Build an Effective Security and Risk Governance Function: It's Much More Than Just Reporting

Tom Scholtz

Key Issues

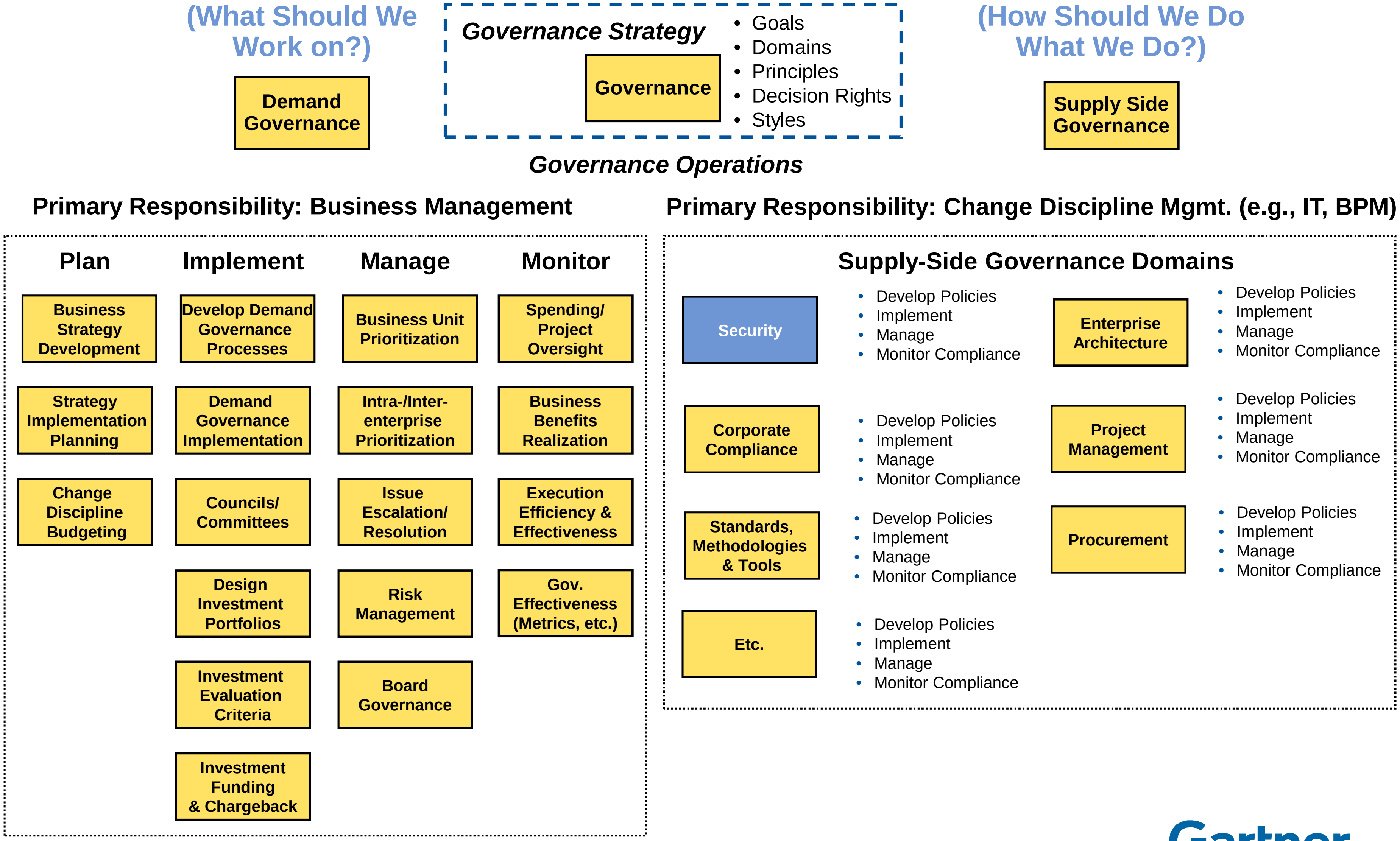
1. What are current security and risk governance best practices?
2. What processes and activities constitute effective security and risk governance?
3. What structures and forums are required?

Some Context: IT Governance — Gartner Definition

"The processes that ensure the effective and efficient use of IT in enabling an organization to achieve its goals"

- IT governance is made up of processes with activities, inputs, outputs, roles and responsibilities.
- IT governance's role is identified as "ensuring" as opposed to "executing."
- The goal of IT governance is a business goal.
- Key performance measures are effectiveness and efficiency.

Gartner's IT Governance Model



(What Should We Work on?)

Demand Governance

Governance Strategy

Governance

- Goals
- Domains
- Principles
- Decision Rights
- Styles

(How Should We Do What We Do?)

Supply Side Governance

Governance Operations

Primary Responsibility: Business Management

Plan	Implement	Manage	Monitor
Business Strategy Development	Develop Demand Governance Processes	Business Unit Prioritization	Spending/ Project Oversight
Strategy Implementation Planning	Demand Governance Implementation	Intra-/Inter-enterprise Prioritization	Business Benefits Realization
Change Discipline Budgeting	Councils/ Committees	Issue Escalation/ Resolution	Execution Efficiency & Effectiveness
	Design Investment Portfolios	Risk Management	Gov. Effectiveness (Metrics, etc.)
	Investment Evaluation Criteria	Board Governance	
	Investment Funding & Chargeback		

Primary Responsibility: Change Discipline Mgmt. (e.g., IT, BPM)

Supply-Side Governance Domains

Security
- Develop Policies
- Implement
- Manage
- Monitor Compliance

Enterprise Architecture
- Develop Policies
- Implement
- Manage
- Monitor Compliance

Corporate Compliance
- Develop Policies
- Implement
- Manage
- Monitor Compliance

Project Management
- Develop Policies
- Implement
- Manage
- Monitor Compliance

Standards, Methodologies & Tools
- Develop Policies
- Implement
- Manage
- Monitor Compliance

