What is IT Governance?

IT Governance
Rich Flanagan

FOX | ITACS
Master of IT Auditing & Cyber Security

Good IT Governance

=

Right Things, Done Right

IT Governance
Rich Flanagan

FOX | ITACS
Master of IT Auditing & Cyber Security

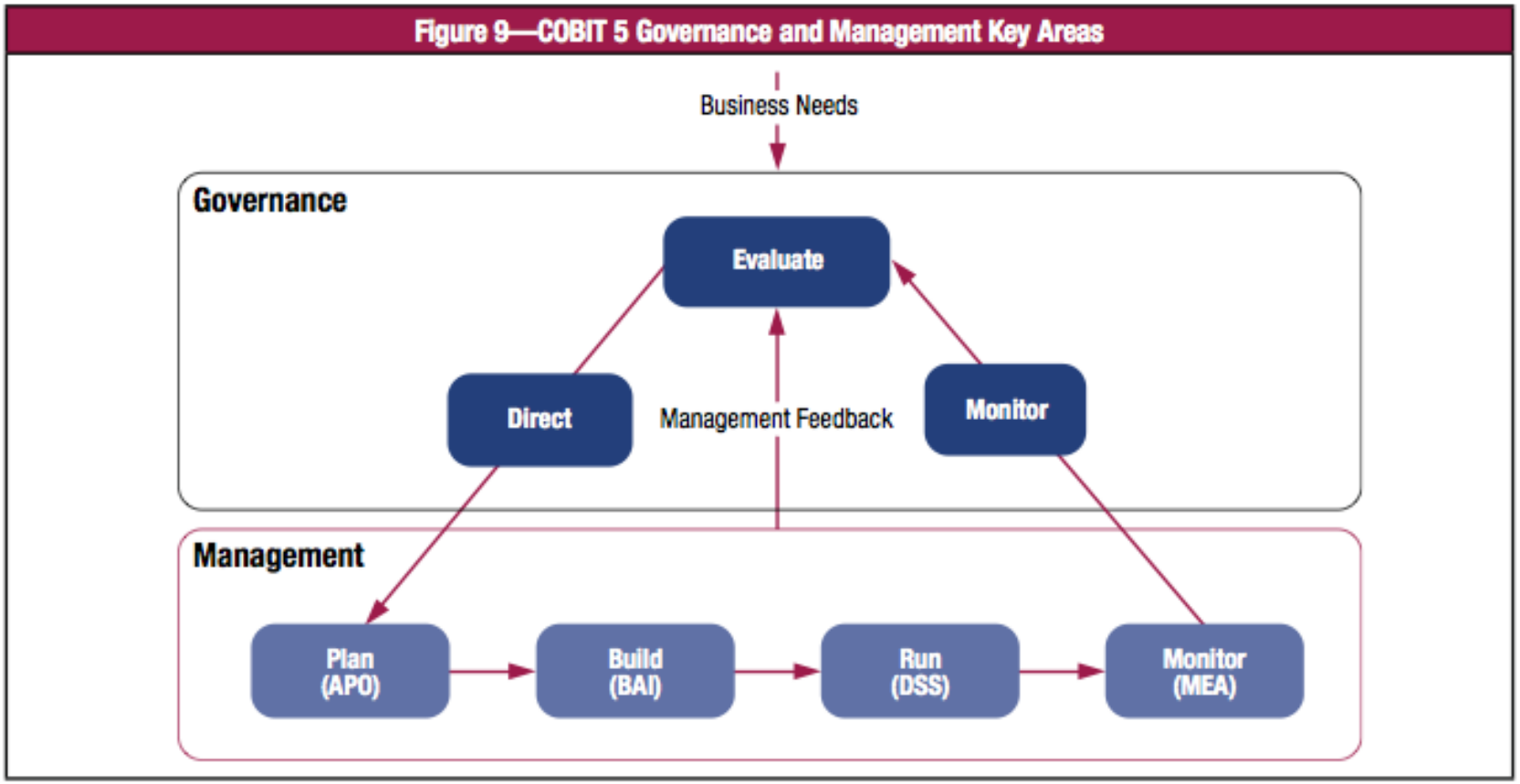
What is IT Governance?

- **Its about doing the right thing…**
  - Who gets to decide?
  - How are we aligned to the business strategy?
  - Are we working on things that will produce the most value?
- **and then, doing them right.**
  - Are we operating under control?
  - Do we run our projects well?
  - Do our services meet our customer's needs?
  - Do we protect the information that is vital to our organization?

