Scuola universitaria professionale della Svizzera italiana
Dipartimento tecnologie innovative

SUPSI

C-I6021 - System Management

Angelo Consoli
ISIN
SUPSI-DTI

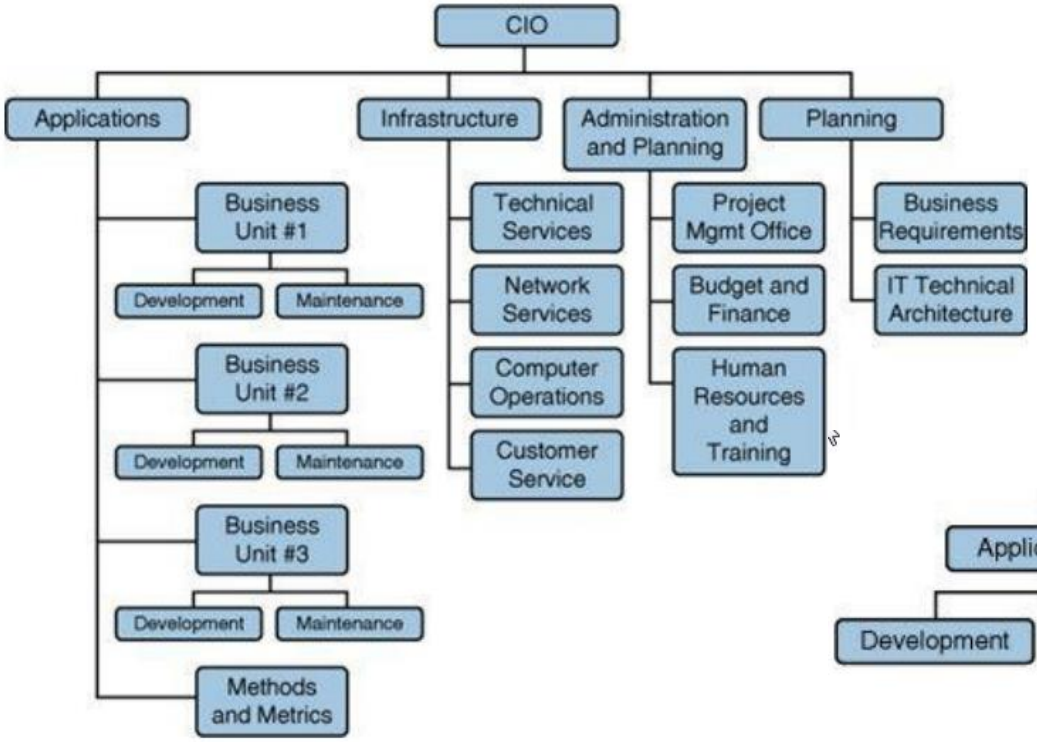
Executive Support

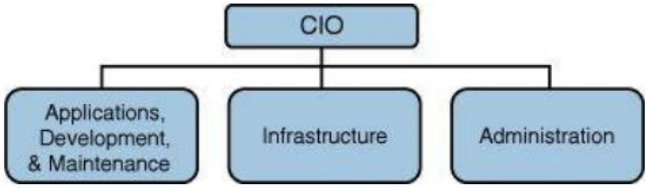
Executive support is crucial to system management

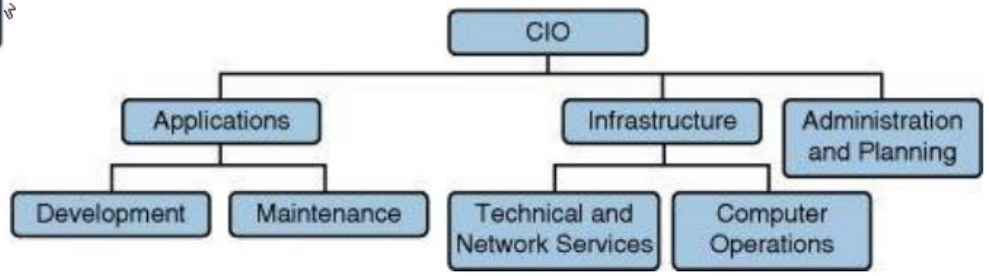
- What is Systems Management, what belongs to System Management
- Systems Management needs Executive Support
- The Benefits of Systems Management
  - Enabling Business Metrics
  - Creating the conditions to ensure Continuous Support
  - Create the bedrock for Business Continuity Planning (BCP)
  - Clarify Roles and Responsibilities
  - Involvement of Executive Support into execution level procedures

Organization models

- Factors to Consider in Designing IT Organizations







Organization models

- Factors to Consider in Designing IT Infrastructures
  - Know Your Business (KYB)
  - Locating Departments, Infrastructure, an available resources
  - Identify Process Owners

Importance of the right Staff

- Determining Required Skill Sets and Skill Levels
- Assessing the Skill Levels of Current Onboard Staff
  - Alternative Sources of Staffing
  - Recruiting Infrastructure Staff from the Outside (operative, consultive)
- Selecting the Most Qualified Candidate
- Retaining Key Personnel
- Using Consultants and Contractors
  - Benefits of Using Consultants and Contractors
  - Drawbacks of Using Consultants and Contractors
  - Steps for Developing Career Paths for Staff Members

Customer Service

- How IT Evolved into a Service Organization
- The Four Key Elements of Good Customer Service
  - Identifying Your Key Customers
  - Identifying Key Services of Key Customers
  - Identifying Key Processes that Support Key Services
  - Identifying Key Suppliers that Support Key Processes
- Integrating the Four Key Elements of Good Customer Service

Customer Service / Support

- The 9 Cardinal Deadly Sins of Customer Service and Support:
    1. Lack of empathy
    2. Offering no alternative solutions
    3. Cold service attitude
    4. Lack of active listening
    5. Robotic customer service
    6. Rulebook treatment
    7. Transferring agent to agent
    8. Ignoring customer's preference
    9. Not acknowledging mistakes

https://fluentsupport.com/deadly-sins-of-customer-support

Availability - 1

- Definition
- Differentiating Availability, Responsiveness, and Uptime
- Differentiating Slow Response from Downtime
- Differentiating Availability from High Availability
- Desired Traits of an Availability Process Owner
- Methods for Measuring Availability

S	Specific	Targets should be straightforward and emphasize what you want to happen
M	Measurable	If a target cannot be measured then you cannot determine whether it has been achieved
A	Achievable	It must be possible to achieve the target with an acceptable investment of time and resources
R	Relevant	Achieving the target must contribute to the overall business mission
T	Timely	The target must be something that can be achieved and measured over the reporting period of the SLA

Availability - 2

- The Seven “R”s of High Availability
  - Redundancy
  - Reputation
  - Reliability
  - Repairability
  - Recoverability
  - Responsiveness
  - Robustness
- Defining a Process to measure and monitor Infrastructure’s Availability
  - Committed hours of availability (A)
  - Outage hours (B)
  - *Achieved availability = ((A-B)/A)*100%*

Performance and Tuning

- Differences between the Performance and Tuning Process and Other Infrastructure Processes
- Definition of Performance and Tuning
- Preferred Characteristics of a Performance and Tuning Process Owner
- Performance and Tuning Applied to the Five Major Resource Environments
  - Server Environment
  - Disk Storage Environment
  - Database Environment
  - Network Environment
  - Client/ (Desktop Computer, Tablet, Smartphone, …) Environment
- Assessing an Infrastructure's Performance and Tuning Process
- Measuring and Streamlining the Performance and Tuning Process