Procurement
- Develop Policies
- Implement
- Manage
- Monitor Compliance

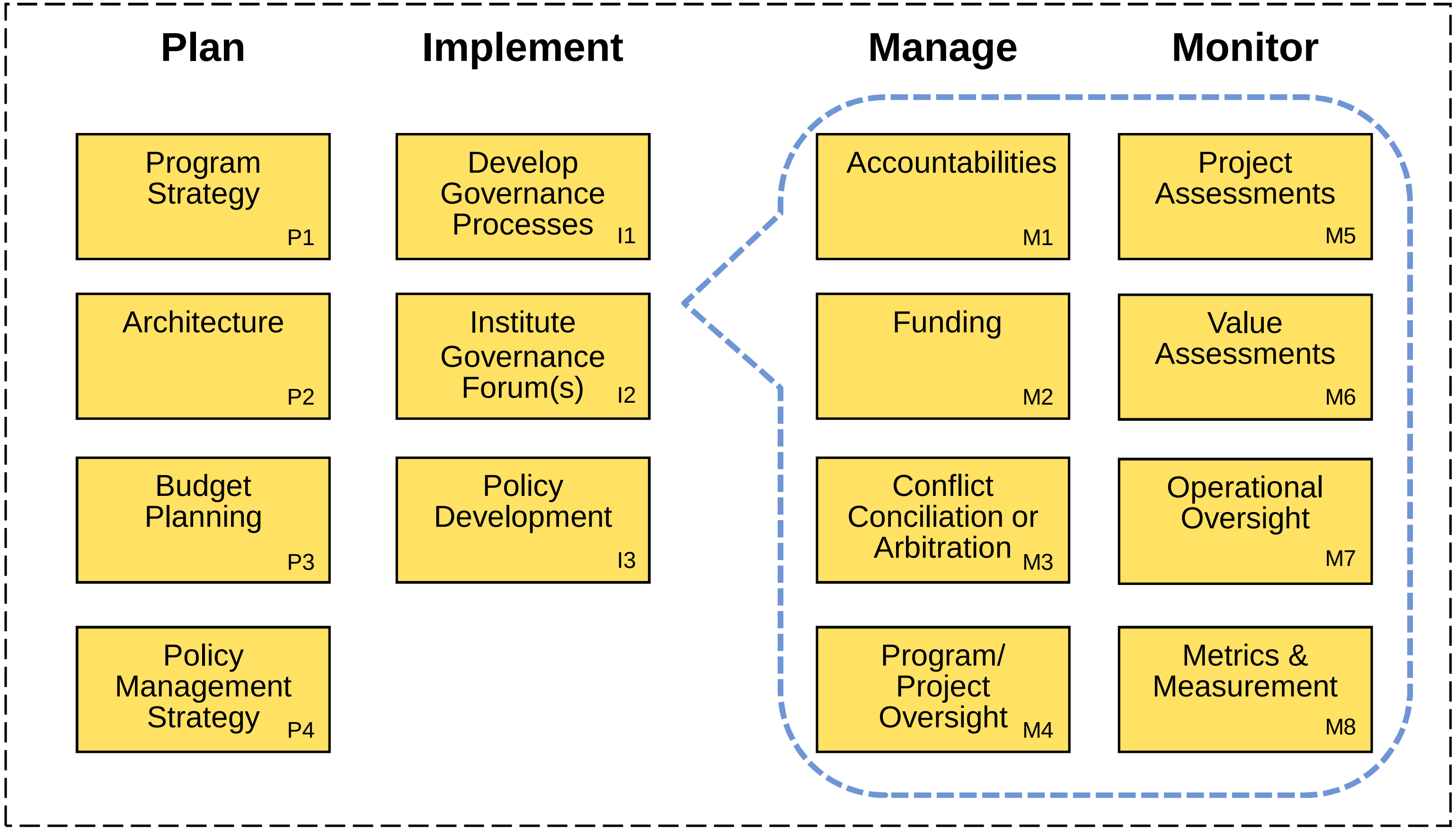
Etc.
- Develop Policies
- Implement
- Manage
- Monitor Compliance

Information Security and Risk Governance

The processes that ensure that reasonable and appropriate actions are taken to protect the organization's information resources, in the most effective and efficient manner, in pursuit of its business goals:

- Sets and manages accountability and decision rights.
- Allocates resources.
- Arbitrates between conflicting security requirements and risk affinities.
- Provides assurance to the executive and stakeholders that information risk is appropriately managed.

