Deloitte.

Implementing and Managing CBCS Policies & Guidelines

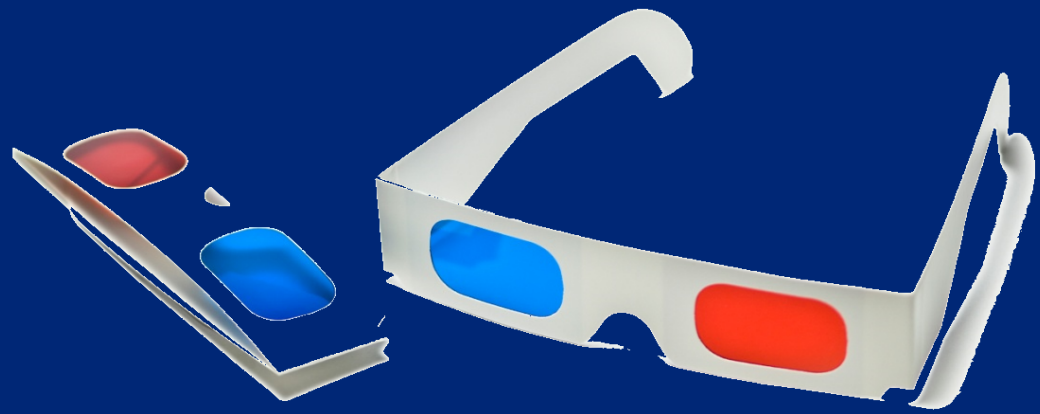
A practical guide for effective compliance

Mario Flores
Willemstad, Curaçao
18 November 2014

Agenda

1. Introduction
2. Context
3. A simplified implementation and management approach
4. Utilizing management tools
5. Conclusion
6. Questions

Context



Action is needed

- Currently CBCS has defined different policies and guidelines for IT Governance and Management - Financial Institutions are aware of requirements, but many don’t take action quickly enough;
- Non-adherence to guidelines may expose organizations to IT risks;
- Increased need for cyber defense;
- Risk-based maturity requirements with emphasis on information security;
- New ITSM policy is directly related to existing policies;
- Public and reputation impact.