Stakeholders: Rules and Roles

Step	Project Initiation	Project Executive	Project Manager	Business Analyst	Technical Architect	Application Developers
1	Task 1	C	A/R	C	I	I
2	Task 2	A	I	R	C	I
3	Task 3	A	I	R	C	I
4	Task 4	C	A	I	R	I

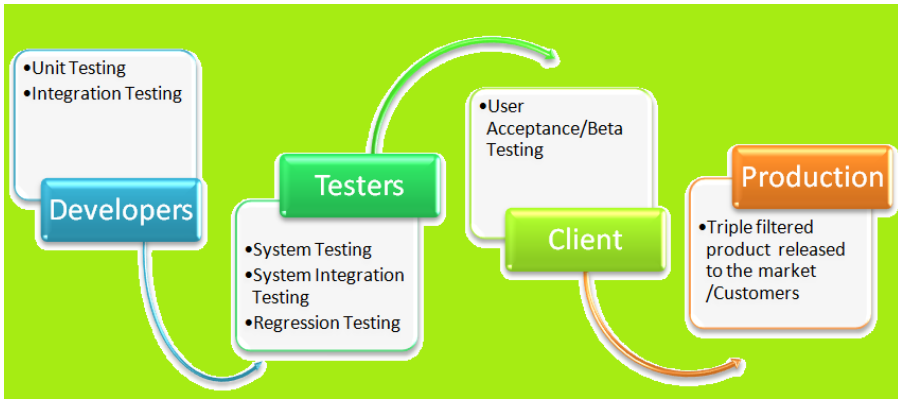
CIO/IDG

The 4 roles that stakeholders might play in any project include:

- **Responsible**: People or stakeholders who do the work. They must complete the task or objective or make the decision. Several people can be jointly Responsible.
- **Accountable**: Person or stakeholder who is the “owner” of the work. He or she must sign off or approve when the task, objective or decision is complete; must make sure that responsibilities are assigned in the matrix for all related activities. Success requires that there is only one person Accountable, which means that “the buck stops there.”
- **Consulted**: Who needs to give input before the work can be done and signed-off on. These people are “in the loop” and active participants.
- **Informed**: People or stakeholders who need to be kept “in the picture.” They need updates on progress or decisions, but they do not need to be formally consulted, nor do they contribute directly to the task or decision.

Production Acceptance - 1

- Definition of Production Acceptance
- The Benefits of a Production Acceptance Process
- Implementing a Production Acceptance Process
  - Step 1: Identify an Executive Sponsor
  - Step 2: Select a Process Owner
  - Step 3: Solicit Executive Support
  - Step 4: Assemble a Production Acceptance Team
  - Step 5: Identify and Prioritize Requirements
  - Step 6: Develop Policy Statements
  - Step 7: Nominate a Pilot System
  - Step 8: Design Appropriate Forms

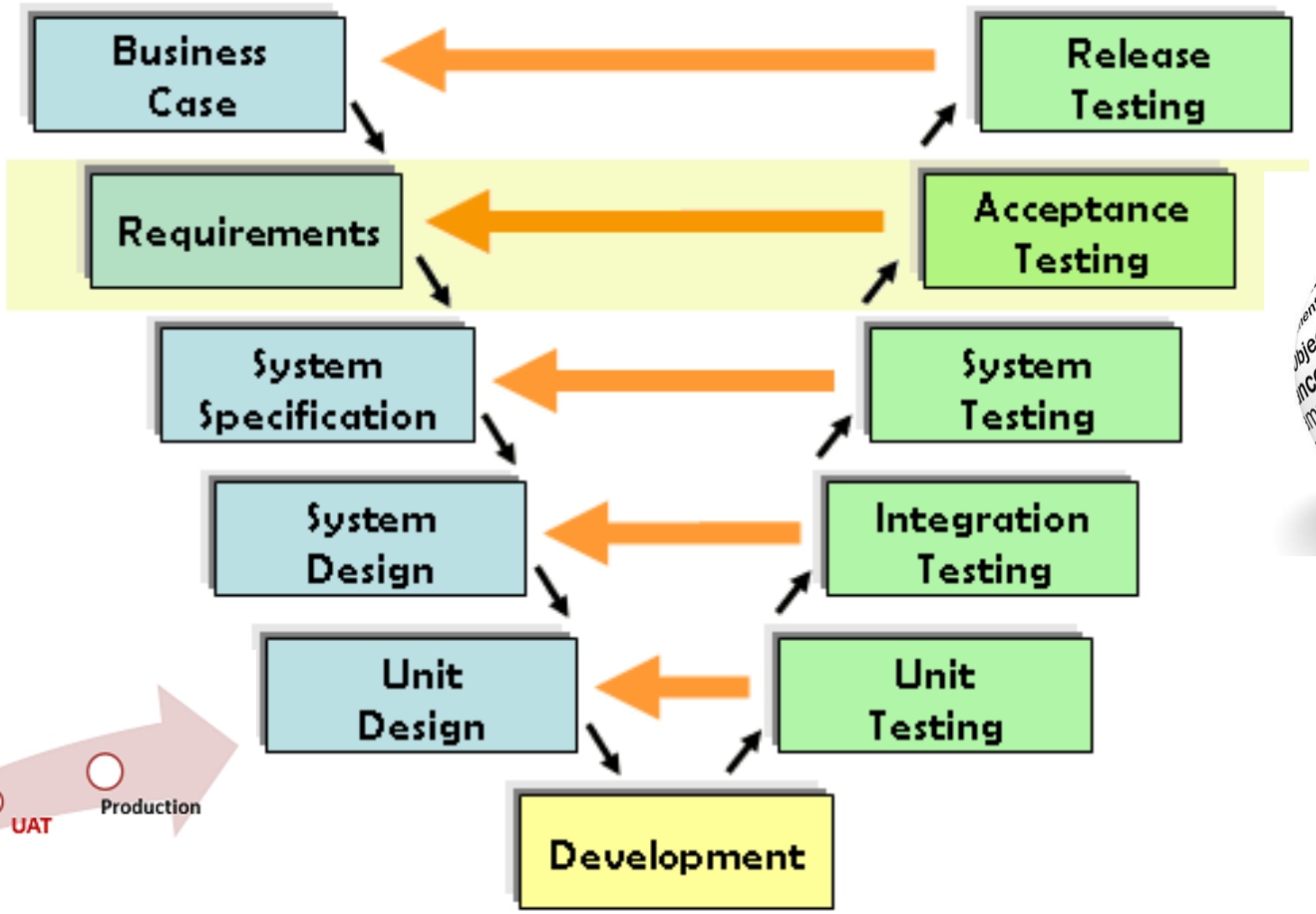


Production Acceptance - 2

Step 9: Document updates, extension and new procedures
Step 10: Run field tests and a solid pilot phase
Step 11: Revise Policies, Procedures, and Forms
Step 12: Define an adequate marketing strategy (if applicable)
Step 13: Conduct a lessons-learned sessions
Step 14: Follow-up with continuous reviews and improvements

- Full Deployment of a New Application
- Pay attention:
  - Production Acceptance is not Change Management
  - New Applications vs. New Versions of Existing Applications

From Business Objectives to User acceptance



Change Management - 1

- Definition of Change Management
- Drawbacks of Most Change Management Processes
- Key Steps Required in Developing a Change Management Process
  - Step 1: Identify an Executive Sponsor
  - Step 2: Assign a Process Owner
  - Step 3: Select a Cross-Functional Process Design Team
  - Step 4: Arrange for Meetings of the Cross-Functional Process Design Team
  - Step 5: Establish Roles and Responsibilities for Members Supporting the Process Design Team
  - Step 6: Identify the Benefits of a Change Management Process

