical path
  b) Interdependencies with other resources IT and non-IT
  c) Coordination with other projects
  d) Communication channels and frequency
  e) All of the above

E there are more factors but these keys are stated in COBIT

Accreditation

Accreditation in COBIT 5 is :

a) An AACSB certification of your accounting & auditing program
b) A NSA certification of your information security educational program as a CAE-IAE
c) The attestation by the project requestor and IT, based on test results, that the project substantially provides the benefits desired in the request as adjusted for appropriately approved modifications
d) All of the above

C sorry, had to make sure occasionally "all of the above" is not always the correct answer to keep you on your toes"

Requirements

The requirements drive the consideration of solutions and choices are made by stakeholders from alternate solutions based upon

a) Feasibility
b) Cost
c) Risk
d) All of the above

D a balanced application of these three criteria will optimize the benefits/resource consumption trade-off, remember to "build security in" to help manage risk, rather than band-aid it on later

Testing Systems, Acquired or Built

Testing acquired or constructed systems may include all except:

a) Peer review of one technical professional of another's work
b) Acceptance or accreditation testing involvement by the business unit
c) Independent or integration testing by a QA group
d) Discarding documentation of resolved issues as they can not be beneficial for other projects, and they are already fixed, and shredding these reduces our discovery footprint

D while testing has a cost, testing at various times by various interested parties can reduce later expensive re-work, issues lists can be a foundation of a knowledge base that helps avoid mistake repetition

Capacity Management

Technology assets, such as a data storage device, should :

a) Be Acquired in the largest units possible to avoid running out of resources
b) Have their acquisition postponed until existing assets are filled up, this will lower our cost per unit
c) Be monitored to enable utilization decisions to be considered timely before asset failure
d) Sign a Cloud contract with an unlimited storage clause

C Excessive resources trigger unnecessary costs, insufficient resources can result in failure, monitoring can help provide appropriate resource balance to reduce both issues

Change Enablement

Motivating staff to embrace the change authorized at an appropriate level may include:

a) Frequent communication of the vision of the change
b) Clear communication of benefits
c) Prompt correction of issues, hopefully few or none, in earlier deployments
d) Training opportunities to allow for adjustment to the new processes
e) Communicate “quick wins” from earlier deployments of the solution if available
f) All of the above

F change benefits must be re-enforced and affected parties must be energized (communication) and empowered (training)

Change Evaluation

The change evaluation process should consider effects upon:

a) Inter-dependent technologies
b) Legal or contractual obligations
c) Security
d) All of the above

D a change seldom only affects the item changed, consider downstream and upstream impacts, and "build security in"

Change Implementation

At implementation the following should be ready:

a) Updated procedures
b) Updated system documentation
c) Trained users
d) All of the above

D many affected parties not part of acceptance testing need to know what changed and how it impacts their roles, accountabilities and workflow

Knowledge Management

Bury all evidence of prior failures:

a) To eliminate litigation discovery
b) To avoid an disgruntled employee posting it on tweetangrybearsbook
c) So your competitors will not find out
d) None of the above

D the real issue of a mistake, is the failure to learn from it

Assets From Suppliers

To manage acquired assets:

a) Know the vendors asset life expectancy term
b) Understand when vendor support expires
c) Limit vendor access to assets
d) Change vendor default passwords
e) All of the above

E Understand when the vendor expects the asset to be replaced, restrict and monitor vendor access to information assets

Configuration Management

A repository of approved configuration settings and associated changes can be used to:

a) Timely on-board a new copy of the same asset
b) Facilitate consistent management of resources
c) Audit existing copies of that asset for configuration drift
d) All of the above

D Standards promote efficiency in deployment and operation and provide a baseline for assurance assessments

Operations Management

Effective and efficient operations are characterized by

a) Documented and scheduled IT processes
b) Monitored IT processes to ensure key outputs are created at specified times.
c) Creation of backups of critical data and systems
d) All of the above

D Plan, Execute and Prepare for contingencies

Logging

Journalizing IT events to a log is a balance of not overwhelming the log with repetitive approved events that make research difficult and missing valuable research data with insufficient logging.

TRUE Chronological recording of IT events should capture useful data without creating production issues.

IT Assets

Many IT assets, particularly hardware :

a) Need to operate in climate conditions specified by the manufacturer
b) Need protection from nature's risks (flood, fire)
c) Should have appropriate levels of risk-shifting using insurance
d) All of the above

D Assets need protection from the elements, and if the cost of protection gets excessive, risk-shifting may be beneficial

Incident Management

Requests and incidents need to be classified to:

a) Assist with prioritization
b) Facilitate the appropriate level of resources are deployed to resolve the issue
c) And combined with a Knowledge Base, the correct type of resources are deployed to resolve the issue
d) All of the above

D Planning before an incident will facilitate the appropriate deployment of resources

Problem Resolution

Resolutions to problems could be:

a) Temporary workarounds
b) Permanent fixes
c) Vendor supplied solutions
d) Any of the above

D Don’t limit where you look for help resolving issues

Business Continuity Planning

A Business Impact Analysis (BIA)should:

a) Help to prioritize the order in which to recover portions of the business
b) Minimum time to recover (how long would it take)
c) Maximum tolerable outage (how much time do we have)
d) All of the above

D Determining the recovery order and the required times and the times before major negative impact allows for a coordinated recovery effort

Endpoint Security

Endpoint security involves:

a) Secure configuration of the operating system
b) Encryption of storage devices
c) Disposition procedures that ensure data is removed
d) All of the above

D Data should be at rest in a secure environment

Physical Security

Ensuring appropriate access to facilities includes:

a) Approval from the appropriate party is not required
b) Issuance of consistent badges that do not designate employees from visitors
c) Allowing unescorted visitors
d) Not using additional authentication factors (palm, retina, keypad,…) based on risk
e) None of the above

E All of these items are components of sound physical security

Network Security

Network security techniques include:

a) Limit connection to authorized devices
b) Require known user authentication when connecting
c) Encrypt transmissions of sensitive data
d) Configure network components per security policy requirements
e) All of the above

E All of these items are components of sound network security

Data Validation

Data creation controls can include:

a) Validating the originator has the authority to do so

b) Segregation of transaction creation and transaction approval

c) Edit routines to validate data

d) All of the above

D Authorization, SOD, and validation help ensure quality data

Monitoring

Review the coverage of the internal and independent assessments and map their scope to the areas in the risk assessment, particularly high risk areas.

D Monitoring should be risk based.

Questions ??

You are not seriously thinking about getting up?

Where would you like the scar?