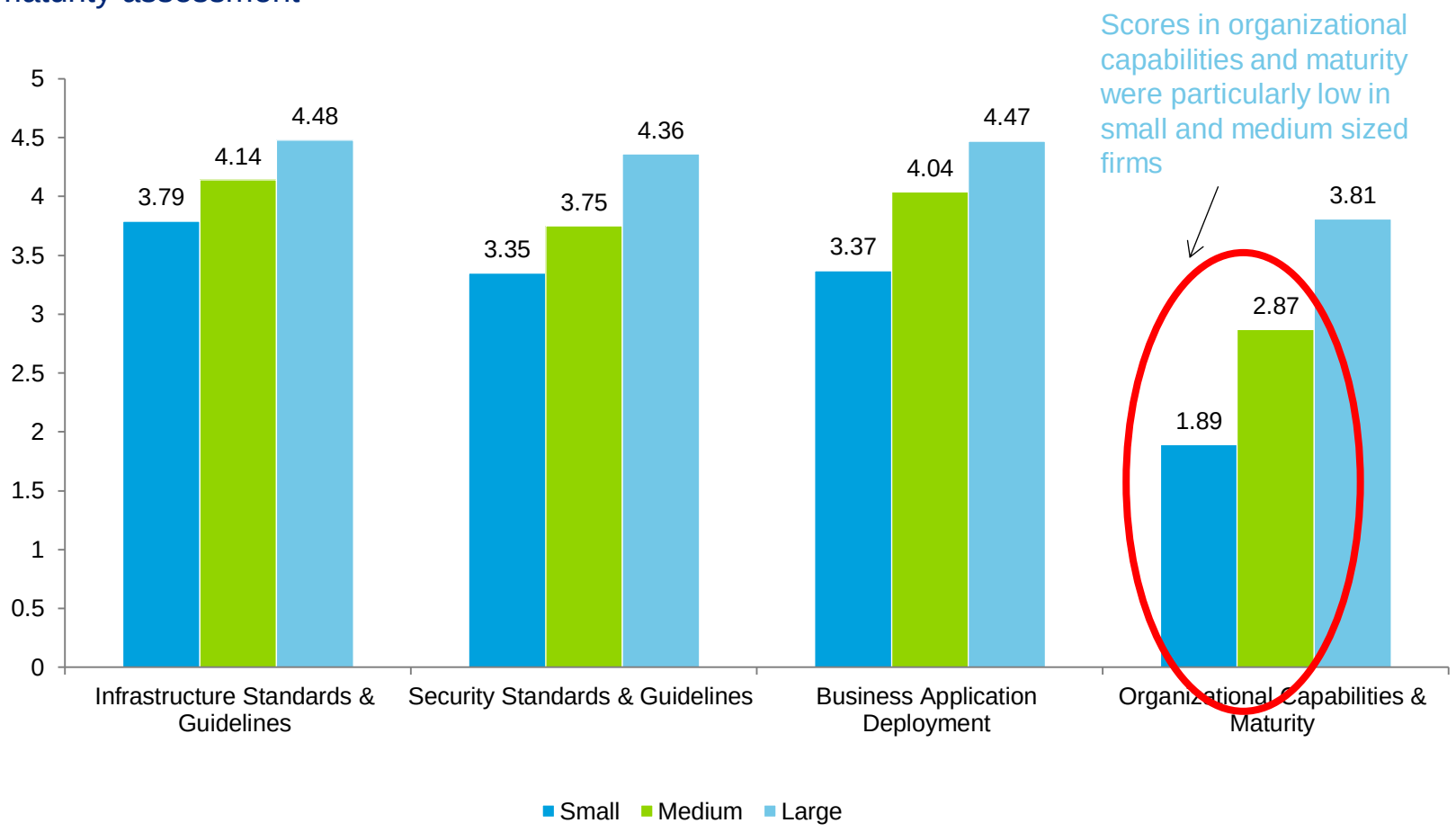
CBCS IT related Policies & Guidelines

The Bank will provide provisions and guidelines for the following 6 IT areas:

1. Information Security
2. Business Continuity management;
3. IT Service Management;
4. IT Governance;
5. Development & Acquisitions;
6. Outsourcing IT Services.

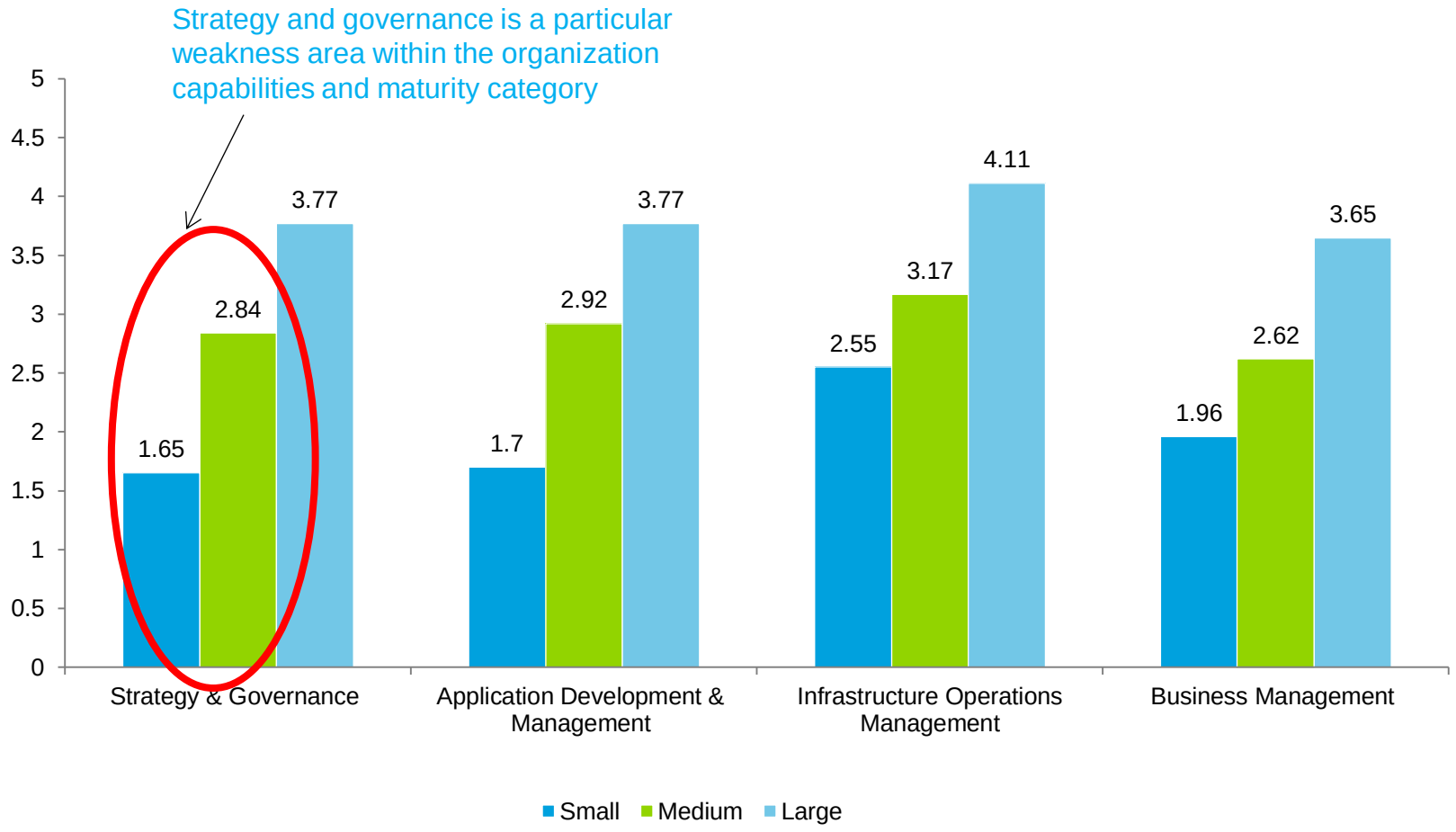
Deloitte Global IT Maturity Assessment

- The maturity assessment reveals that small and medium sized firms are particularly weak in organizational capabilities and maturity
- The following table summarizes average scores of each group of firms by size against the four areas of the maturity assessment



Organizational capabilities and maturity category breakdown

- Further breakdown of the organization capabilities and maturity sections reveal that strategy & governance is particularly weak in small and medium sized firms