(- cont. -)

Change Management - 2

Step 7: If Change Metrics Exist, Collect and Analyze them; If Not, Set Up a Process to Do So

Step 8: Identify and Prioritize Requirements

Step 9: Develop Definitions of Key Terms

Step 10: Design the Initial Change Management Process

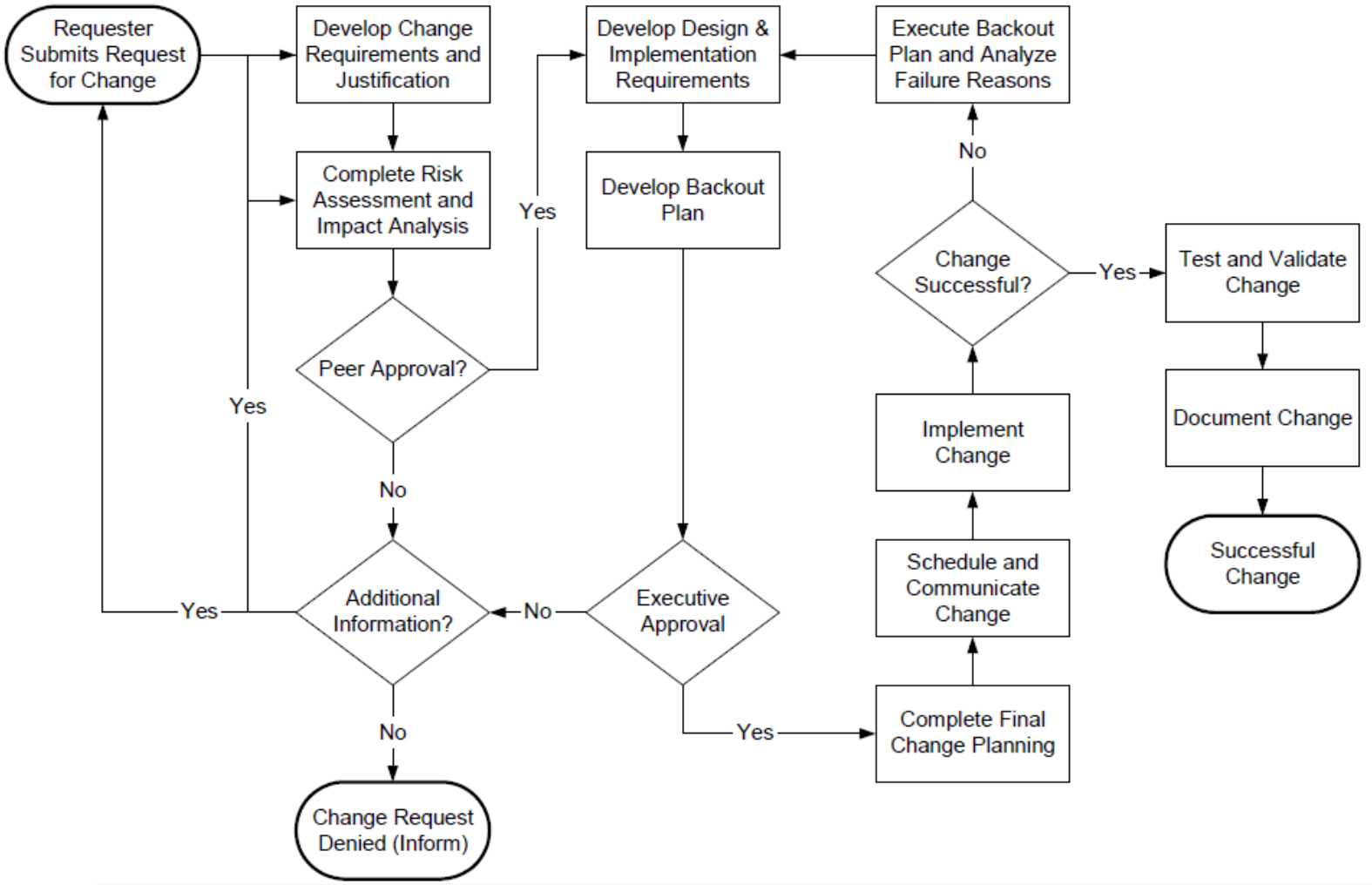
Step 11: Develop Policy Statements

Step 12: Develop a Charter for a Change Advisory Board (CAB)

Step 13: Use the CAB to Continually Refine and Improve the Change Management Process

- Emergency Changes Metric
- Assessing an Infrastructure's Change Management Process
- Measuring and Streamlining the Change Management Process

Change Management - 3



Tasks in the scope of Change Management Process

- Hardware – Installation, modification, removal or relocation of computing equipment.
- Software – Installation, patching, upgrade or removal of software products including operating systems, access methods, commercial off-the-shelf (COTS) packages, internally developed packages and utilities.
- SDLC – Changes handled through the formal software development life cycle will be included within the company's change management program.
- Database – Changes to databases or files such as additions, reorganizations and major
- maintenance.
- Application – Application changes being promoted to production as well as the integration of new application systems and the removal of obsolete elements.
- Changes to system configuration. : Moves, Adds, Changes and Deletes
- Schedule Changes - Requests for creation, deletion, or revision to job schedules, back-up schedules or other regularly scheduled jobs managed by the company's IT organization.
- Telephony – Installation, modification, de-installation, or relocation of PBX equipment and services.
- Desktop – Any modification or relocation of desktop equipment and services.
- Generic and Miscellaneous Changes – Any changes that are required to complete tasks associated with normal job requirements.

NOT part of Change Management Process

- Contingency/Disaster Recovery
- BCM related activities
- Changes to non-production elements or resources
- Changes made within the daily administrative process. Examples of daily administrative tasks:
  - Password resets
  - User adds/deletes
  - User modifications
  - Adding, deleting or revising security groups
  - Rebooting machines when there is no change to the configuration of the system
  - File permission changes

Problem Management - 1

- Definition of Problem Management
- Scope of Problem Management
- Distinguishing Between Problem, Change, and Request Management
- Distinguishing Between Problem Management and Incident Management
- The Role of the Service Desk
- Segregating and Integrating Service Desks
- Key Steps to Developing a Problem Management Process
  - Step 1: Select an Executive Sponsor
  - Step 2: Assign a Process Owner
  - Step 3: Assemble a Cross-Functional Team
  - Step 4: Identify and Prioritize Requirements

(- continue -)

Problem Management - 2

Step 5: Establish a Priority and Escalation Scheme
Step 6: Identify Alternative Call-Tracking Tools
Step 7: Negotiate Service Levels
Step 8: Develop Service and Process Metrics
Step 9: Design the Call-Handling Process
Step 10: Evaluate, Select, and Implement the Call-Tracking Tool
Step 11: Review Metrics to Continually Improve the Process

- Opening and Closing Problems
- Client Issues with Problem Management
  - Assessing an Infrastructure's Problem Management Process
  - Measuring and Streamlining the Problem Management Process

Storage Management

- What is Storage Management
- The important role of the Storage Management Process Owner
- Storage Management:
  - Capacity
  - Performance
  - Reliability
  - Recoverability
- Assessing an Infrastructure's Storage Management Process
- Measuring and Validate the Storage Management Process