The Gartner Information Security and Risk Governance Model

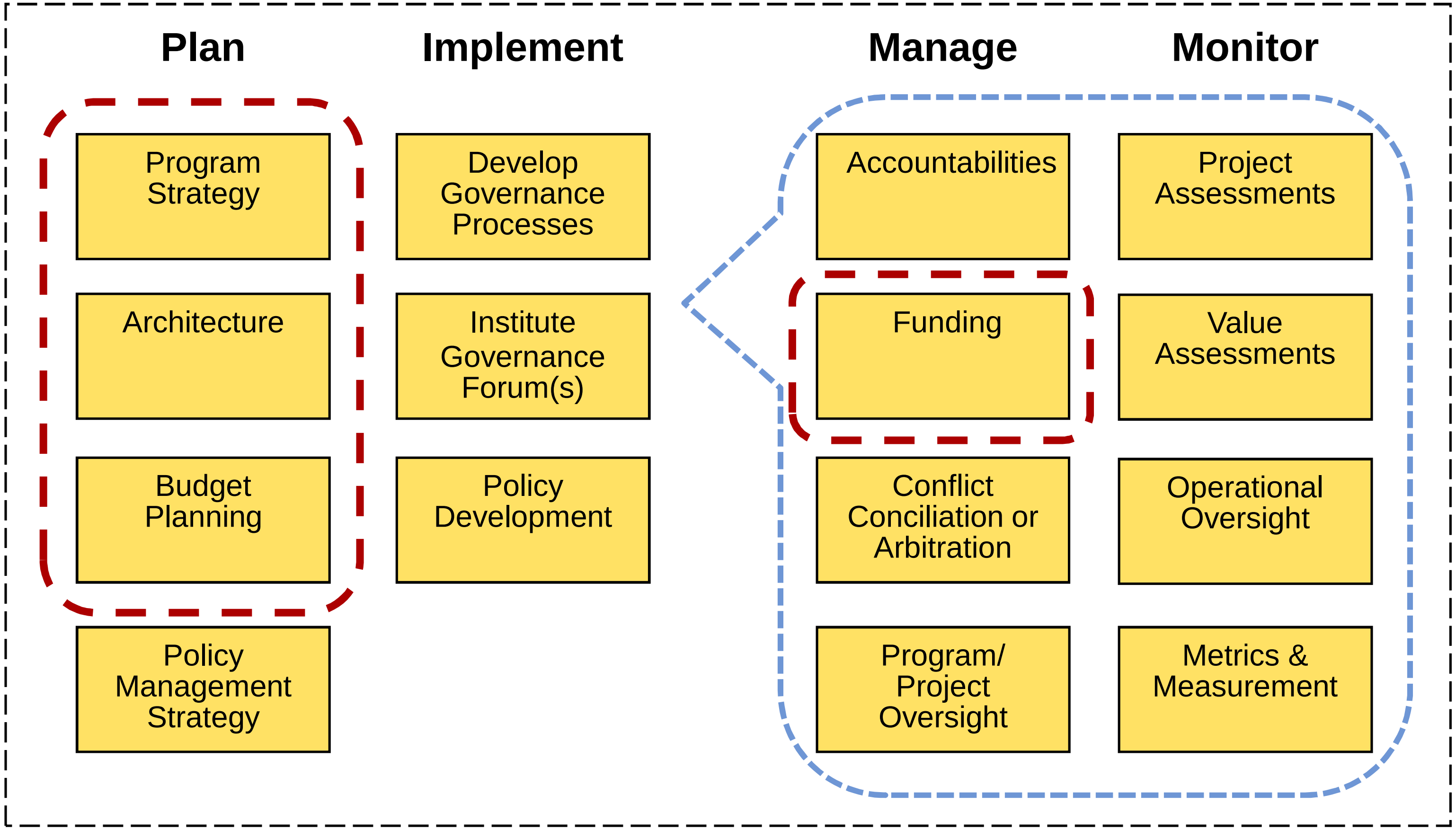


Plan	Implement	Manage	Monitor
Program Strategy P1	Develop Governance Processes I1	Accountabilities M1	Project Assessments M5
Architecture P2	Institute Governance Forum(s) I2	Funding M2	Value Assessments M6
Budget Planning P3	Policy Development I3	Conflict Conciliation or Arbitration M3	Operational Oversight M7
Policy Management Strategy P4		Program/ Project Oversight M4	Metrics & Measurement M8