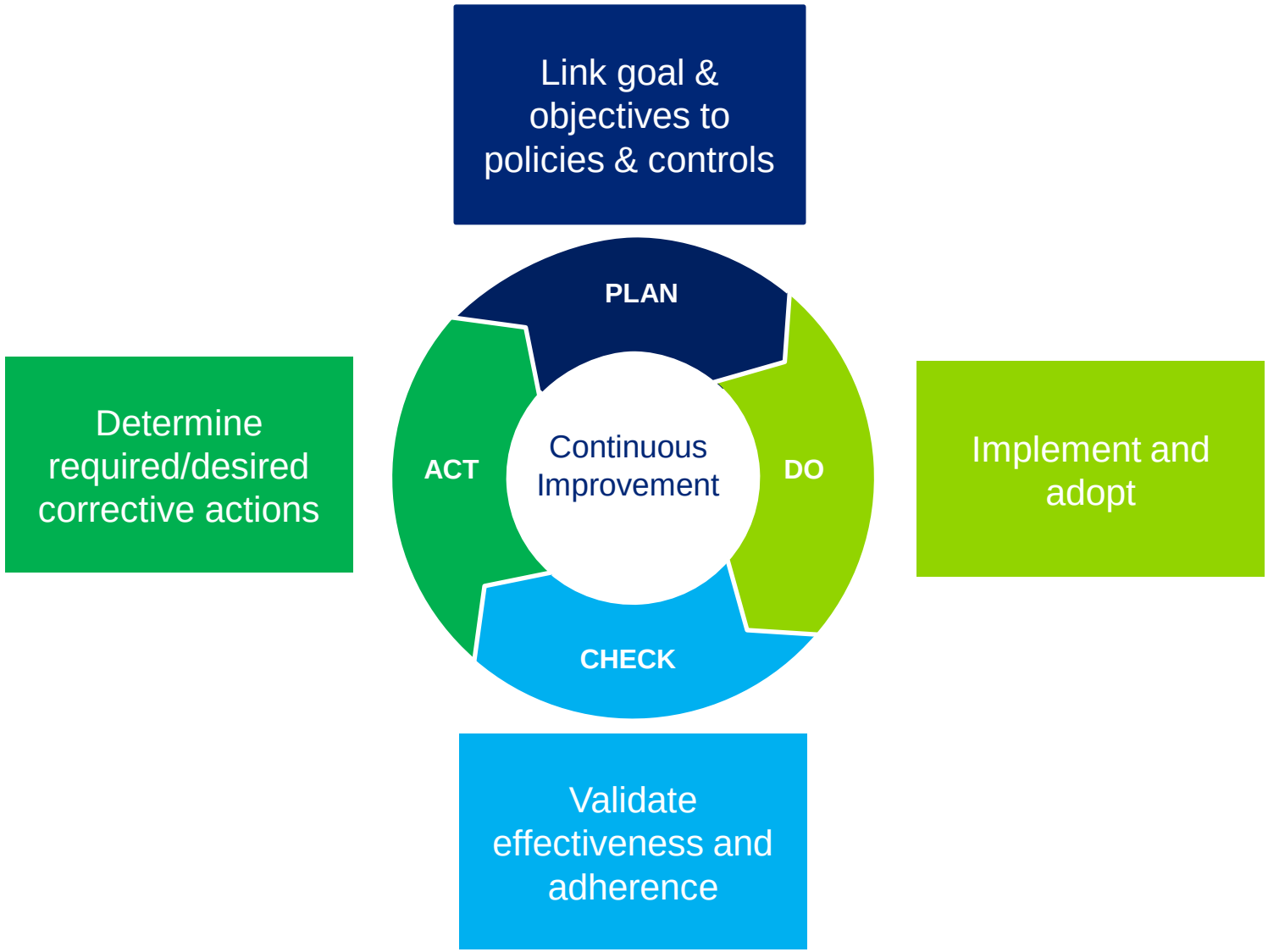


Benefits of implementing CBCS Policies and Guidelines

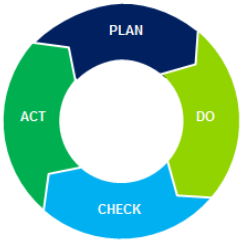
1. Compliance with CBCS requirements
2. Assist your financial institution to improve its IT maturity, and in particular associated IT risk management
3. Formal and standardized processes that leave less room for CBCS guideline interpretation by IT department(s) employees.
4. Improved effectiveness as it relates to IT Governance & Management and subsequently improved overall operational effectiveness (primary business processes)
5. Formal adoption by management provides an overall insight in maturity across your financial institution, and a framework for internal performance measurement and management
6. Learning and benchmarking opportunities

Simplified implementation and management approach

Plan-Do-Check-Act (Deming)



Plan (Analyze & Prepare)



- Determine IT requirements based on business requirements;
- How do you get the most value out of IT?;
- Determine if one or more formal frameworks should be adopted;
- Carry out IT Risk Assessment + BIA – using the CBCS SIIQ as input;
- Map risks to control objectives and CBCS policies/guidelines;
- Determine applicability of CBCS policies and guidelines;
- Translate CBCS principles to controls and processes;
- Group control objectives;
- Carry out current state assessment;
- Carry out gap analysis;
- Develop medium/long-term maturity plan for implementation on a control (group) level;
- **Start simple!**

