Webinar on
The Importance of
IT Governance for NGOs

Vincent Ip

Hon. Secretary and Treasure

Professional Information Security Association

9 January 2024

Agenda

Why do we need IT Governance?

Basic Areas of IT Governance

- Strategic Alignment
- Architecture
- Risk Management
- Performance Management
- IT Service Management

What is IT Governance

- Ensures Business and IT strategy alignment
- Ensures IT investment support business objectives
- Provides performance measure
- Part of Corporate Governance

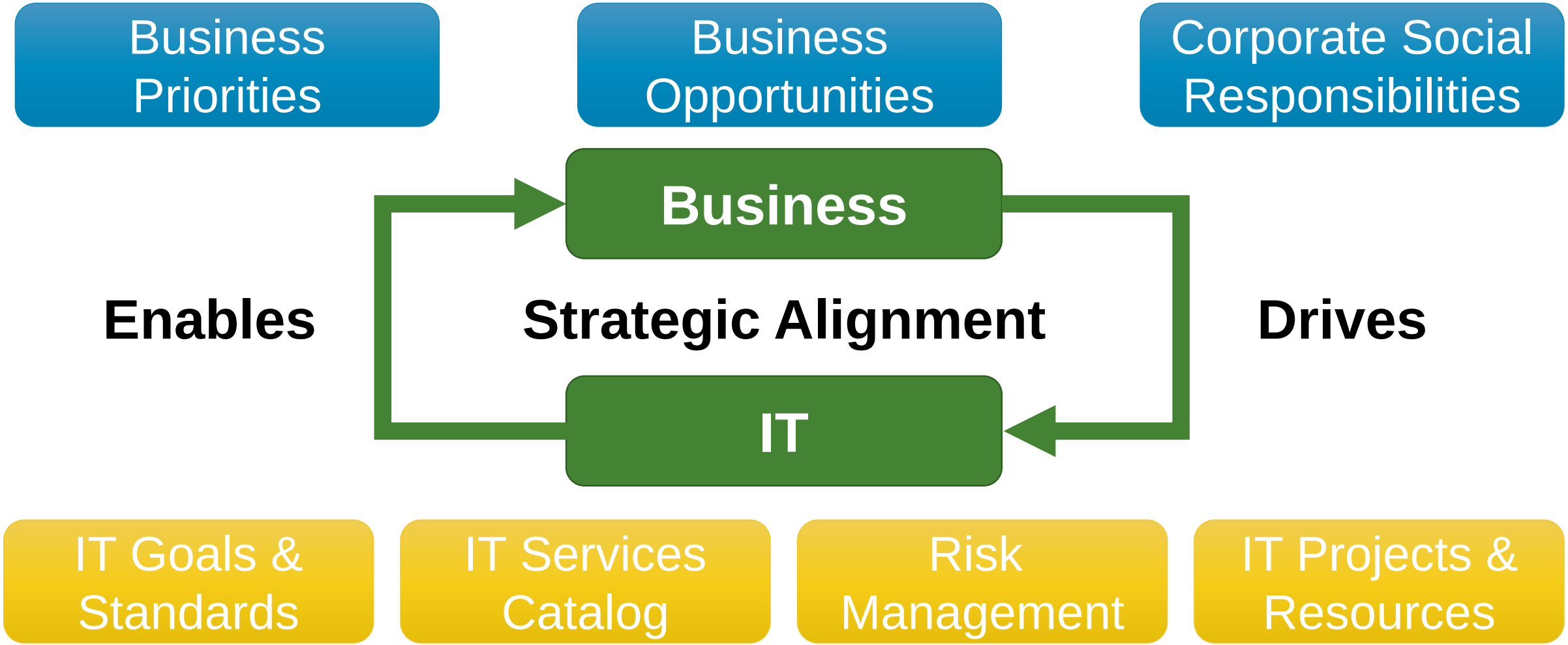
IT Governance is NOT

- IT Governance is NOT Management
- IT Governance is NOT Governance, Risk & Compliance
- IT Governance is NOT internal audit

Strategic Alignment

- Focus on ensuring the linkage of business and IT plans
- Define, maintain, and validate IT value proposition
- Aligning IT operations with enterprise operations/processes
- Ensure that an organization’s IT investment is in harmony with their strategy objectives

Strategic Alignment



IT Governance and Management

Governance

- Board Level
- Focus more on strategic

Management

- Executive Level
- Focus more on operational

Why do We Need IT Governance?

- Mitigate risk and avoid waste, esp. essential for NGOs
- Produce value for business
- Build key measurement for business about IT performance
- Improve stabilities and resilience of services
- Optimize cost, invest better
- Operate more efficiently
- Speed up IT response to business needs
- Reduce the chance of overran, over-budgeted projects, avoid pet projects

Why do We Need IT Governance?

- Mitigate risk and avoid waste, esp. essential for NGOs
- Produce value for business
- Build key measurement for business about IT performance
- Im
- Op
- Op
- Spe
- Reduce the chance of overran, over-budgeted projects, avoid pet projects

Build up confidence of management about IT

Why do We Need IT Governance?

- Mitigate risk and avoid waste, esp. essential for NGOs
- Produce value for business
- Build key measurement for business about IT performance
- Im
- Op
- Op
- Spe
- Reduce the chance of overran, over-budgeted projects, avoid pet projects

It’s even more essential for NGO with limited resources, error budget is lower

What Happens without Proper IT Governance?

https://www.theregister.com/2023/09/05/birmingham_city_council_oracle/

https://itassetmanagement.net/2023/09/06/did-birmingham-city-councils-disastrous-oracle-migration-contribute-to-its-bankruptcy/

ITAM review

News Events Resources Services Marketplace Subscribe

Did Birmingham City Council's disastrous Oracle migration contribute to its bankruptcy?

On Tuesday, 5th September 2023, Birmingham City Council (the largest local authority in Europe) effectively declared bankruptcy after being hit with a £760m bill to settle claims in a more than decade long equal pay dispute. ...

Read more

What Happens without Proper IT Governance?

https://www.zdnet.com/article/ten-budget-busting-it-disasters-you-should-learn-from/

1. National Programme for IT - £10.1bn

What was it?

One of the most expensive IT projects of all time - designed to transform healthcare in England and spanning at least 10 separate technology projects.

What went wrong?