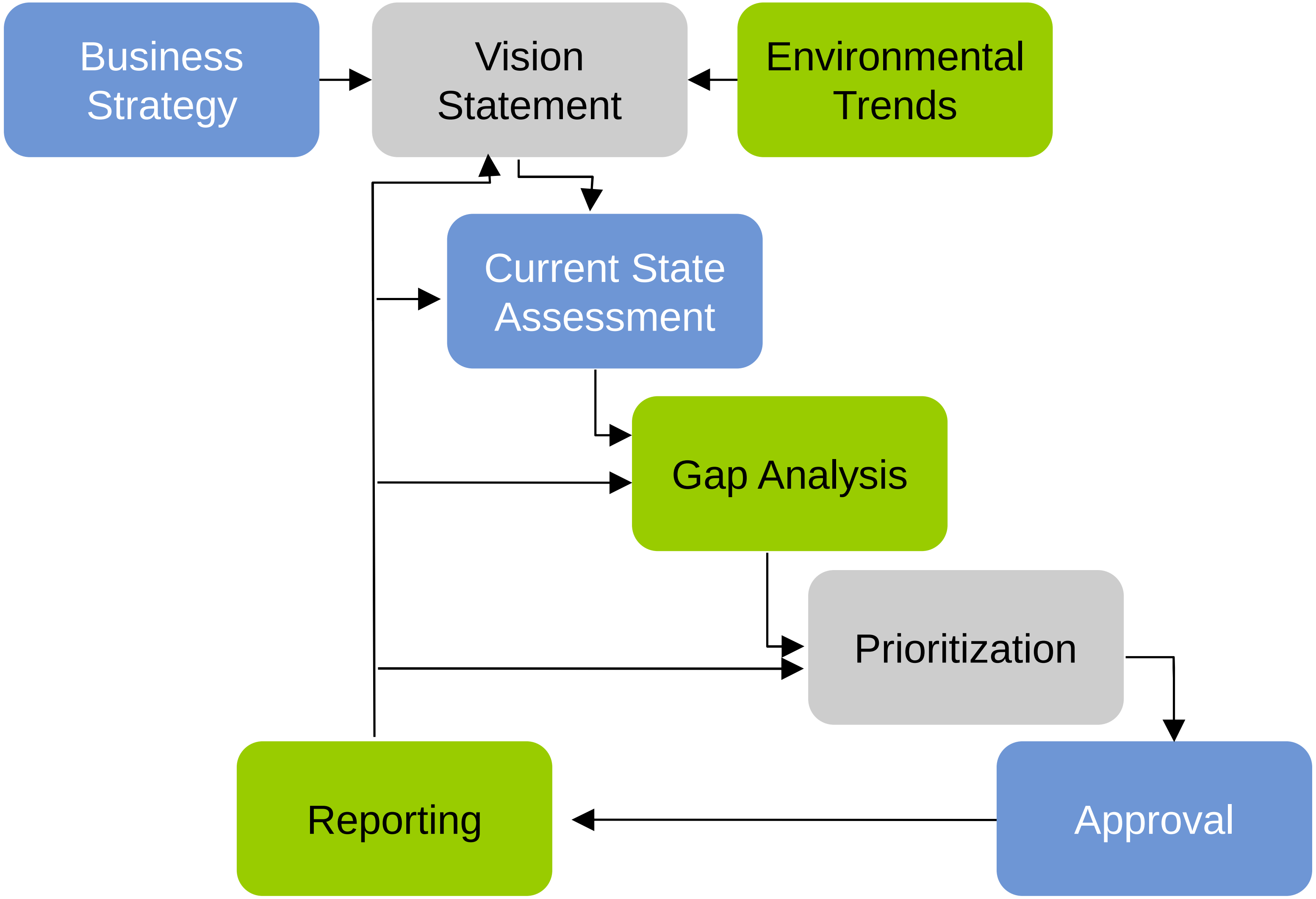
Best Practice Approach

Governance Objectives:	Manifested by:
Sets and manages accountability and decision rights.	• Policy Management • Organization
Allocates resources.	• Strategy • Budget Planning • Funding
Arbitrates between conflicting security requirements and risk affinities.	• Committee Discussions • Mandates
Provides assurance to the executive and stakeholders that information risk is appropriately managed.	• Oversight and Assessments • Measurement and Reporting