What is COBIT 5?

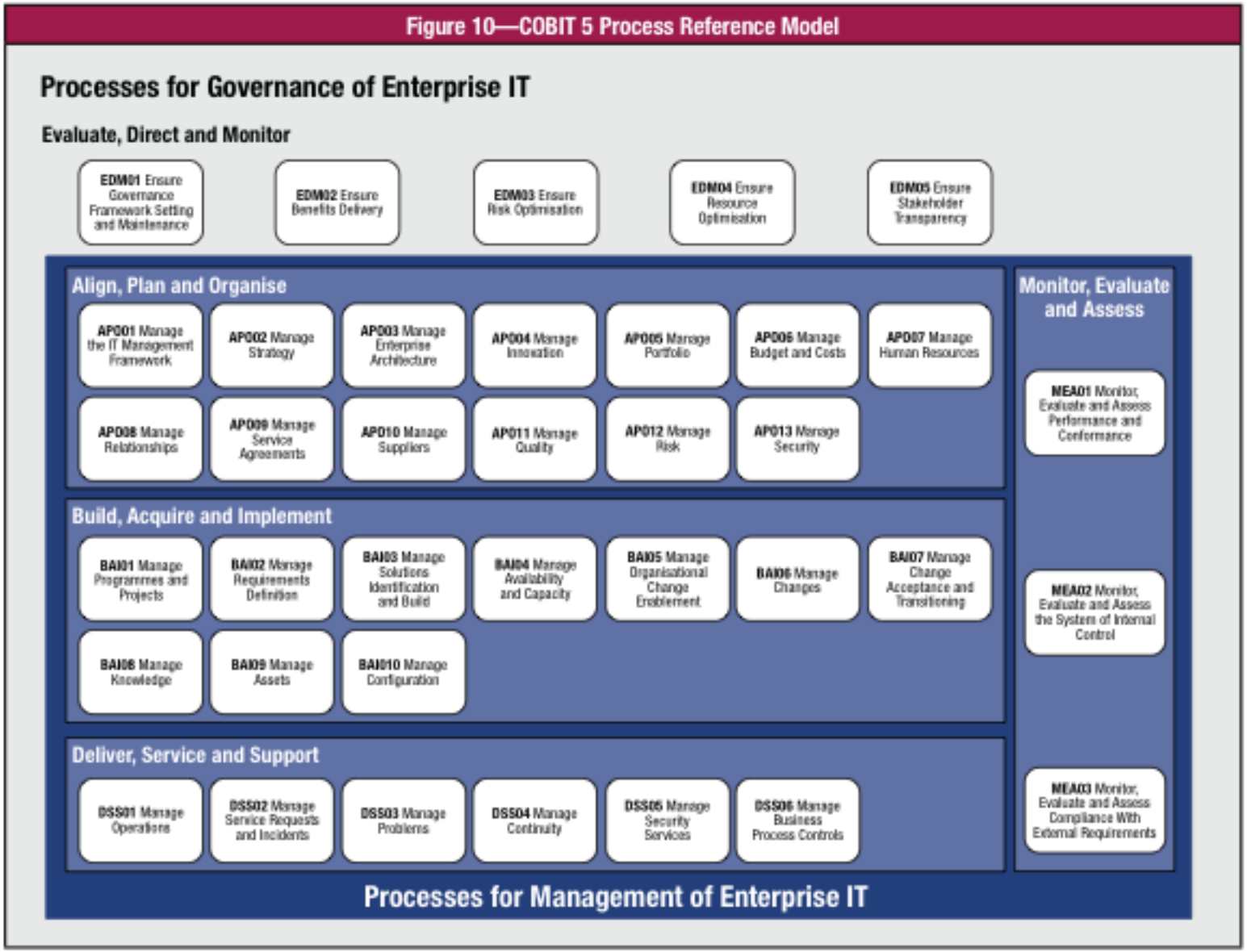
- Its about best practice.
- It tries to cover IT end-to-end.
- It tells you what you need to be thinking about when running (or auditing) IT.
- Its not about the technology, its about the processes you use to deliver technology.
- Its about how to decide what you do(Right Things) and then how to do them in an efficient, effective and secure manner (Done Right).
- It is critical that you understand the processes it recommends.