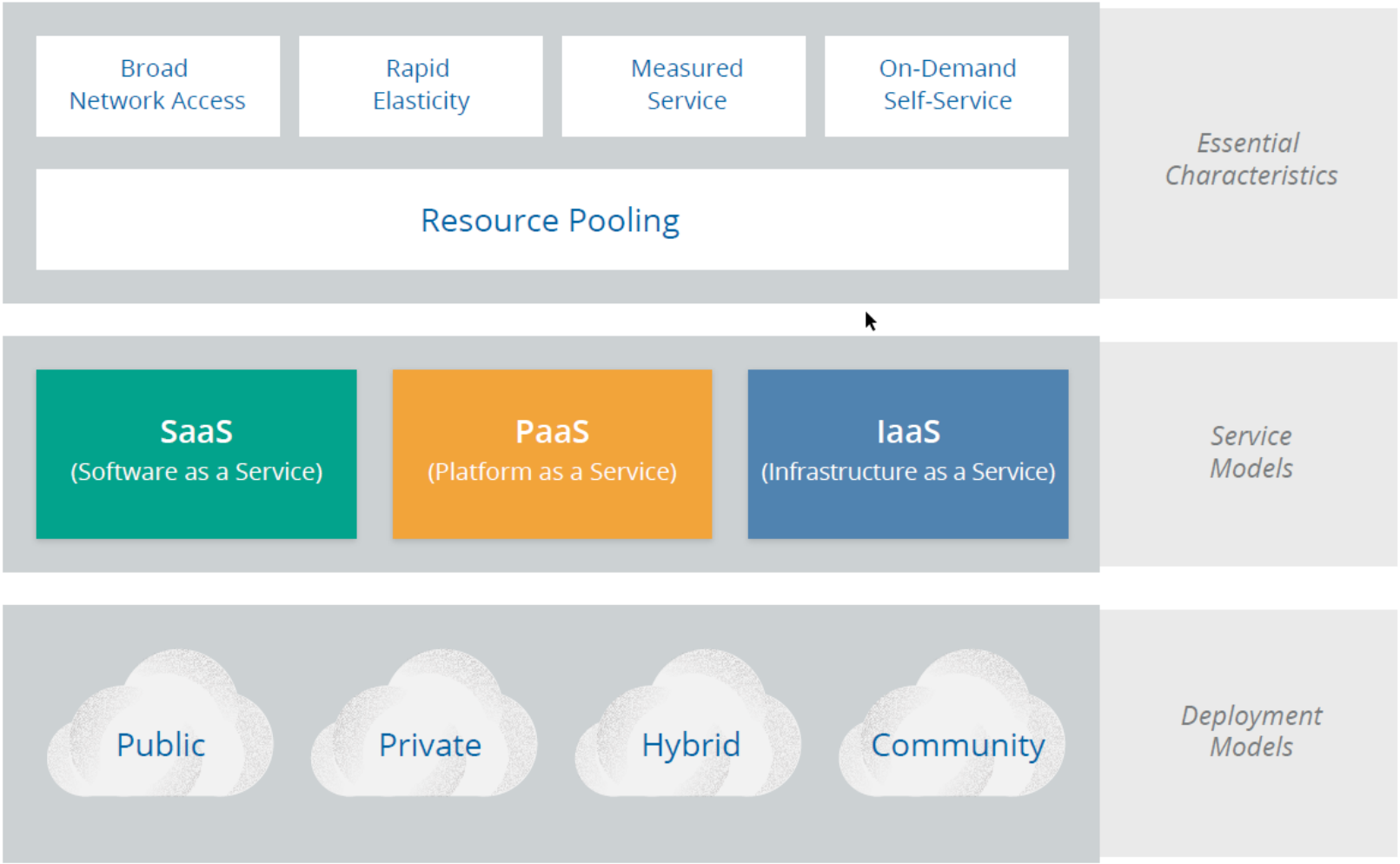
Network Management

- Definition of Network Management
- Key Decisions about Network Management
  - What Will Be Managed by This Process?
  - Who Will Manage It?
  - How Much Authority Will This Person Be Given?
  - What Types of Tools and Support Will Be Provided?
  - To What Extent Will Other Processes Be Integrated With This Process?
  - What Levels of Service and Quality Will Be Expected?
- Assessing an Infrastructure's Network Management Process
- Measuring and Streamlining the Network Management Process

Configuration Management

- Definition of Configuration Management
- Practical Tips for Improving Configuration Management
  1. Select a Qualified Process Owner
  2. Acquire Assistance of a Technical Writer or a Docum. Analyst
  3. Match the Backgrounds of Writers to Technicians
  4. Evaluate the Quality and Value of Existing Configuration Documentation
  5. Involve Appropriate Hardware Suppliers
  6. Involve Appropriate Software Suppliers
  7. Coordinate Documentation Efforts in Advance of Major Hardware and Software Upgrades
  8. Involve the Asset-Management Group for Desktop Equipment Inventories
- Assessing an Infrastructure's Configuration Management Process
- Measuring and Streamlining the Configuration Management Process

Cloud services



Cloud services

- Characteristics of a Cloud:
  - *Resource pooling* is the most fundamental characteristic, as discussed above. The provider abstracts resources and collects them into a pool, portions of which can be allocated to different consumers (typically based on policies).
  - Consumers provision the resources from the pool using *on-demand self-service*. They manage their resources themselves, without having to talk to a human administrator.
  - *Broad network access* means that all resources are available over a network, without any need for direct physical access; the network is not necessarily part of the service.
  - *Rapid elasticity* allows consumers to expand or contract the resources they use from the pool (provisioning and deprovisioning), often completely automatically. This allows them to more closely match resource consumption with demand (for example, adding virtual servers as demand increases, then shutting them down when demand drops).
  - *Measured service* meters what is provided, to ensure that consumers only use what they are allotted, and, if necessary, to charge them for it. This is where the term *utility computing* comes from, since computing resources can now be consumed like water and electricity, with the client only paying for what they use.