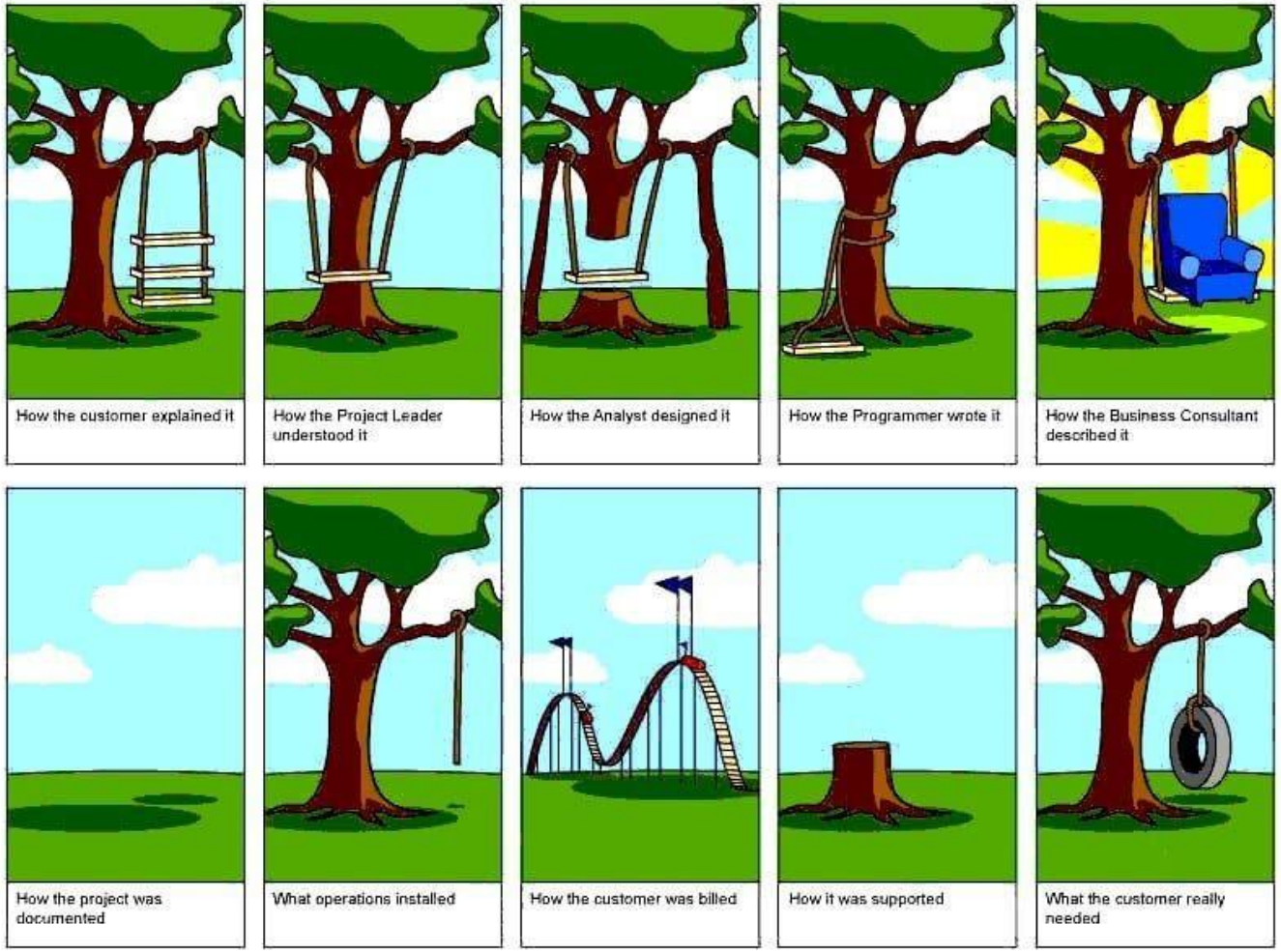
While many aspects of the programme delivered results, key projects ballooned in cost and missed deadlines. The National Programme for IT was originally costed at £2.3bn but by 2013 the three year project was still running, albeit in a different guise, and had an estimated lifetime cost of £10.1bn. One of the most delayed and expensive parts of the programme was a project to install patient administration systems (PAS) in English hospitals - with complaints that systems had been designed without consulting frontline hospital staff - resulting in software labelled hopeless by politicians.

And some (well known) cybersecurity incidents…

Why Related to Inefficient IT Governance?

- Poorly defined business requirements, or ever-changing ones
- Low visibility about value creation
- Inability to set priorities
- Complexity of projects
- Lack of committed business sponsors
- Lack of clear business drivers for solutions
- Communication gaps between business and IT
- Poor upkeep / maintenance

However, Communication is Difficult…



How Other Organizations Enforce Governance

- Project Governance
- Data Governance
- Architecture Governance
- Governance, Risk & Compliance (GRC)
- Procurement Governance
- Software and Technology Governance
- Operations Governance
- Cloud Usage Governance
- ITIL
- AI Governance …

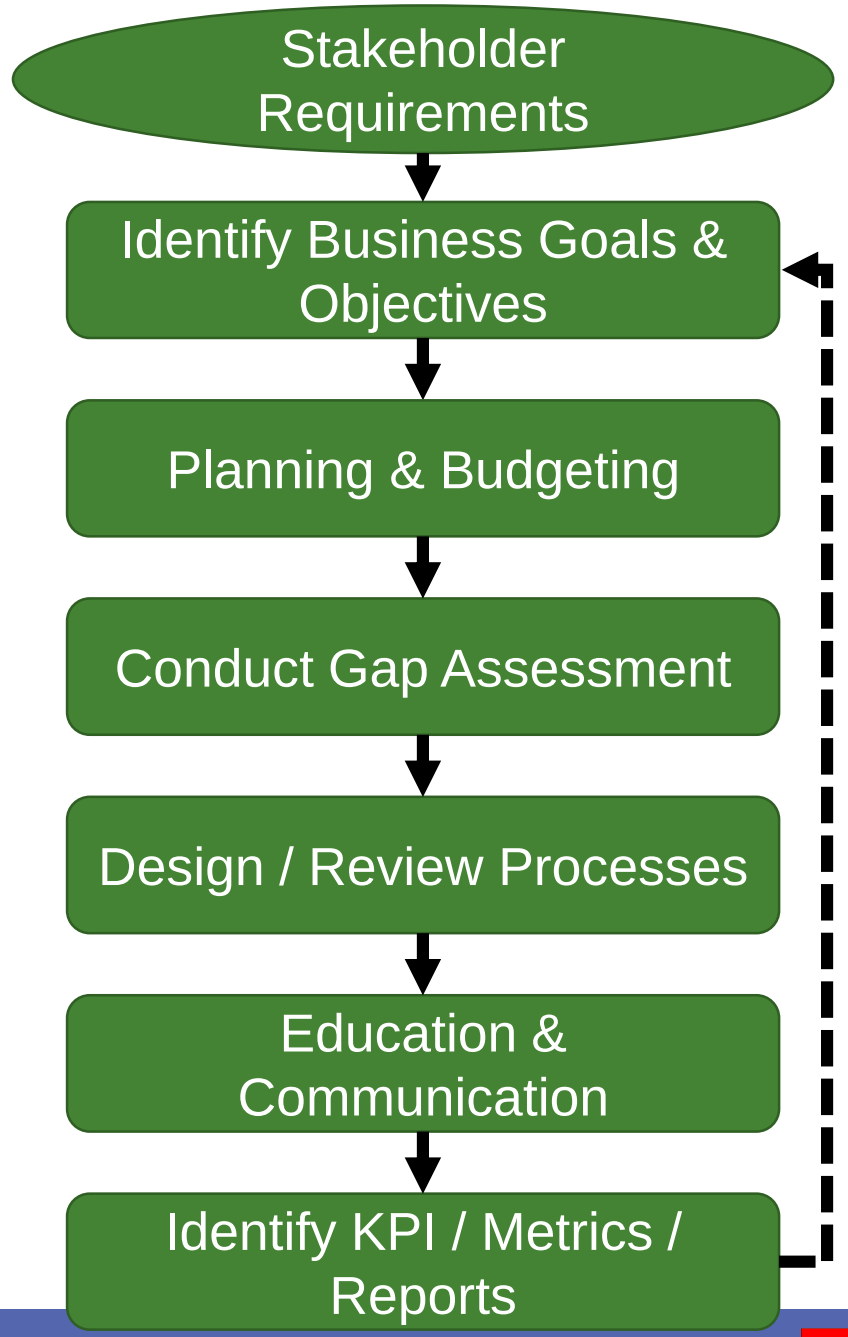
How Other Organizations Enforce Governance

- Project Governance
- Data Governance
- Architecture Governance
- Go
- Pro
- So
- Op
- Cloud Usage Governance
- ITIL
- AI Governance …

But don’t overload in an NGO

Implementing IT Governance

- Executive Buy-Ins and goal-setting
- Planning of activities
- Budget Estimation
- Process Design
- Organization Structure
  - Roles & Responsibilities
- Culture Change
- Metrics



Implementing IT Governance – Self Help

- Take references of best practices from established framework
- Start small and agile – focus on one particular area
- Base on public templates of IT Governance activities
- Establish a task force with business and technical people
- Leverage GenAI for certain uses