COBIT 5



IT Governance
Rich Flanagan

FOX | ITACS
Master of IT Auditing & Cyber Security



IT Governance
Rich Flanagan

FOX | ITACS
Master of IT Auditing & Cyber Security

APO07 Manage Human Resources	Area: Management Domain: Align, Plan and Organise
Process Description Provide a structured approach to ensure optimal structuring, placement, decision rights and skills of human resources. This includes communicating the defined roles and responsibilities, learning and growth plans, and performance expectations, supported with competent and motivated people.	
Process Purpose Statement Optimise human resources capabilities to meet enterprise objectives.	
The process supports the achievement of a set of primary IT-related goals:	
IT-related Goal	**Related Metrics**
01 Alignment of IT and business strategy	• Percent of enterprise strategic goals and requirements supported by IT strategic goals • Level of stakeholder satisfaction with scope of the planned portfolio of programmes and services • Percent of IT value drivers mapped to business value drivers
11 Optimisation of IT assets, resources and capabilities	• Frequency of capability maturity and cost optimisation assessments • Trend of assessment results • Satisfaction levels of business and IT executives with IT-related costs and capabilities
13 Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards	• Number of programmes/projects on time and within budget • Percent of stakeholders satisfied with programme/project quality • Number of programmes needing significant rework due to quality defects • Cost of application maintenance vs. overall IT cost
16 Competent and motivated business and IT personnel	• Percent of staff whose IT-related skills are sufficient for the competency required for their role • Percent of staff satisfied with their IT-related roles • Number of learning/training hours per staff member
17 Knowledge, expertise and initiatives for business innovation	• Level of business executive awareness and understanding of IT innovation possibilities • Level of stakeholder satisfaction with levels of IT innovation expertise and ideas • Number of approved initiatives resulting from innovative IT ideas
Process Goals and Metrics	
Process Goal	**Related Metrics**
1. The IT organisational structure and relationships are flexible and responsive.	• Number of service definitions and service catalogues • Level of executive satisfaction with management decision making • Number of decisions that could not be resolved within management structures and were escalated to governance structures
2. Human resources are effectively and efficiently managed.	• Percent of staff turnover • Average duration of vacancies • Percent of IT posts vacant

IT G
Rich

AP007 RACI Chart																								
Key Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
AP007.01 Maintain adequate and appropriate staffing.									R		I				R			A	R	R	R	R	R	R	R	
AP007.02 Identify key IT personnel.									R						R			A	R	R	R	R	R	R	R	
AP007.03 Maintain the skills and competencies of personnel.									R						R			A	R	R	R	R	R	R	R	
AP007.04 Evaluate employee job performance.									R						R			A	R	R	R	R	R	R	R	
AP007.05 Plan and track the usage of IT and business human resources.					R	C	A	R	R						I			R	R	R	R	R	R	R	R	
AP007.06 Manage contract staff.									R						R			A	R	R	R	R	R	R	R	

IT Governance
Rich Flanagan

FOX | ITACS
Master of IT Auditing & Cyber Security

AP007 Process Practices, Inputs/Outputs and Activities				
Management Practice	**Inputs**		**Outputs**	
AP007.01 Maintain adequate and appropriate staffing. Evaluate staffing requirements on a regular basis or upon major changes to the enterprise or operational or IT environments to ensure that the enterprise has sufficient human resources to support enterprise goals and objectives. Staffing includes both internal and external resources.	**From**	**Description**	**Description**	**To**
	EDM04.01	• Approved resources plan • Guiding principles for allocation of resources and capabilities	Staffing requirement evaluations	Internal
	EDM04.03	Remedial actions to address resource management deviations	Competency and career development plans	Internal
	AP001.02	Definition of supervisory practices	Personnel sourcing plans	Internal
	AP006.03	• Budget communications • IT budget and plan		
	Outside COBIT	• Enterprise goals and objectives • Enterprise HR policies and procedures		

Activities
1. Evaluate staffing requirements on a regular basis or upon major changes to ensure that the: • IT function has sufficient resources to adequately and appropriately support enterprise goals and objectives • Enterprise has sufficient resources to adequately and appropriately support business processes and controls and IT-enabled initiatives
2. Maintain business and IT personnel recruitment and retention processes in line with the overall enterprise's personnel policies and procedures.
3. Include background checks in the IT recruitment process for employees, contractors and vendors. The extent and frequency of these checks should depend on the sensitivity and/or criticality of the function.
4. Establish flexible resource arrangements to support changing business needs, such as the use of transfers, external contractors and third-party service arrangements.
5. Ensure that cross-training takes place and there is backup to key staff to reduce single-person dependency.