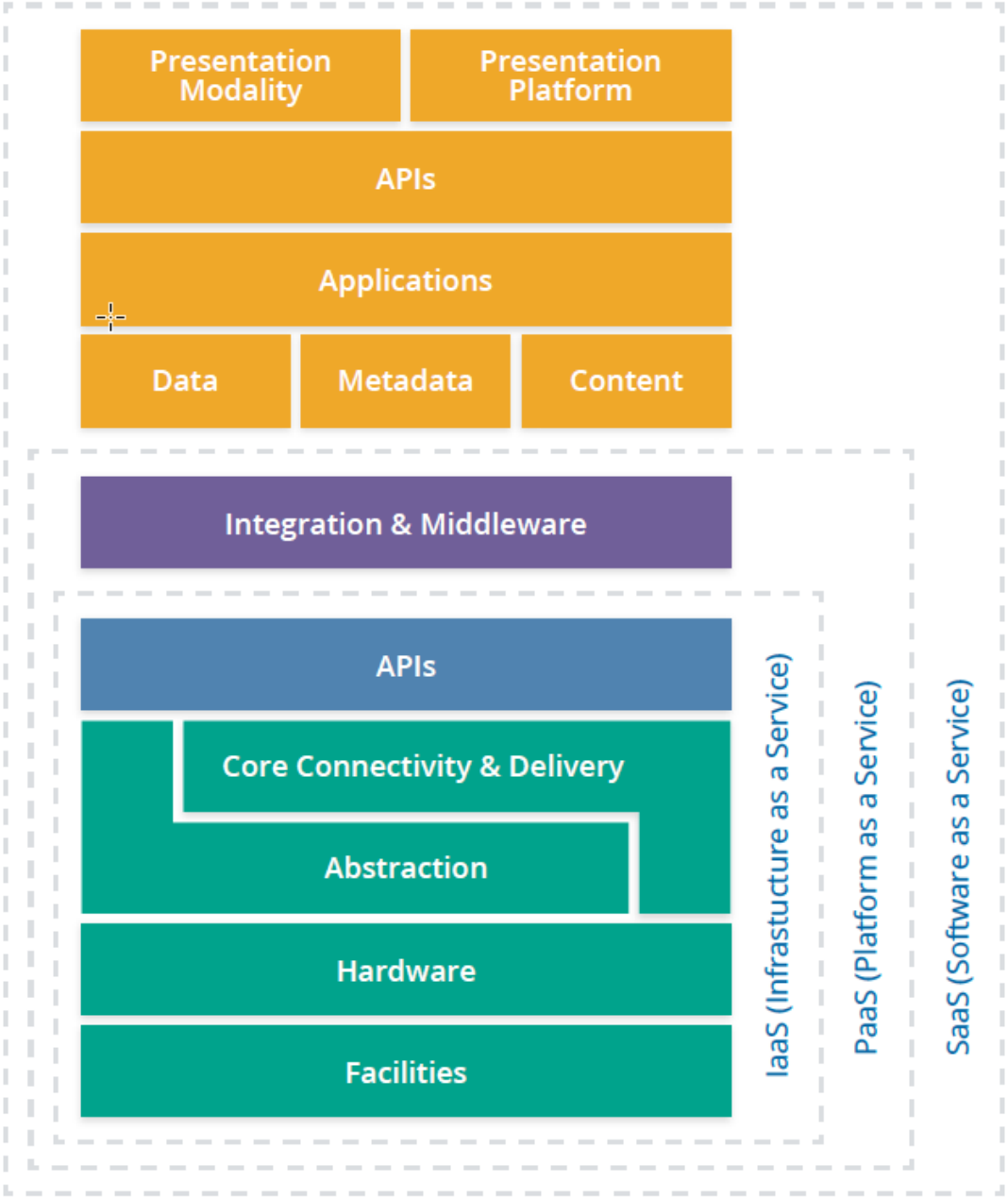
Cloud services

- *Software as a Service (**SaaS**)* is a full application that's managed and hosted by the provider. Consumers access it with a web browser, mobile app, or a lightweight client app.
- *Platform as a Service (**PaaS**)* abstracts and provides development or application platforms, such as databases, application platforms (e.g. a place to run Python, PHP, or other code), file storage and collaboration, or even proprietary application processing (such as machine learning, big data processing, or direct Application Programming Interfaces (API) access to features of a full SaaS application). The key differentiator is that, with PaaS, you don't manage the underlying servers, networks, or other infrastructure.
- *Infrastructure as a Service (**IaaS**)* offers access to a resource pool of fundamental computing infrastructure, such as compute, network, or storage.

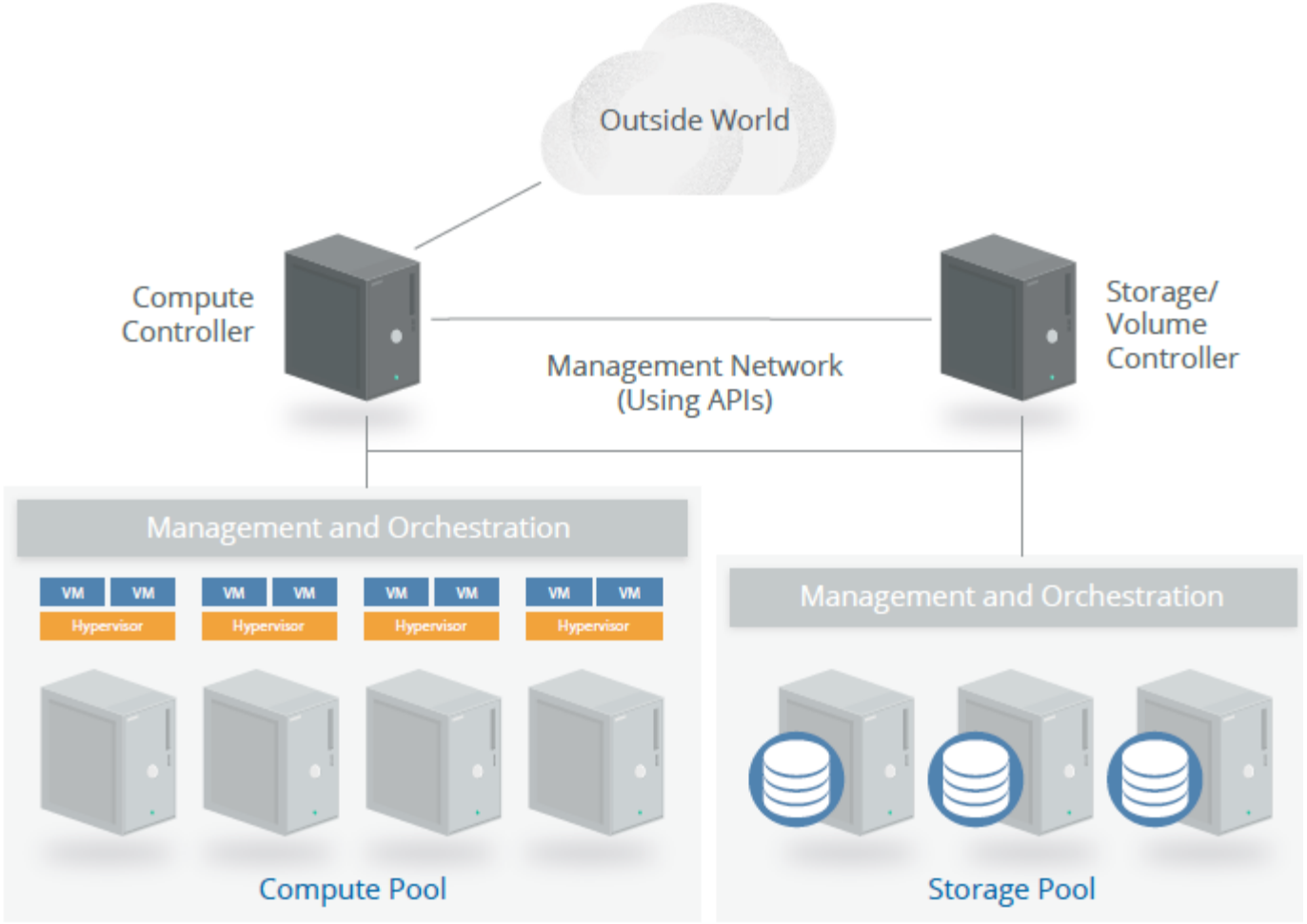
Cloud services security

	Infrastructure Owned By[1]	Infrastructure Owned By[2]	Infrastructure Located[3]	Accessible and Consumed By[4]
Public	Third-Party Provider	Third-Party Provider	Off-Premises	Untrusted
Private/ Community	Organization / Third-Party Provider	Organization / Third-Party Provider	On-Premises / Off-Premises	Trusted
Hybrid	Both Organization & Third-Party Provider	Both Organization & Third-Party Provider	Both On-Premises & Off-Premises	Trusted & Untrusted