Resource Allocation

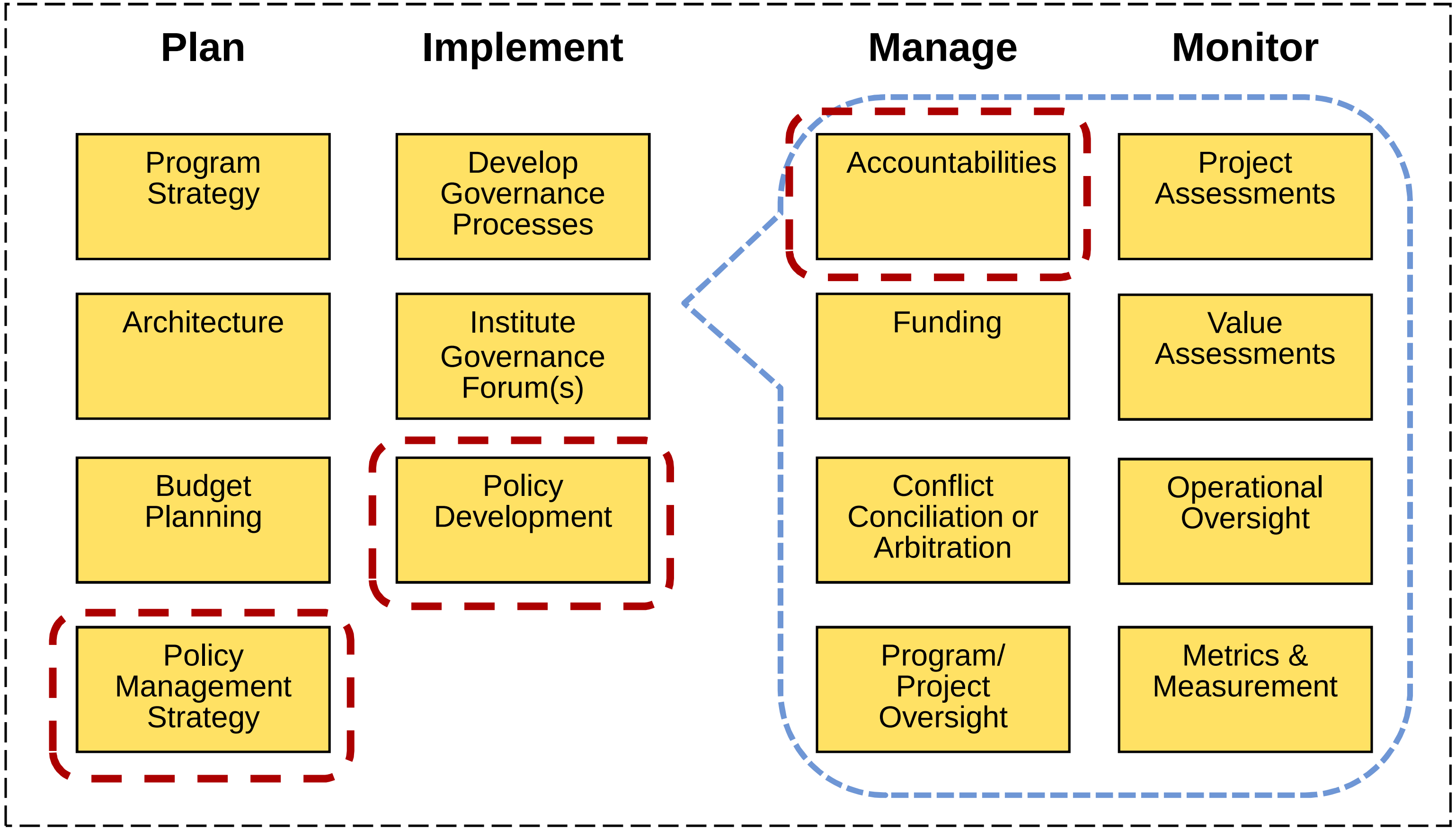


Security Strategy Planning



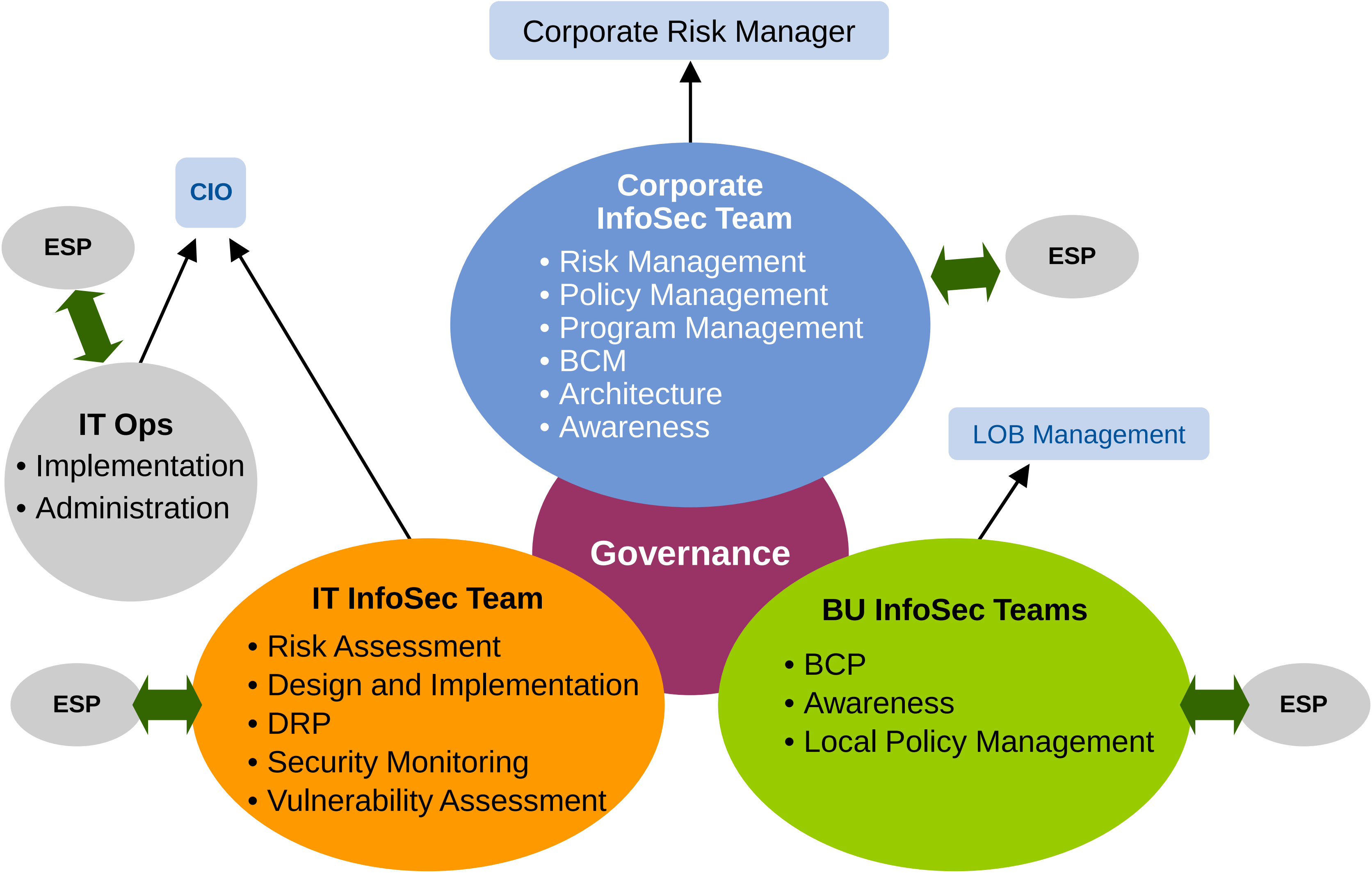
Gartner

Policy and Accountabilities



Gartner

Security Organization Dynamics



Corporate Risk Manager

CIO

ESP

Corporate InfoSec Team

- Risk Management
- Policy Management
- Program Management
- BCM
- Architecture
- Awareness

ESP

LOB Management

IT Ops

- Implementation
- Administration

Governance

ESP

IT InfoSec Team

- Risk Assessment
- Design and Implementation
- DRP
- Security Monitoring
- Vulnerability Assessment