COBIT Framework - Domains

Governance of the Enterprise IT

Evaluate, Direct & Monitor (EDM)

Management of the Enterprise IT

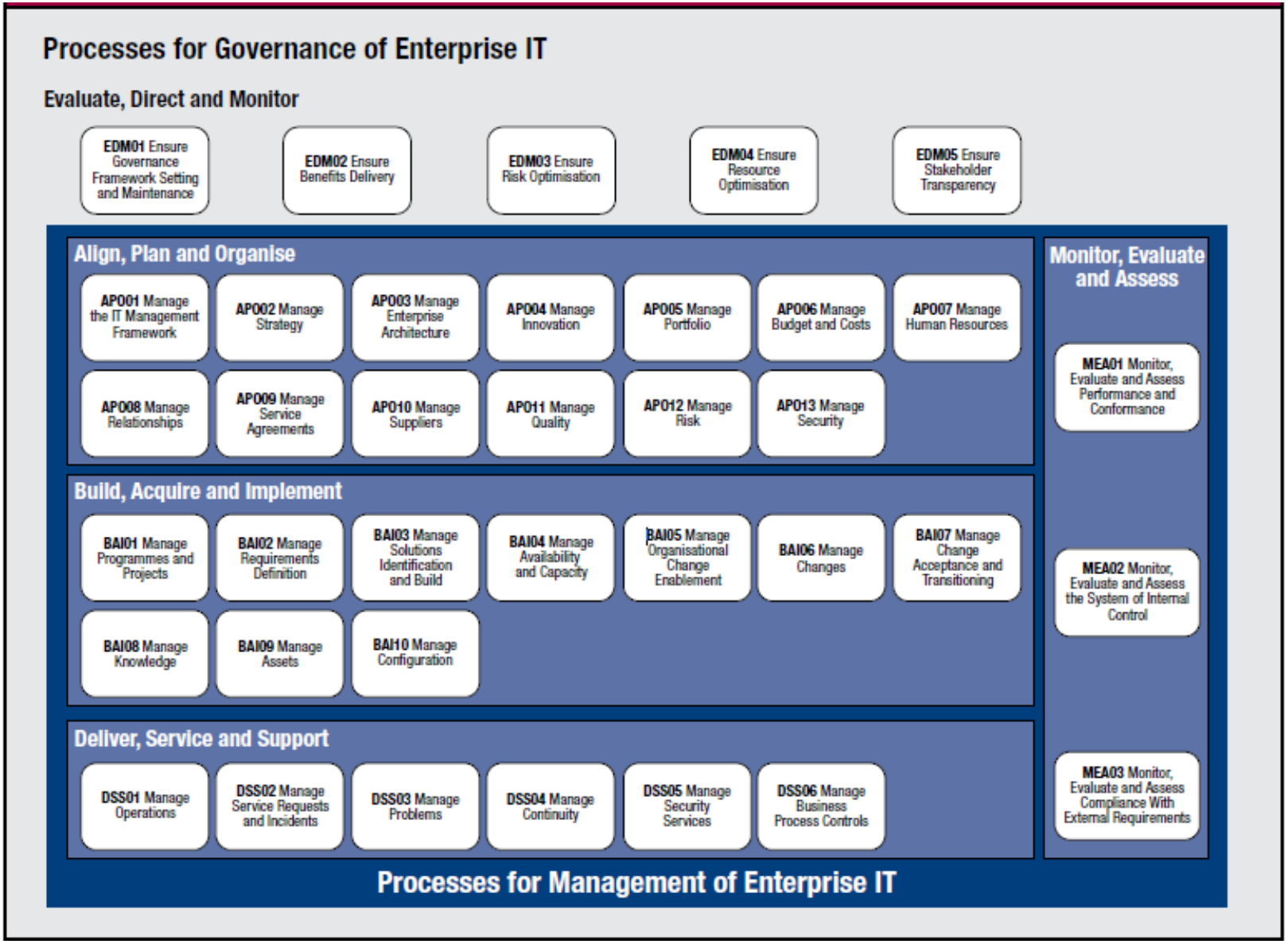
Align, Plan & organize (APO)

Build, Acquire & Implement (BAI)

Deliver, Service & Support (DSS)