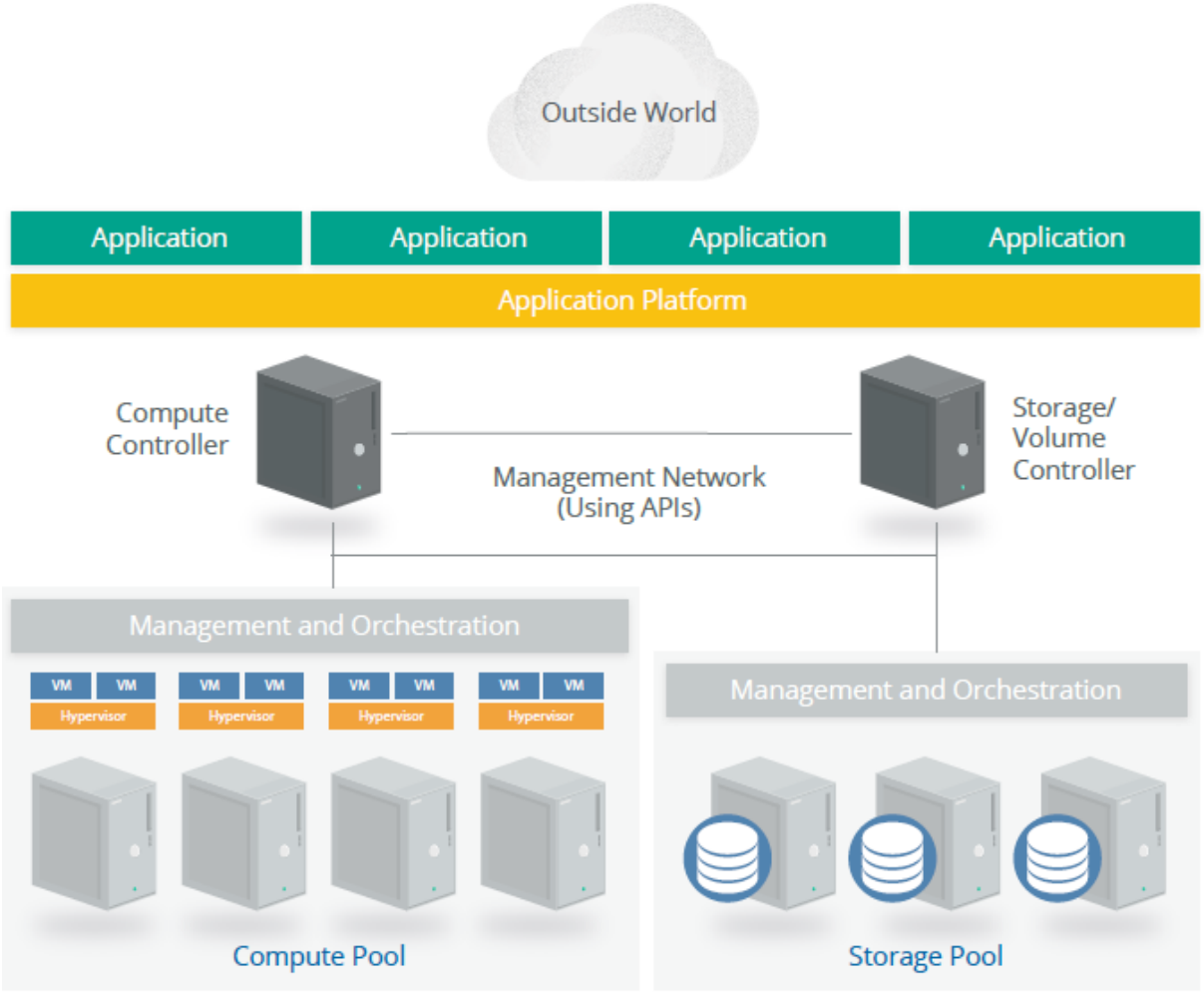
Cloud services: reference architecture



Cloud services: simplified architectural example of a compute IaaS platform



Cloud services: simplified architecture diagram shows an application platform (SaaS) running on top of our IaaS architecture



Capacity Planning - 1

- Definition of Capacity Planning
- Why Capacity Planning Is Seldom Done Well
  1. Analysts Are Too Busy with Day-To-Day Activities
  2. Users Are Not Interested (or able?) in Predicting Future Workloads
  3. Users Who Are Interested Cannot Forecast Accurately
  4. Capacity Planners May Be Reluctant to Use Effective Measuring Tools
  5. Need for updates: Corporate or IT Directions May Change over time (e.g. yearly)
  6. Planning Is Typically Not Part of an Infrastructure Culture
  7. Managers Sometimes Confuse Capacity Management with Capacity Planning

Capacity Planning - 2

- How to Develop an Effective Capacity Planning Process
  - Step 1: Select an Appropriate Capacity Planning Process Owner
  - Step 2: Identify the Key (Critical?) Resources to be Measured
  - Step 3: Monitor the Utilizations or Performance of the Resources
  - Step 4: Compare Utilizations to Maximum Capacities
  - Step 5: Collect Workload Forecasts from Developers and Users
  - Step 6: Transform Workload Forecasts into IT Resource Requirements
  - Step 7: Map Requirements onto Existing Utilizations
  - Step 8: Predict When the Business/Company Will Be Out of Capacity
  - Step 9: Update Forecasts and Utilizations

Capacity Planning - 3

- Additional Benefits of Capacity Planning
  1. Strengthens Relationships with Developers and End-Users
  2. Improves Communications with Suppliers
  3. Encourages Collaboration with Other Infrastructure Groups
  4. Promotes a Culture of Strategic Planning as Opposed to Tactical Firefighting
- Helpful Hints for Effective Capacity Planning
  1. Start Small
  2. Speak the Language of Your Customers
  3. Consider Future Platforms
  4. Share Plans with Suppliers
  5. Anticipate Nonlinear Cost Ratios
  6. Plan for Occasional Workload Reductions
  7. Prepare for the Turnover of Personnel
  8. Strive to Continually Improve the Process
  9. Evaluate the Hidden Costs of Upgrades

Capacity Planning - 4

- Uncovering the Hidden Costs of Upgrades
  1. Hardware Maintenance
  2. Technical Support
  3. Software Maintenance
  4. Memory Upgrades
  5. Channel Upgrades
  6. Cache Upgrades
  7. Data Backup Time
  8. Operations Support
  9. Offsite Storage
  10. Network Hardware
  11. Network Support
  12. Floor Space
  13. Power and Air Conditioning
- How to measure and streamline the Capacity Planning Process

Strategic Security

- Definition of Strategic Security
- Developing a Strategic Security Process
  - Step 1: Identify an Executive Sponsor
  - Step 2: Select a Security Process Owner
  - Step 3: Define Goals of Strategic Security
  - Step 4: Establish Review Boards
  - Step 5: Identify, Categorize, and Prioritize Requirements
  - Step 6: Inventory Current State of Security
  - Step 7: Establish Security Organization
  - Step 8: Develop Security Policies
  - Step 9: Assemble Planning Teams
  - Step 10: Review and Approve Plans
  - Step 11: Evaluate Technical Feasibility of Plans
  - Step 12: Assign and Schedule the Implementation of Plans
- Assessing an Infrastructure's Strategic Security Process
- Measuring and Streamlining the Security Process

Business Continuity - 1

- Definition of Business Continuity
- Steps to Developing an Effective Business Continuity Process
  - Step 1: Acquire Executive Support
  - Step 2: Select a Process Owner
  - Step 3: Assemble a Cross-Functional Team
  - Step 4: Conduct a Business Impact Analysis
  - Step 5: Identify and Prioritize Requirements
  - Step 6: Assess Possible Business Continuity Recovery Strategies