Example Structure of Implementing Governance

Challenges of Implementing Governance

- Demand resources for NGOs
  - Staff with experiences and certification: ITIL, CEGIT, COBIT, etc.
  - Money $$
- Expertise needed
- Commitment and long-term plan
- Needs to be Agile or suffocating innovations
- The governance process cannot keep pace with evolving NGO business situations

Reference Governance Frameworks

COBIT by ISACA

- Provides a comprehensive framework of designed for governance and management of enterprise IT

COSO model by Committee of Sponsoring Organizations of the Treadway Commission

- Evaluates internal control and more on enterprise risk management (ERM)

CMMI by the Software Engineering Institute

- Progresses performance improvement

Factor Analysis of Information Risk (FAIR)

- Helps organizations quantify cyber security and operational risk

ITIL (Information Technology Infrastructure Library)

- Ensures that IT services support core processes of the business

Glimpse of COBIT 2019

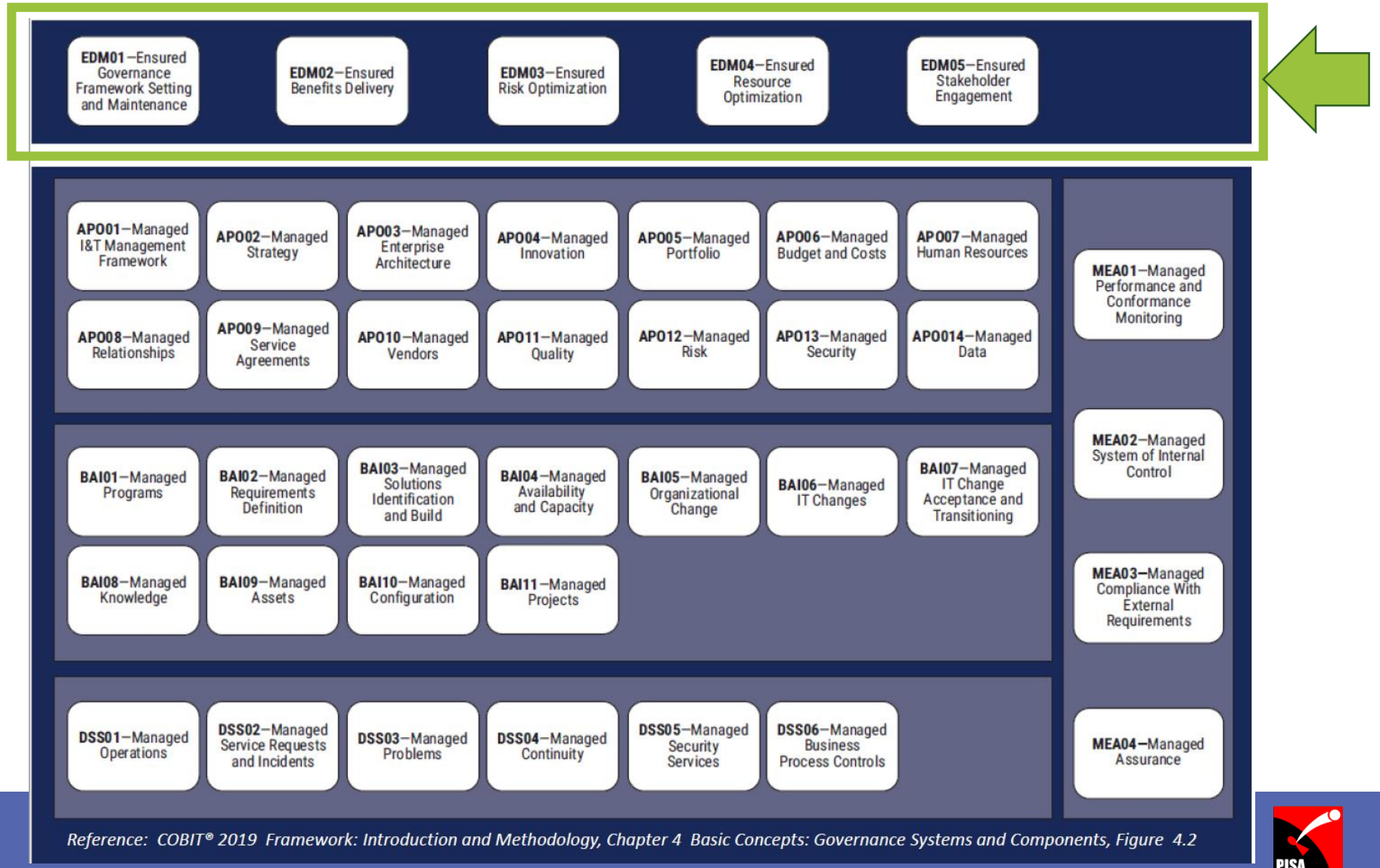
Evaluate, Direct and Monitor

Align, Plan and Organize

Build, Acquire and Implement

Deliver, Service and Support

Monitor, Evaluate and Assess



Reference: COBIT® 2019 Framework: Introduction and Methodology, Chapter 4 Basic Concepts: Governance Systems and Components, Figure 4.2

Myths of IT Governance

- There is a one-size fits all framework
- SaaS can solve the problem
- Outsourcing process can outsource risks
- It’s a checklist exercise of ticking boxes
- It can be static and optimal

Agenda (Recap)

Why do we need IT Governance?

Basic Areas of IT Governance

- Strategic Alignment
- Architecture
- Risk Management
- Performance Management
- IT Service Management

Architecture

Enterprise Architecture relates organizational mission, goals and objectives to business tasks, activities and relations and to the technology or IT infrastructure required to execute them