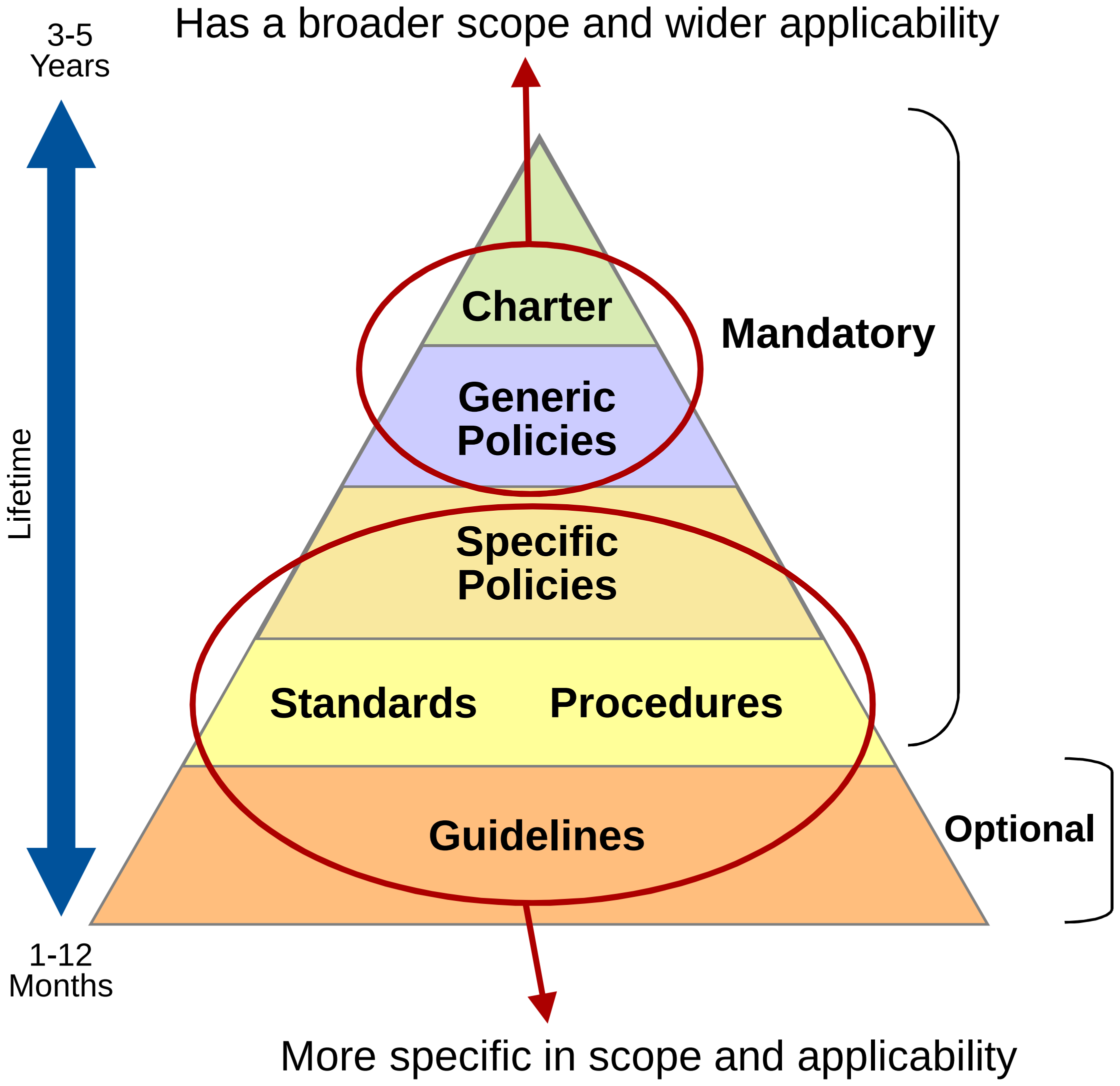
BU InfoSec Teams

- BCP
- Awareness
- Local Policy Management

ESP

Gartner

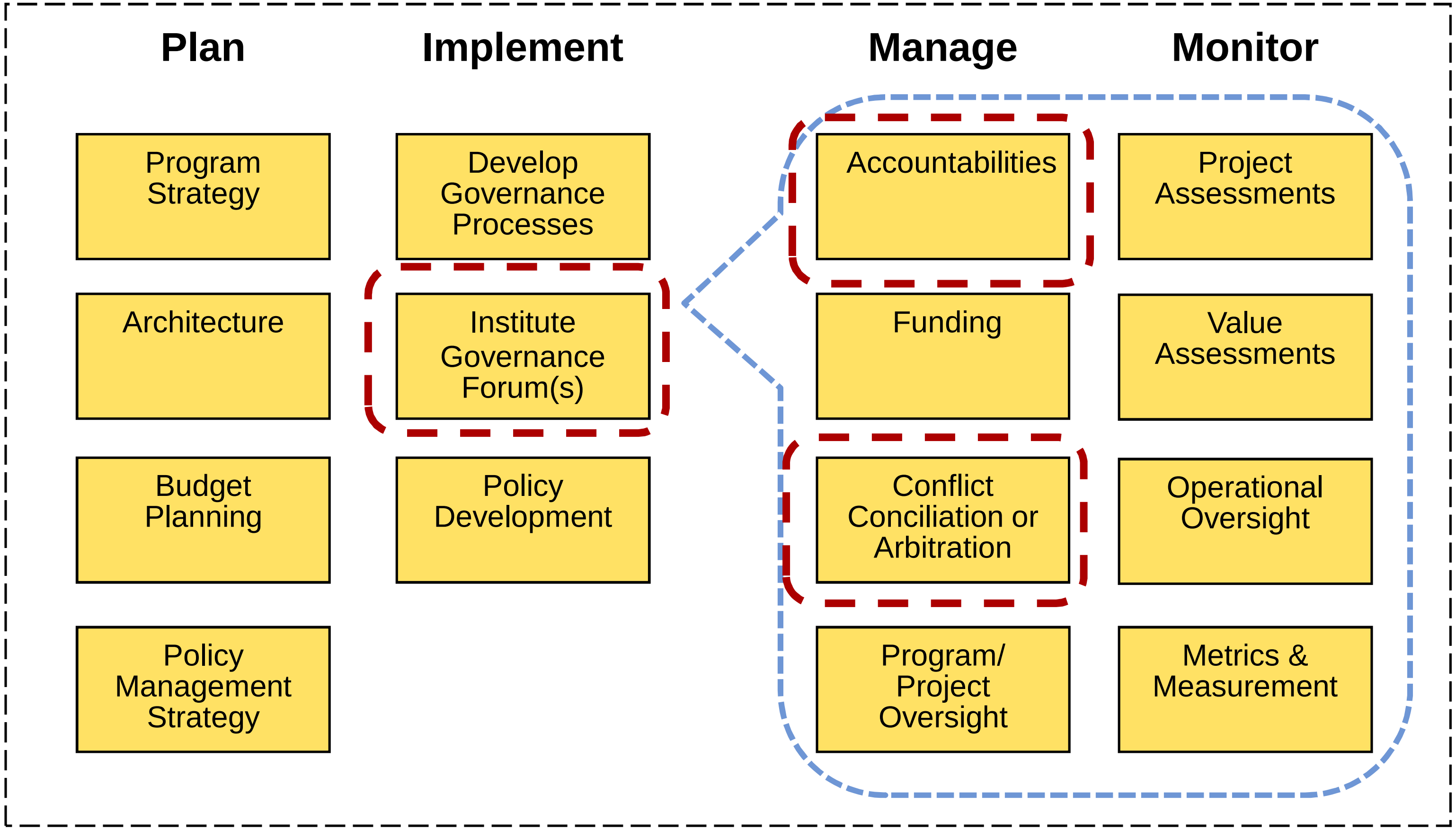
Effective Policy Management



Benefits of a policy framework:

- Defines a foundation that doesn't change often
- Documents can be kept short and concise
- Improves communication with stakeholders and auditors
- Establishes a clear connection from "what" to "how"
- Facilitates document standardization for consistency
- Simplifies storage and online retrieval of related policy documents