Business Continuity - 2

Step 7: Develop a Request for Proposal (RFP) for Outside Services

Step 8: Evaluate Proposals and Select the Best Offering

Step 9: Choose Participants and Clarify Their Roles on the Recovery Team

Step 10: Document the Business Continuity Plan

Step 11: Plan and Execute Regularly Scheduled Tests of the Plan

Step 12: Conduct a Lessons-Learned Postmortem after Each Test

Step 13: Continually Maintain, Update, and Improve the Plan

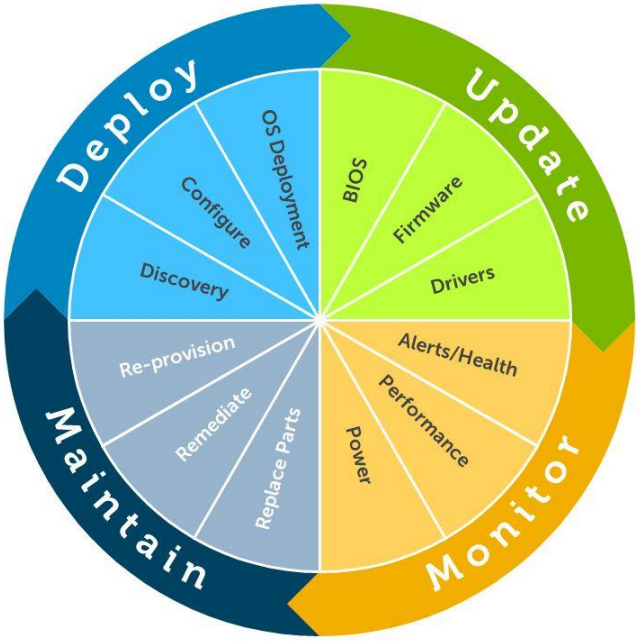
- Nightmare Incidents with Disaster Recovery Plans
- Assessing an Infrastructure's Disaster Recovery Process
- Measuring and Streamlining the Disaster Recovery Process

Facilities Management

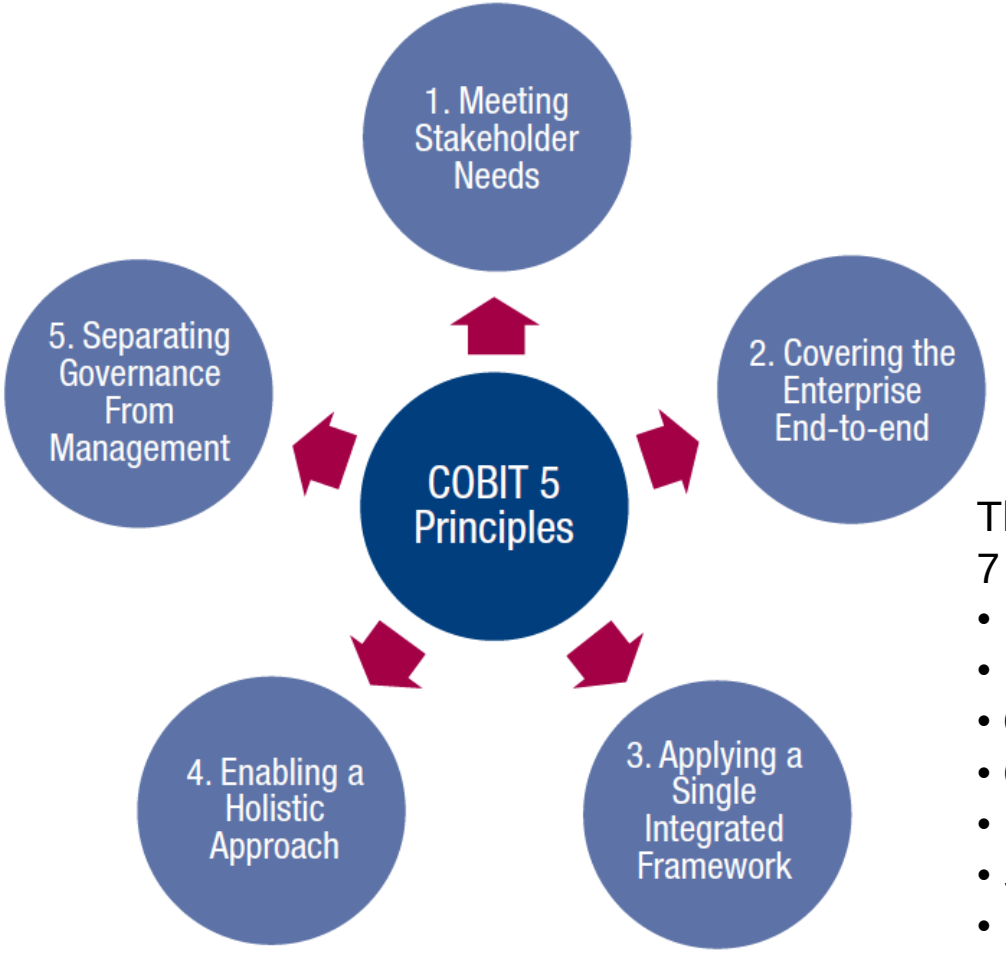
- Definition of Facilities Management
- Major Elements of Facilities Management
- The Facilities Management Process Owner
  - Determining the Scope of Responsibilities of a Facilities Management Process Owner
  - Desired Traits of a Facilities Management Process Owner
- Evaluating the Physical Environment
  - Major Physical Exposures Common to a Data Center
  - Keeping Physical Layouts Efficient and Effective
- Tips to Improve the Facilities Management Process
- Facilities Management at Outsourcing Centers
- Assessing an Infrastructure's Facilities Management Process
- Measuring and Streamlining the Facilities Management Process

IT Monitoring

- Monitoring Priorities for Systems Management
  - Operating System Performance and Availability
  - Server Hardware Status
  - Data and Storage Availability
  - Directory Services
  - Patches and Updates
  - Virtualization Infrastructure Performance
  - Problem and Incident Alarming and Reporting
  - Change Detection and Behavioral analysis
  - Capacity Planning
  - Email Server Monitoring
- The 80% rule
- Continous verification of adequateness



CoBIT Framework



The COBIT 5 framework defines
7 categories of enablers:

- Principles, Policies and Frameworks
- Processes
- Organisational Structures
- Culture, Ethics and Behaviour
- Information
- Services, Infrastructure and Applications
- People, Skills and Competencies