- Related to IT Governance

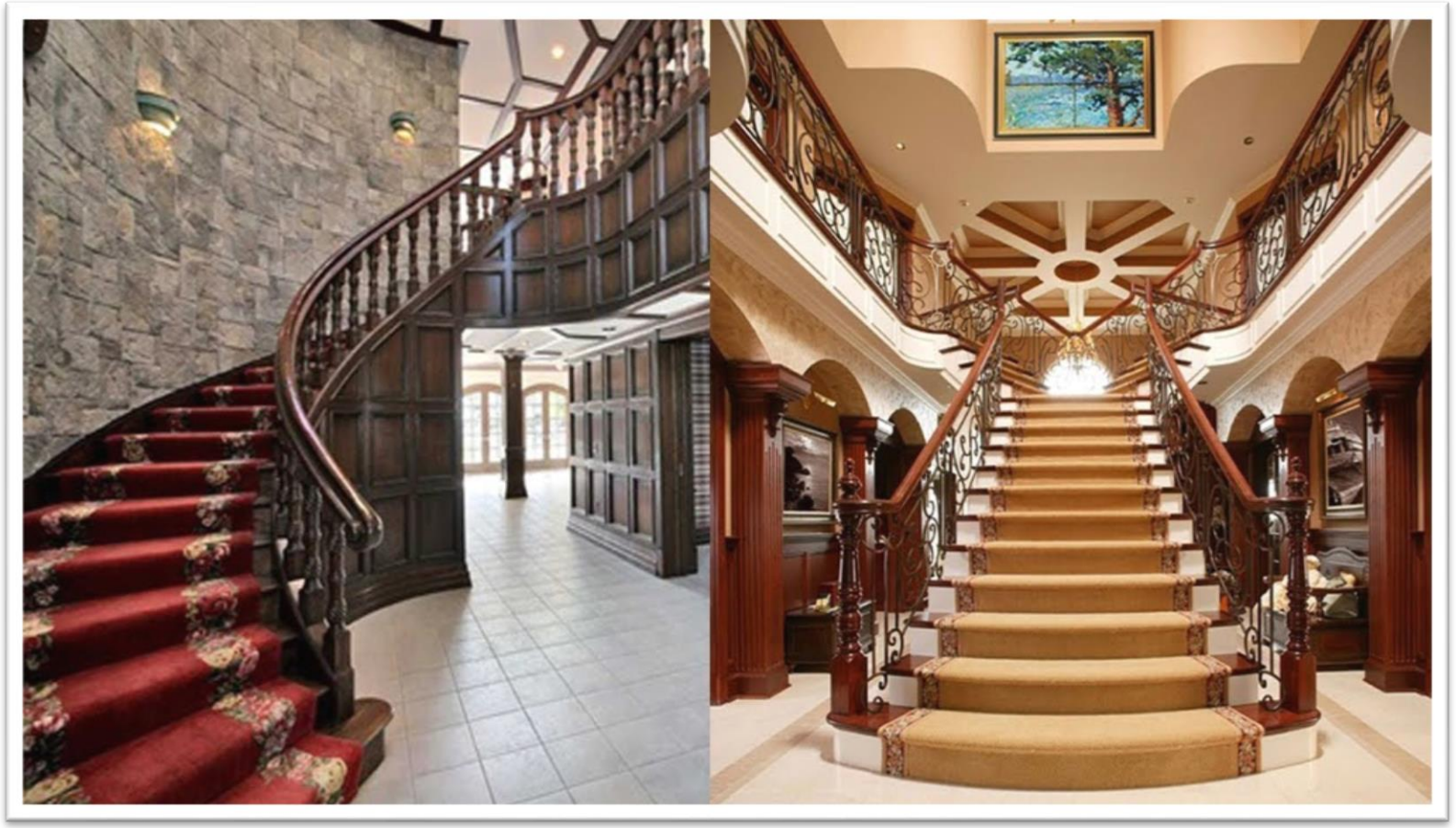
Exemplar Framework - TOGAF

- Architecture Principles, Capabilities, Technical Debts, Architecture Building Blocks

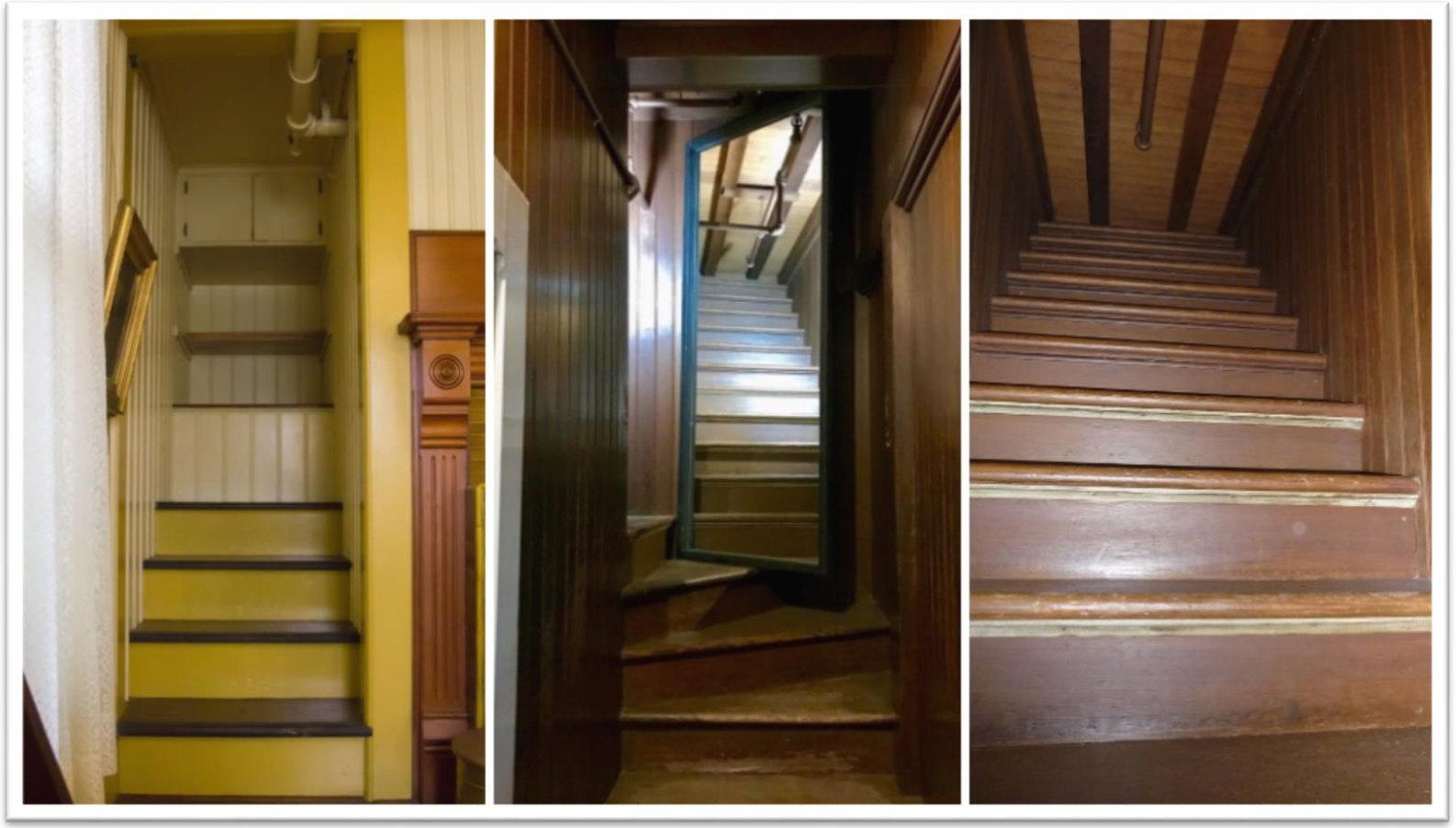
Examples of Technical Architecture

- https://aws.amazon.com/architecture/
- https://www.alibabacloud.com/architecture/
- https://learn.microsoft.com/en-us/azure/architecture/browse/

What One Wants Their House To Be Like



Without Proper Architecture Governance, It can be Messy



https://insights.som.yale.edu/insights/your-organization-mrs-winchesters-house

Glimpse of TOGAF

Principle 20: Control Technical Diversity

Statement:

Technological diversity is controlled to minimize the non-trivial cost of maintaining expertise in and connectivity between multiple processing environments.

Rationale:

There is a real, non-trivial cost of infrastructure required to support alternative technologies for processing environments. There are further infrastructure costs incurred to keep multiple processor constructs interconnected and maintained.

Limiting the number of supported components will simplify maintainability and reduce costs.

The business advantages of minimum technical diversity include: standard packaging of components; predictable implementation impact; predictable valuations and returns; redefined testing; utility status; and increased flexibility to accommodate technological advancements. Common technology across the enterprise brings the benefits of economies of scale to the enterprise. Technical administration and support costs are better controlled when limited resources can focus on this shared set of technology.