Manage Conflict

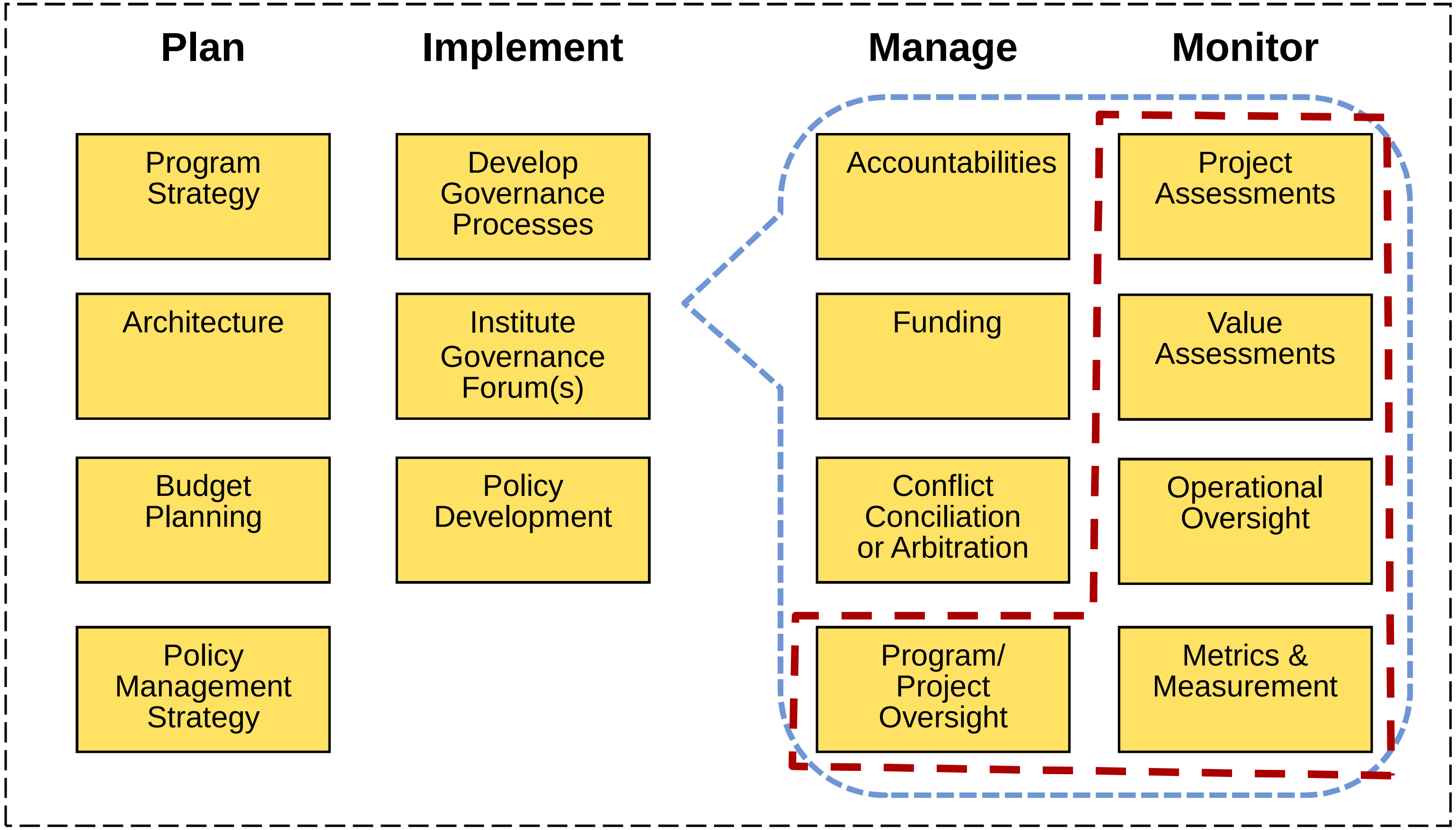


Plan	Implement	Manage	Monitor
Program Strategy	Develop Governance Processes	Accountabilities	Project Assessments
Architecture	Institute Governance Forum(s)	Funding	Value Assessments
Budget Planning	Policy Development	Conflict Conciliation or Arbitration	Operational Oversight
Policy Management Strategy		Program/ Project Oversight	Metrics & Measurement

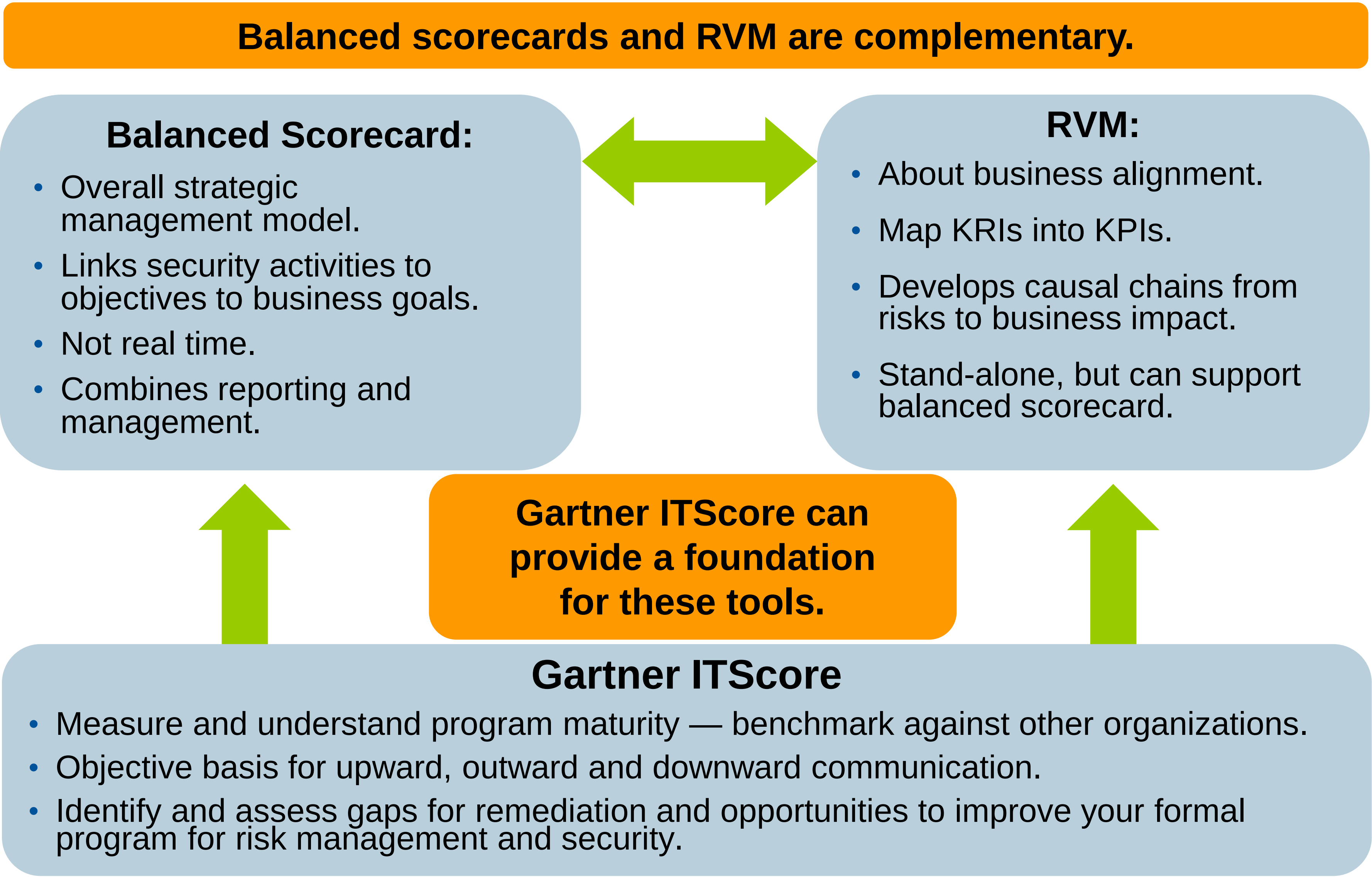
Conflict Resolution

- Approaches:
  - Dictatorial
  - Collaborative/Consensus — Mediation
  - Procedural (Have a Given Procedure to Assess and Allocate Risks and Benefits)
  - Arbitration
- Escalation

Provide Assurance



Balanced Scorecards, Risk-Adjusted Value Management (RVM) and Maturity



Balanced scorecards and RVM are complementary.