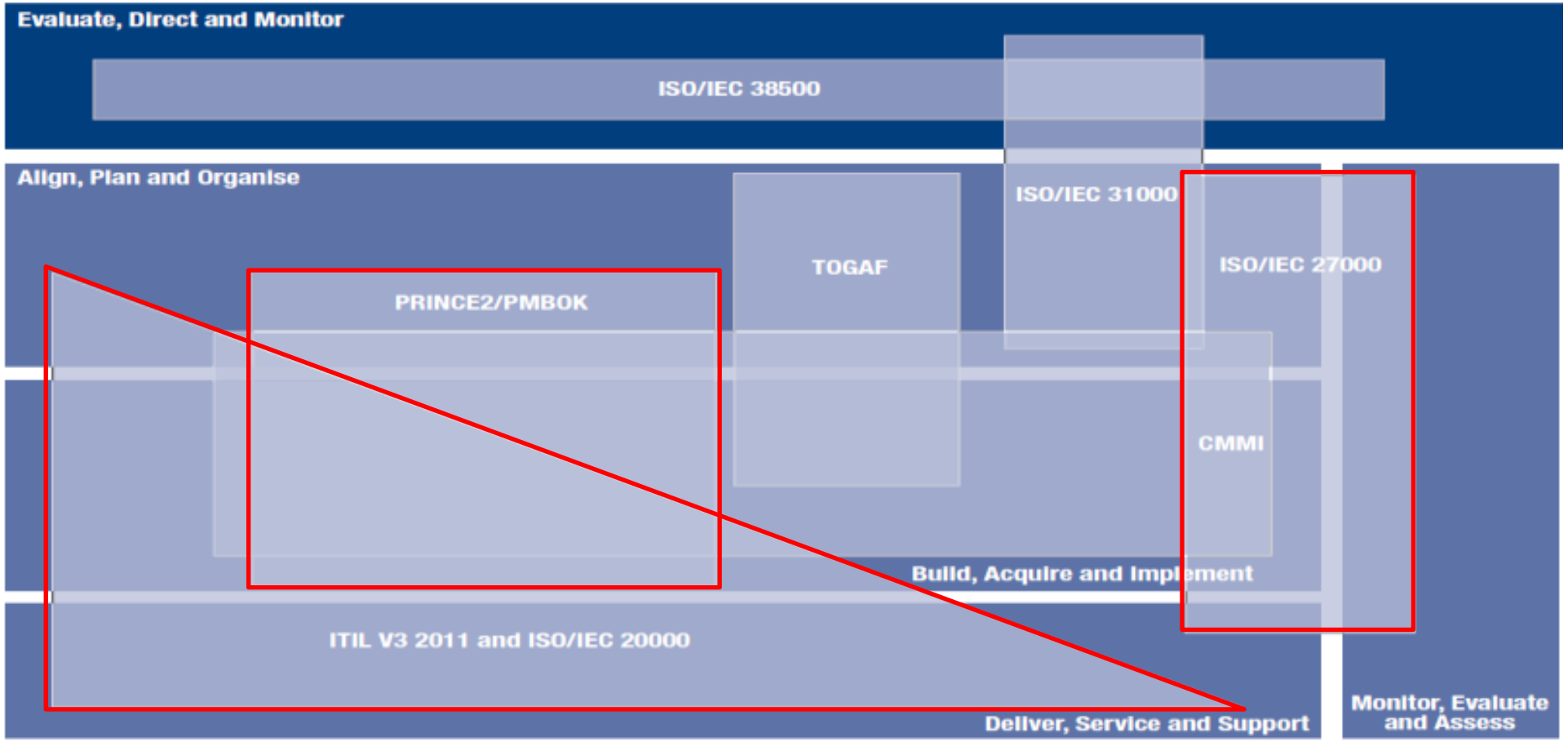
Monitor, Evaluate & Assess (MEA)