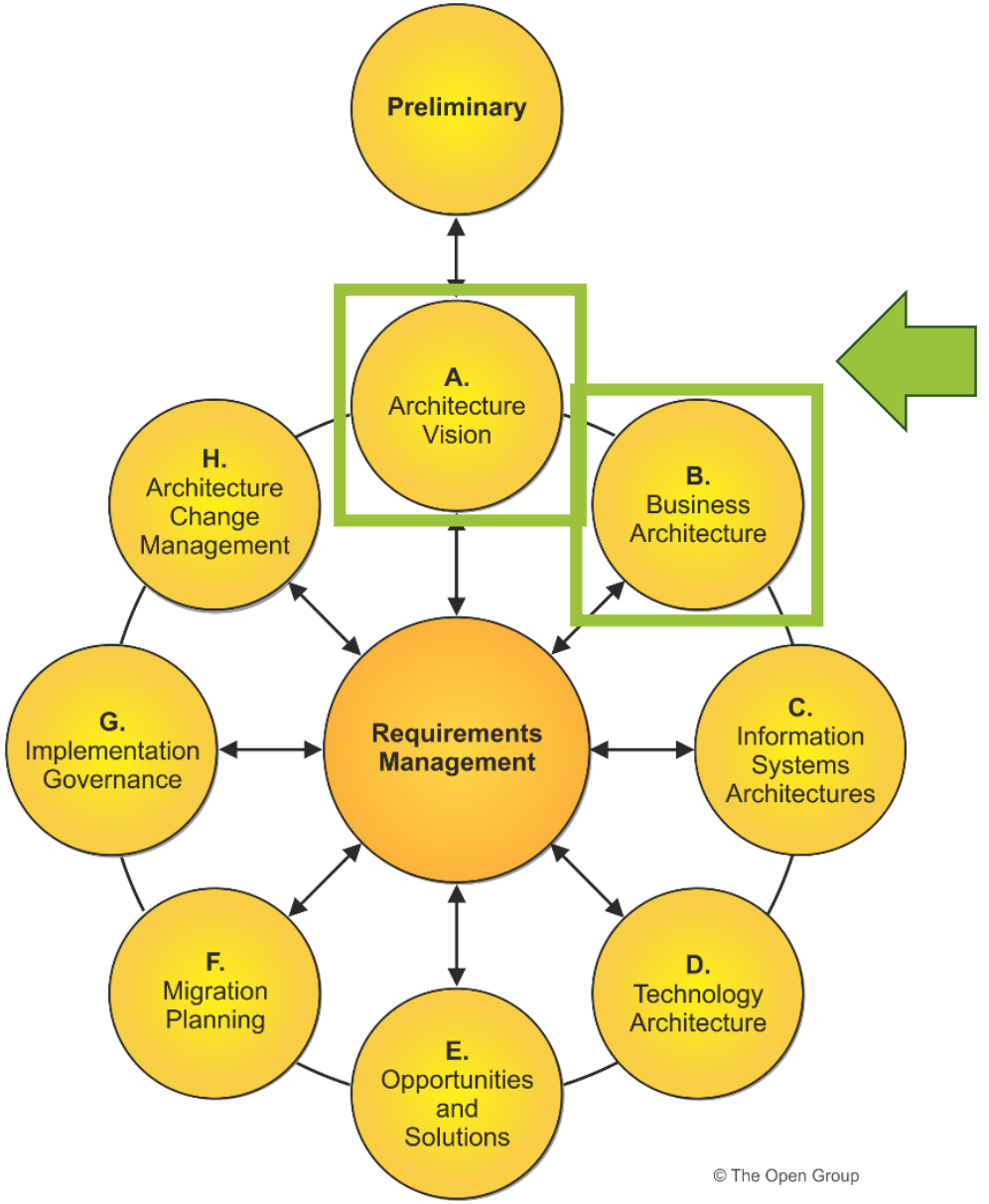
Implications:

- Policies, standards, and procedures that govern acquisition of technology must be tied directly to this principle
- Technology choices will be constrained by the choices available within the technology blueprint

Procedures for augmenting the acceptable technology set to meet evolving requirements will have to be developed and put in place.

- The technology baseline is not being frozen

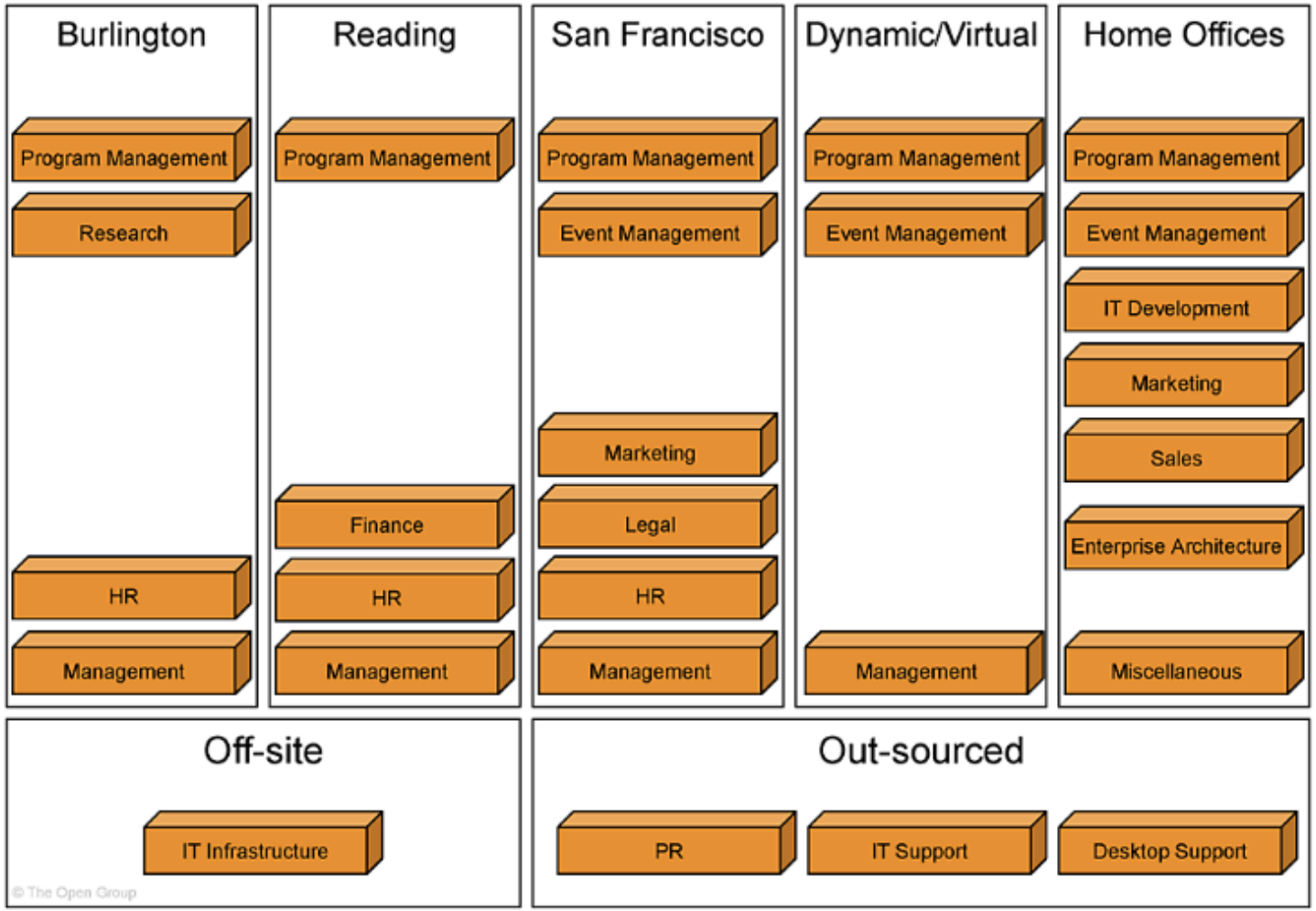
Technology advances are welcomed and will change the technology blueprint when compatibility with the current infrastructure, improvement in operational efficiency, or a required capability has been demonstrated.