Balanced Scorecard:

- Overall strategic management model.
- Links security activities to objectives to business goals.
- Not real time.
- Combines reporting and management.

RVM:

- About business alignment.
- Map KRIs into KPIs.
- Develops causal chains from risks to business impact.
- Stand-alone, but can support balanced scorecard.

Gartner ITScore can provide a foundation for these tools.

Gartner ITScore

- Measure and understand program maturity — benchmark against other organizations.
- Objective basis for upward, outward and downward communication.
- Identify and assess gaps for remediation and opportunities to improve your formal program for risk management and security.

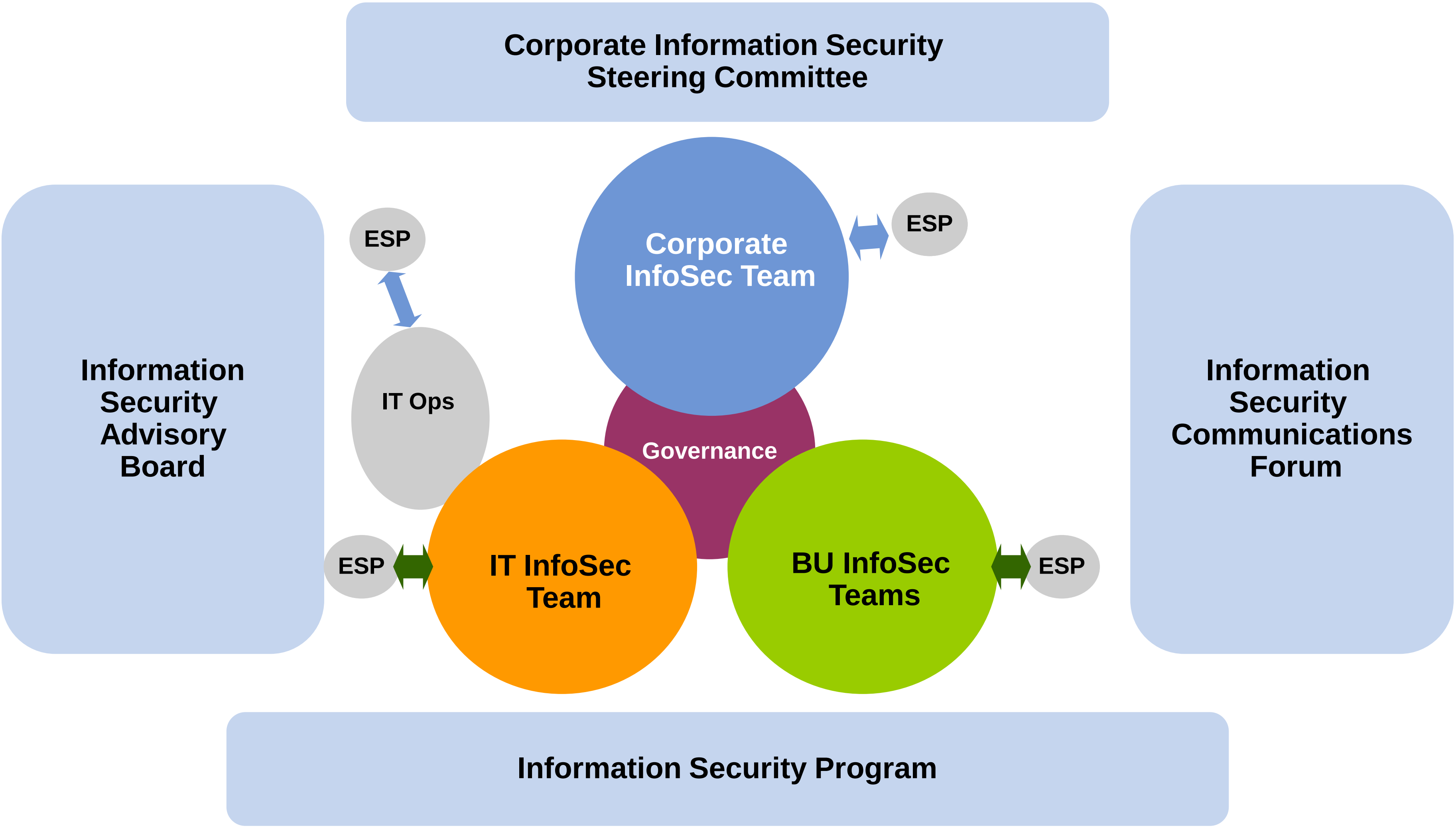
Security Governance Forums

Authority

Forums	Functions	Outcomes
Executive Sponsor	• Set accountability and authority	• Policy legitimacy and awareness • Authority of the information security program
High-Level Council(s)	• Policy and strategy definition • Program oversight • Conciliation/arbitration • Budget allocation • Approvals and exemptions	• Policy and strategy • Budgets • Priorities
Midlevel Council(s)	• Project oversight • Local policy definition • Reporting	• Local policies • Reports
Information Security Team(s)	• Project oversight • Operations oversight • Policy compliance monitoring • Reporting	• Compliance certifications and exceptions • Reports

Assurance

Sample Implementation


Corporate Information Security Steering Committee
Information Security Advisory Board
ESP
IT Ops
Corporate InfoSec Team
ESP
Governance
ESP
IT InfoSec Team
BU InfoSec Teams
ESP
Information Security Communications Forum
Information Security Program

Strategic Planning Assumption

Through 2015, 70% of large enterprises will successfully establish mature risk governance processes, up from 25% in 2011.

Recommendations

- ✓ Formalize a common definition of security and risk governance in your organization.
- ✓ Define and implement an information security and risk governance function that is integrated with the organization's corporate and IT governance functions.
- ✓ Focus on the governance processes and functions, rather than on the organizational position of the activities.

Recommended Gartner Research

- **Introducing the Gartner Information Security Governance Model**
  Tom Scholtz (G00201410)
- **Information Security and Risk Governance: Forums and Committees**
  Tom Scholtz, F. Christian Byrnes (G00207477)
- **Information Security and Risk Governance: Functions and Processes**
  Tom Scholtz (G00210937)
- **Security Governance and Operations Are Not the Same**
  Rob McMillan, Tom Scholtz (G00206708)
- **Survey Analysis: Information Security Governance, 2012**
  Tom Scholtz (G00233398)

For more information, stop by Gartner Research Zone.