COBIT Framework - detailed

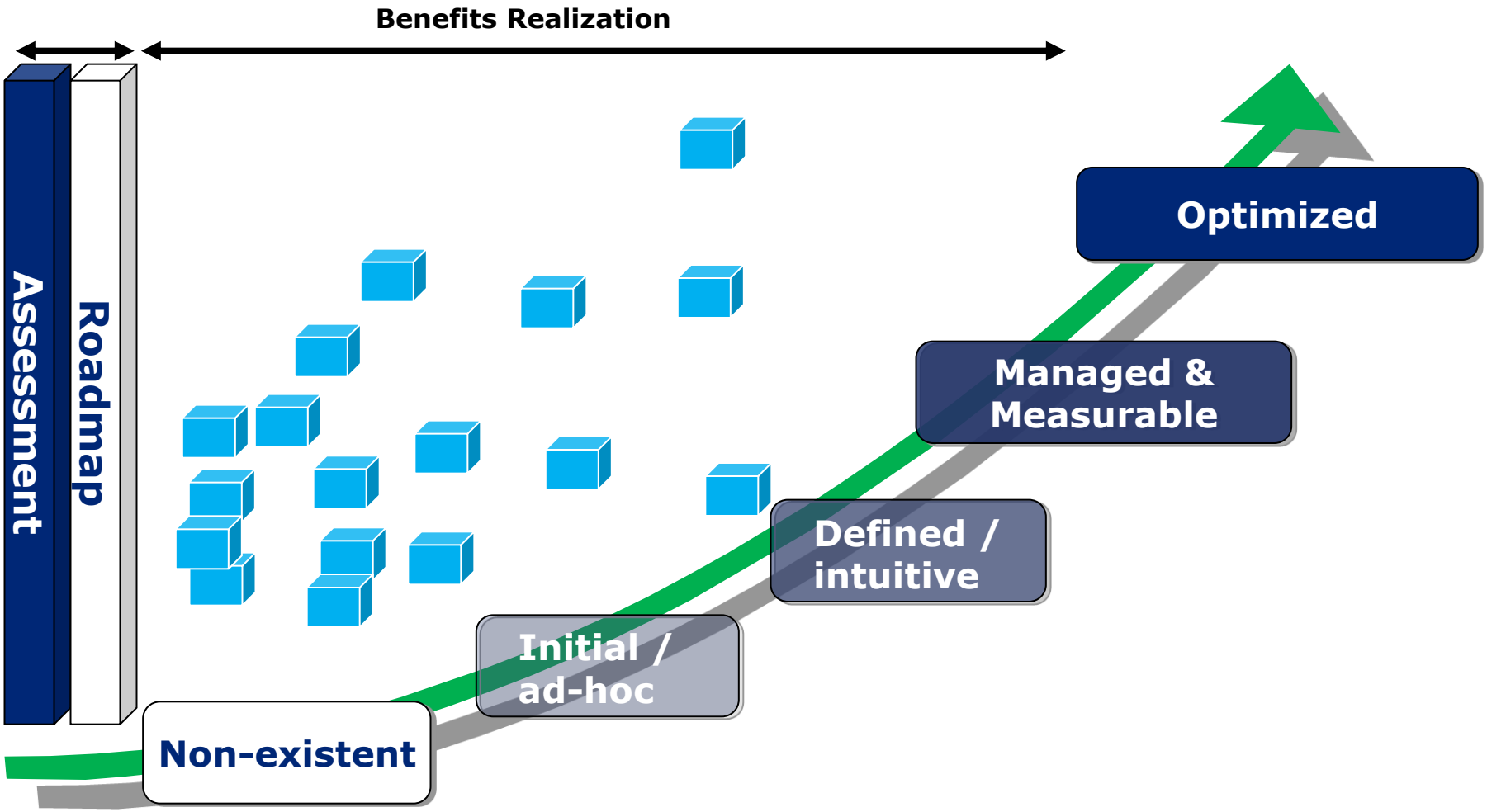


A range of standards and frameworks is linked through the five COBIT 5 process domains

COBIT 5 areas and domains covering common standards and frameworks



Maturity Transition Roadmap (Capability – CobIT 5.0)



Maturity Levels

0 – **Non-existent -** No documentation. There is no awareness or attention for certain control.

1 - **Initial/ad hoc -** Control is (partly) defined, but performed in an inconsistent way. The way of execution is depending on individuals.

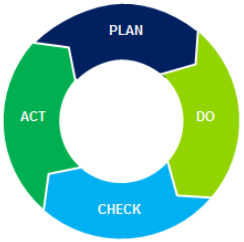
2 - **Repeatable *but intuitive* -** Control is in place and executed in a structured and consistent, but informal way.

3 - **Defined -** Control is documented, executed in a structured and formalized way. Execution of control can be proved.

4 - **Managed and measurable -** The effectiveness of the control is periodically assessed and improved when necessary. *This assessment is documented.*

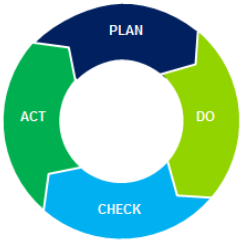
5 - ***Optimised -*** *An enterprisewide risk and control programme provides continuous and effective control and risk issues resolution.*

Do (develop and implement)



- Create a list of controls for managing the process / risk;
- Assign owners per process / control objective / control activity;
- Evaluate options for controls/processes;
- Make strategic decisions (ex. In-house vs. outsourced);
- Formalize contracts with external parties + ensure they meet your needs;
- Acquire resources (if necessary)
- Develop processes, procedures, templates, etc.;
- Make it actionable and measurable;
- Implement quick wins;
- Train staff in new procedures;
- Implement a formal Governance Structure;
- Embed periodic reporting on key controls / KPIs (take from CobIT);
- Celebrate.

Check (Test & Validate)



- Based on risk assessment and control objectives → develop testing plan;
- Test process / control effectiveness internally (Internal Audit, etc);
- Carry out independent audits;
- Periodic audits by CBCS;

How do you know if your IT Governance is effective?

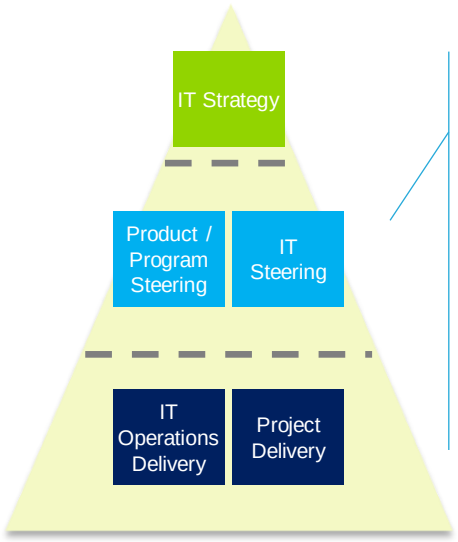
Indicators of effective IT governance:

- ✓ Recognition of IT as a strategic enabler of business capabilities
- ✓ Business guidance in the formulation of IT strategy
- ✓ Shared understanding between business and IT of how IT-related decisions are made
- ✓ Involvement of business in prioritization of IT investments
- ✓ Understanding of trade-offs to maximize value and minimize risk
- ✓ Optimized allocation of resources across IT initiatives and operations
- ✓ Collaborative oversight and direction for implementation of IT initiatives
- ✓ Growth and development of internal IT capability
- ✓ Dependable delivery of IT services
- ✓ Mechanisms to identify and track the realization of benefits and delivery of value to the business
- ✓ Clear accountability for results across both the business and IT

Are you getting the most value out of IT?