Four Domains of TOGAF Architecture

Business Domain	Goals & Strategy of an organization
Information Domain	Storage, analysis and usage of physical & logical data
Application Domain	Applications and system integrations that enable the business strategy
Technology Domain	All end points, cloud, network, system, infrastructure, storage that enable applications and information

Business Domains Architecture



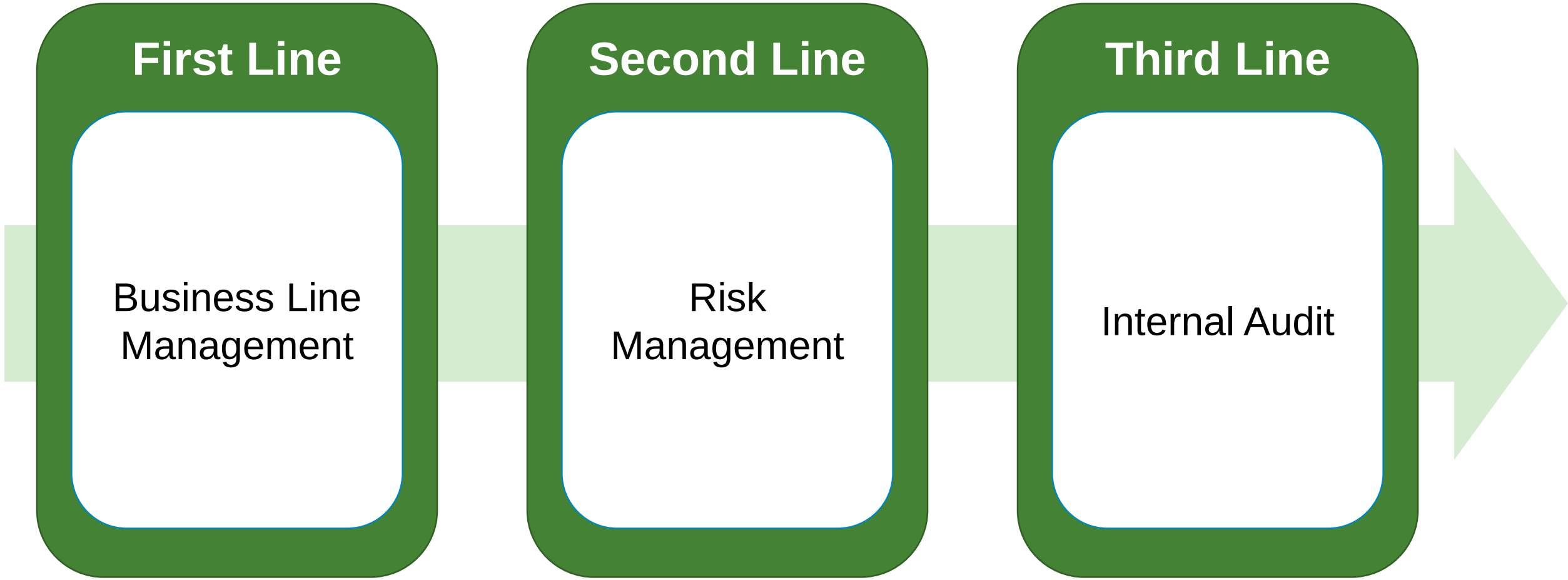
https://pubs.opengroup.org/architecture/togaf9-doc/arch/chap31.html

Risk Management

- A process to identify, assess, record and handle cyber security risks in an organization
- Understand the risk appetite
- Risk register to follow up
- Assign a risk management owner to handle all tasks with authority
- Take reference and checklist of ISO27001:2022 or HKSARG S17 Baseline IT Security Policy
- Conduct (Qualitative) Risk assessment

https://www.smartsheet.com/content/iso-27001-checklist-templates
https://www.govcert.gov.hk/doc/S17-v7_EN.pdf
https://www.ogcio.gov.hk/en/our_work/information_cyber_security/government/doc/ISPG-SM01.pdf

Risk Management – Lines of Defense



Glimpse of ISO27001 Framework

NIST CyberSecurity Framework

Identify	Protect	Detect	Respond	Recover
Governance	Awareness Control	Anomalies and Events	Response Planning	Recover Planning
Business Environment	Awareness & Training	Security Continuous Monitoring	Communications	Improvements
Asset Management	Data Security	Detection Process	Analysis	Communications
Risk Assessment	Info Protection and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

https://www.nist.gov/cyberframework

Glimpse of COSO Enterprise Risk Management

Governance & Culture

1. Exercises Board Risk Oversight
2. Establishes Operating Structures
3. Defines Desired Culture
4. Demonstrates Commitment to Core Values
5. Attracts, Develops, and Retains Capable Individuals

Strategy & Objective-Setting

6. Analyzes Business Context
7. Defines Risk Appetite
8. Evaluates Alternative Strategies
9. Formulates Business Objectives

Performance

10. Identifies Risk
11. Assesses Severity of Risk
12. Prioritizes Risks
13. Implements Risk Responses
14. Develops Portfolio View

Review & Revision

15. Assesses Substantial Change
16. Reviews Risk and Performance
17. Pursues Improvement in Enterprise Risk Management

Information, Communication, & Reporting

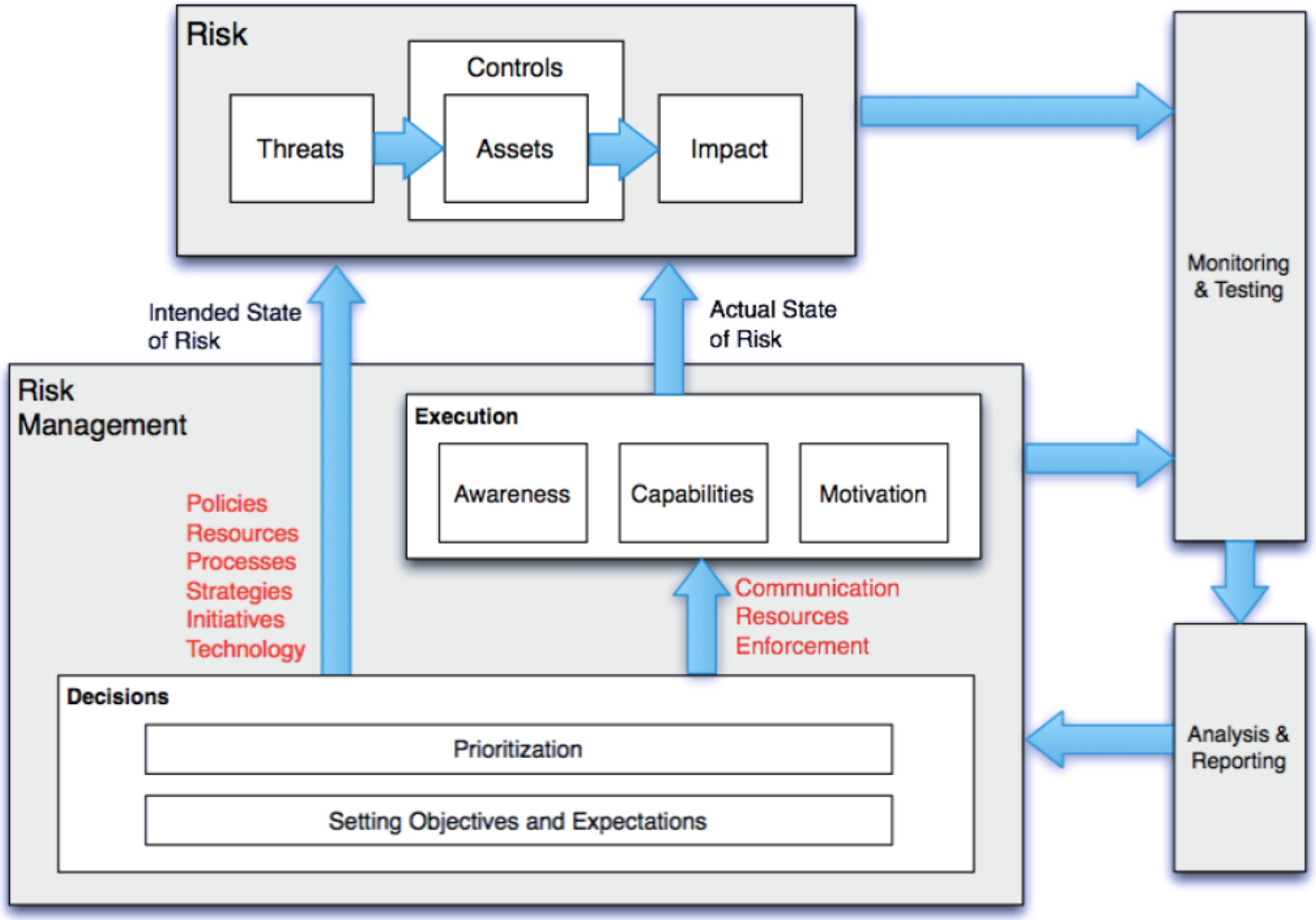
18. Leverages Information and Technology
19. Communicates Risk Information
20. Reports on Risk, Culture, and Performance

Source: *Enterprise Risk Management – Integrated Framework: Executive Summary*, Committee of Sponsoring Organizations of the Treadway Commission, September 2004, p. 5

Glimpse of FAIR Model

https://www.fairinstitute.org/blog/fair-risk-basics-what-is-loss-magnitude

Glimpse of FAIR Model

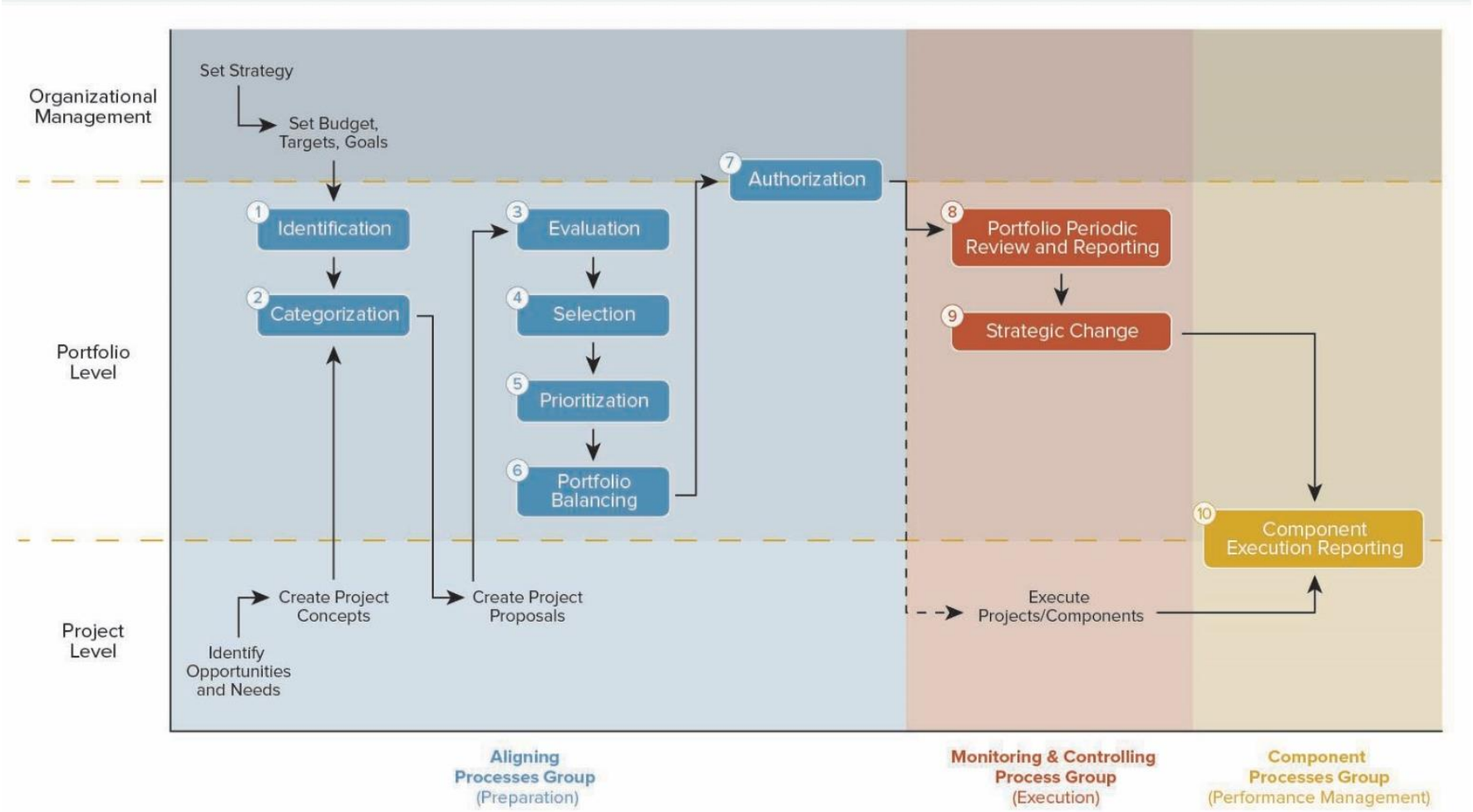


https://www.fairinstitute.org/resources/cyber-risk-management-maturity

Performance Management

- Measure value, performance of IT, performance of projects
- Optimal Investment and proper management of IT assets
- Manage for current and developing needs
- Building competencies and capacity for the future
- Identify key metrics …
- CMMI or ITIL can be applied to measure performance

Portfolio and Project Management



https://www.smartsheet.com/content-center/best-practices/project-management/project-management-guide/project-portfolio-management-ppm

Portfolio and Project Management

Portfolio Management

- Strategic (planned in years)
- Aligned to organization goals
- Managed through strategic planning or budget cycle
- Measured by business opportunities, value creation and business KPIs
- Focusing on prioritization
- Focusing on NPV & IRR