4 key questions to answer

- To know if we are getting the most value out of IT, these following 4 questions need to be answered:



- What are the right things to do?
- Are we doing enough of the right things?
- Are we doing the right things right?
- Are we getting the results we want?

Critical success factors to realize IT value

- To begin getting the most value out of IT, IT needs to start by doing the following:
  - Engage the business
  - Build a framework for decision making
  - Ensure transparency of trade-offs, and understand implications and risks
  - Need support/funding to deliver on decided priorities

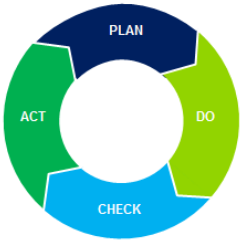
Typical IT Adoption Challenges and Root Causes

Governance brings the right individuals to the table to have the right conversations under the right process to make the best decisions given the available information.

Challenges	Root Causes
• Lack of IT representation at the executive-level • Lack of structured decision-making authority and processes • Lack of solutions deployment processes • Lack of project management discipline • Lack of transparency of business drivers and priorities for trade-off decisions	• Insufficient discussion of IT governance among business executives • Lack of buy-in from the executive level into the value, importance or need for IT governance • Limited knowledge on how to implement IT governance

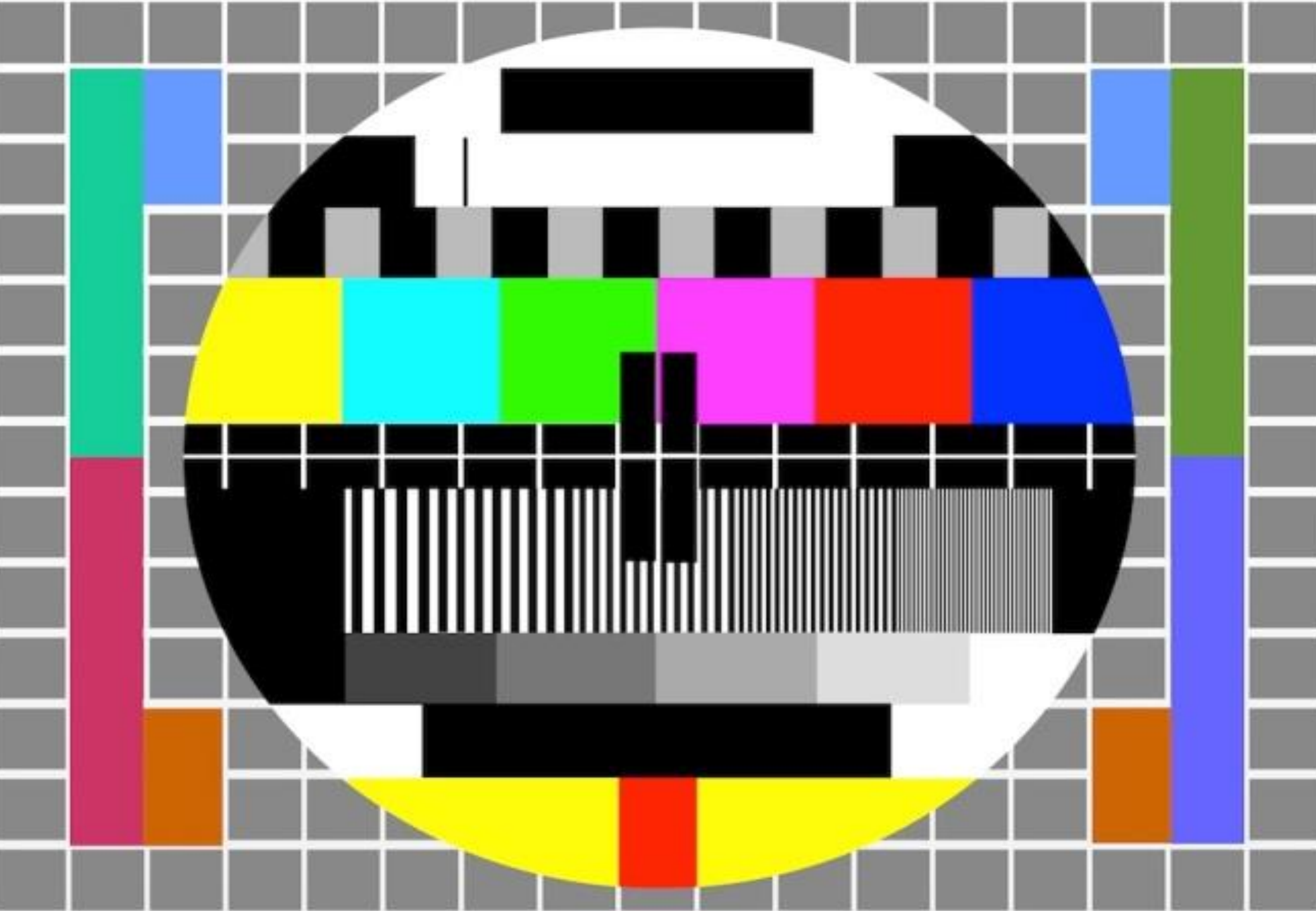
To address, need to understand:
• "How do I explain IT governance to an executive?"
• "How do I make the case for IT governance to my business leaders?"
• "How do I implement IT governance?"