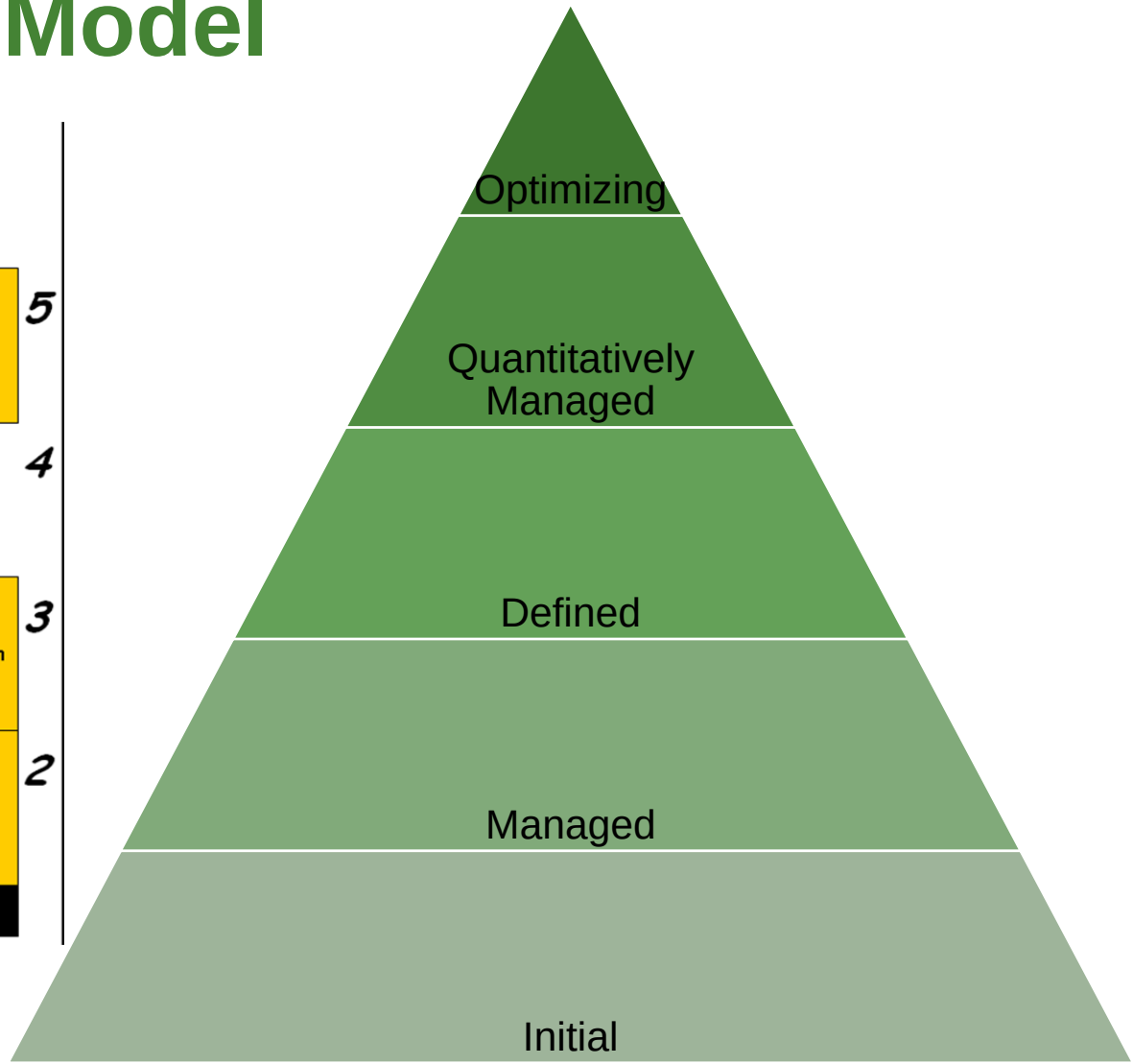
Project Management

- Tactical (planned in Quarters / months)
- Defined project objectives
- Managed through PDLC
- Measured by project risks, budgets and schedule
- Focusing on execution
- Focusing on project cost

Glimpse of CMMI Maturity Model

The Process Areas

	Engineering	Project Management	Process Management	Support	
5			• Organizational Innovation & Deployment	• Causal Analysis & Resolution	5
4		• Quantitative Project Management	• Organizational Process Performance		4
3	• Validation • Verification • Product Integration • Technical Solution • Requirements Development	• Risk Management • Integrated Project Management + IPPD	• Organizational Training • Organizational Process Definition + IPPD • Organizational Process Focus	• Decision Analysis & Resolution	3
2	• Requirements Management	• Supplier Agreement Management • Project Monitoring and Control • Project Planning		• Configuration Management • Process & Product Quality Assurance • Measurement & Analysis	2



IT Service Management

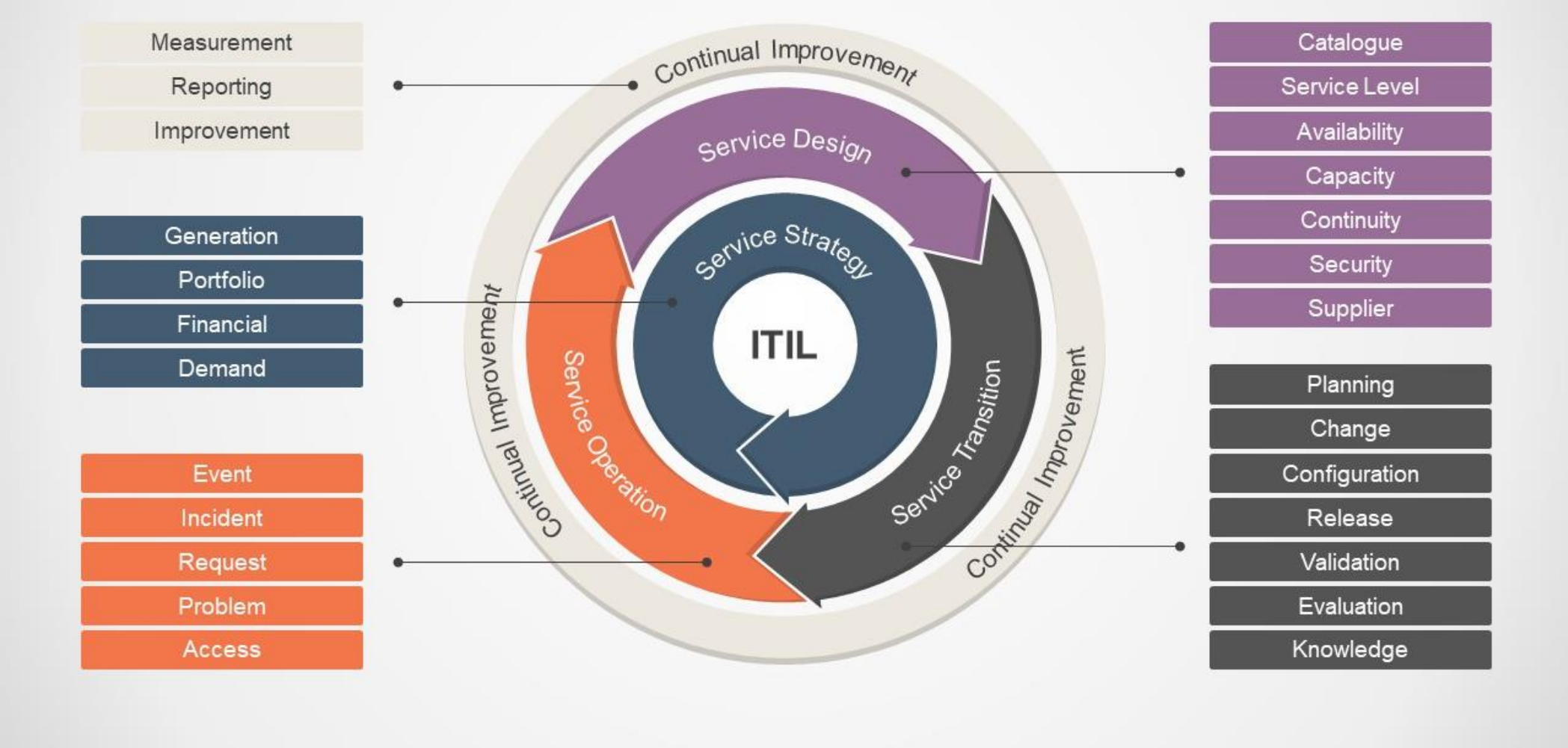
"*ITSM includes all the activities, policies, and processes that organizations use for deploying, managing, and improving IT service delivery*" Joe Hertvik

- A framework to achieve IT governance of IT services
- Ensure the IT service brings value to the business
- Change / Release Management
- Procurement

Change / Release Management

- Minimize risks of system failures
- Provide faster responses in case of incidents
- Provide better internal (or external) communication
- Tackle resistance to change
- Produce good documentation, records and knowledge

Glimpse of ITIL Framework



Procurement

- Clear and definite functional and non-functional requirements
- Evaluation of products – proof of concepts/value
- Multiple vendors / suppliers
- Evaluation criteria with a balance of technical and price
- Underpinning contract for support, service level commitments
- Proof/evidence of continuity support and references
- Legal terms and indemnification
- Finance arrangement
- Assess Supply Chain Risks

Conclusion

Recap

- IT Governance brings confidence to business
- IT Governance aligns values with business strategy and avoid wastes
- Reliable IT services
- Implementing IT Governance needs resources commitment, careful planning and culture change
- Don’t over-govern
- Existing frameworks provides good references about processes and best practices for NGO

Q & A

Contact: vincent.ip@pisa.org.hk