Act (rework & optimize)



- Learn from results and try alternatives;
- Document lessons learned;
- Optimize what is not working effectively based on lessons learned;
- Adjust/adhere to initial improvement plans (from Plan & Do stage).

Utilizing management tools



Aud[i]Sec - GlobalSuite

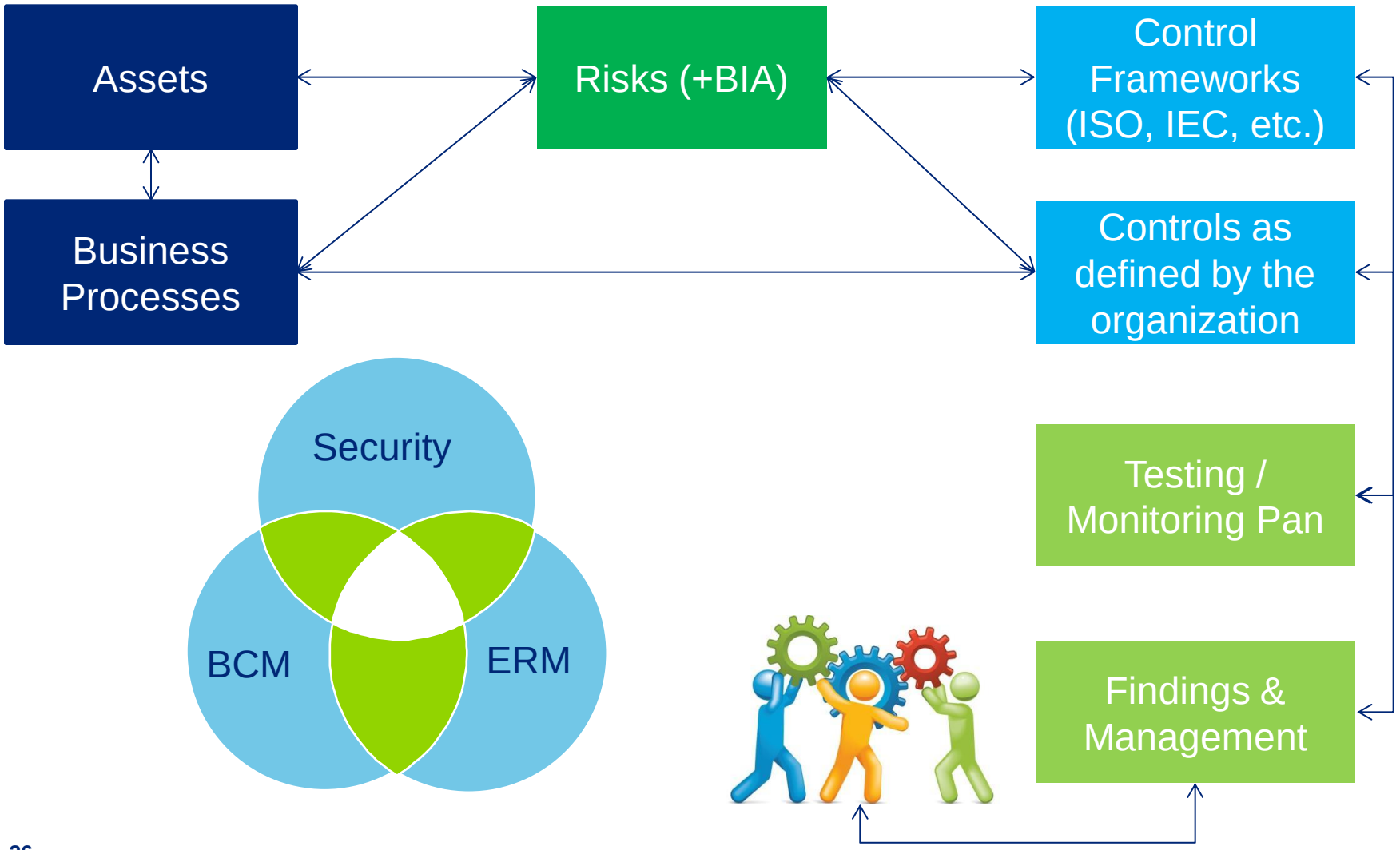
Administer	Manage	Monitor

Comply

GlobalRISK	Integral Risk management of your company based on ISO 31000
GlobalContinuity	Integrated management of Business Continuity according to ISO/IEC 22301
Global20000	Service management ISO/IEC 20000
GlobalCMDB	Configuration Management Database System
GlobalSGSI	Analysis, implementation, management, integration & maintenace of ISO 27001
GlobalBSC	Integral Control Panel – Balanced ScoreCard

GlobalCompliance	Legal, Contractual & Regulatory Compliance
GlobalSG	Quality- (ISO 9001) Environmental - (ISO 14001) Occupational health and Safety - (OSHAS 18001)
Global28000	Suply Chain Security (ISO 28000)
GlobalTicketing	Ticket management
GlobalPD	Personal Data Protection
GlobalSGPIC	Systems for the Critical Infrastructures Protection

Aud[i]Sec - GlobalSuite



Conclusion

Conclusion

- Focus on what's really important from both a business and risk perspective;
- Be realistic – full adherence takes (a lot of) time and effort;
- Get help where needed (CBCS, parent company, industry, advisors, etc.);
- Don't wait for the CBCS to come and audit.

Questions ….