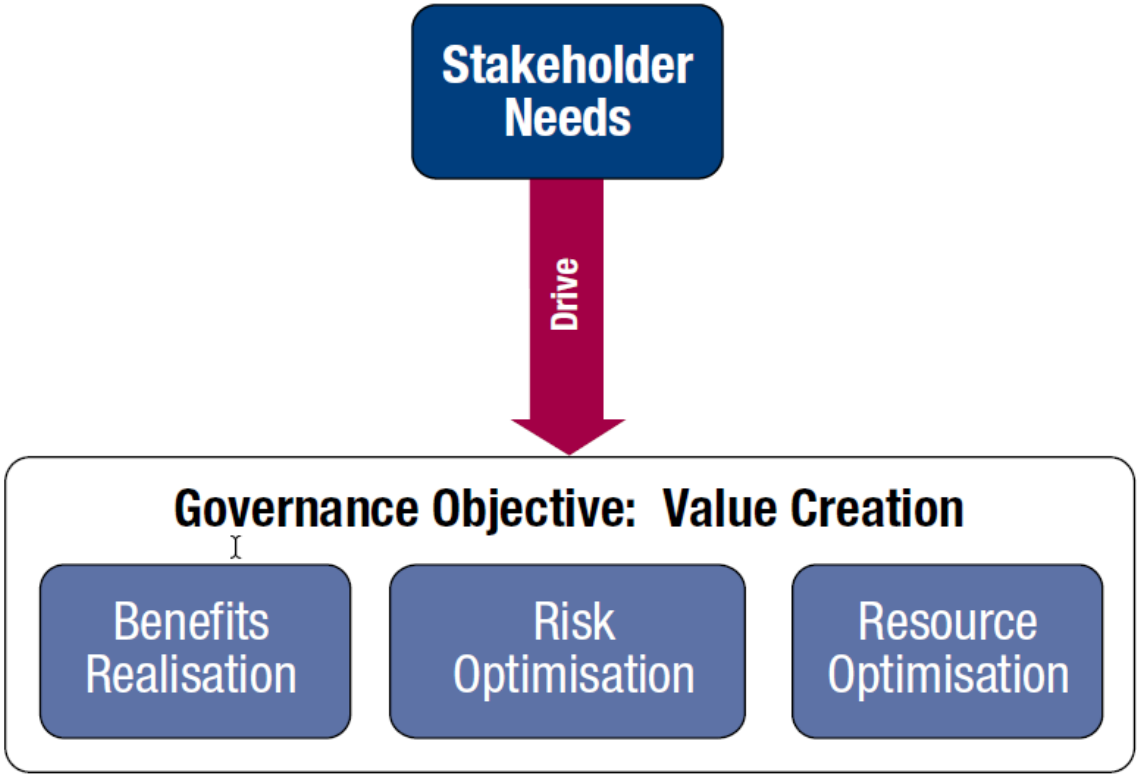
ISACA

- ISACA (*www.isaca.org*) is a leading global provider of
  - knowledge,
  - certifications,
  - community,
  - advocacy,
  - education on information systems (IS),
  - assurance and security,
  - enterprise governance and management of IT,
  - IT-related risk and compliance
- 95,000 constituents in 160 countries
- ISACA attests IT skills & knowledge through recognized certifications:
  - Certified Information Systems Auditor® (CISA®),
  - Certified Information Security Manager® (CISM®),
  - Certified in the Governance of Enterprise IT® (CGEIT®) and
  - Certified in Risk and Information Systems ControlTM (CRISCTM) designations

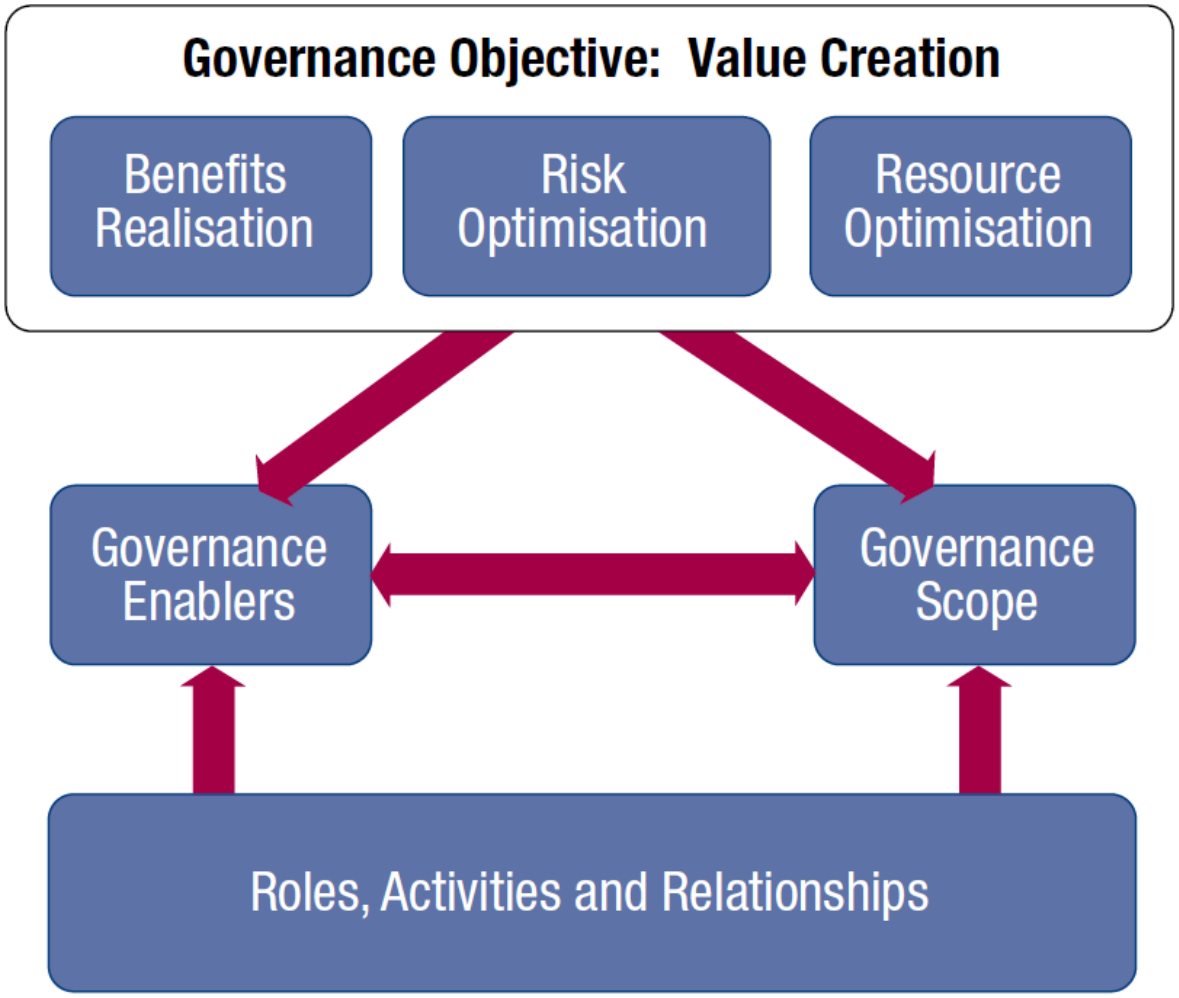
CoBIT Framework

- The COBIT 5 framework makes a clear distinction between governance and management. These two disciplines encompass different types of activities, require different organisational structures and serve different purposes. COBIT 5's view on this key distinction between governance and management is:
  - Governance ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritisation and decision making; and monitoring performance and compliance against agreed-on direction and objectives (e.g. board of directors).
  - Management plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives (e.g. CEO).

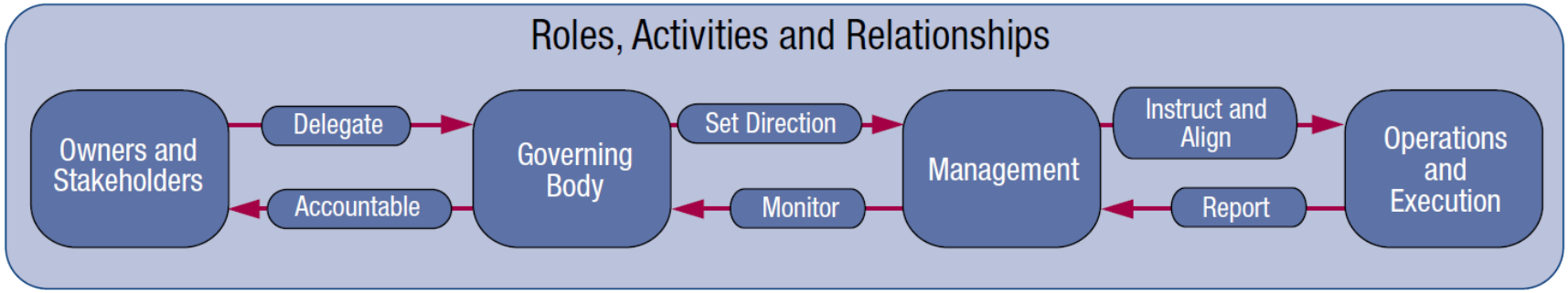
Governance Objective: the value creation



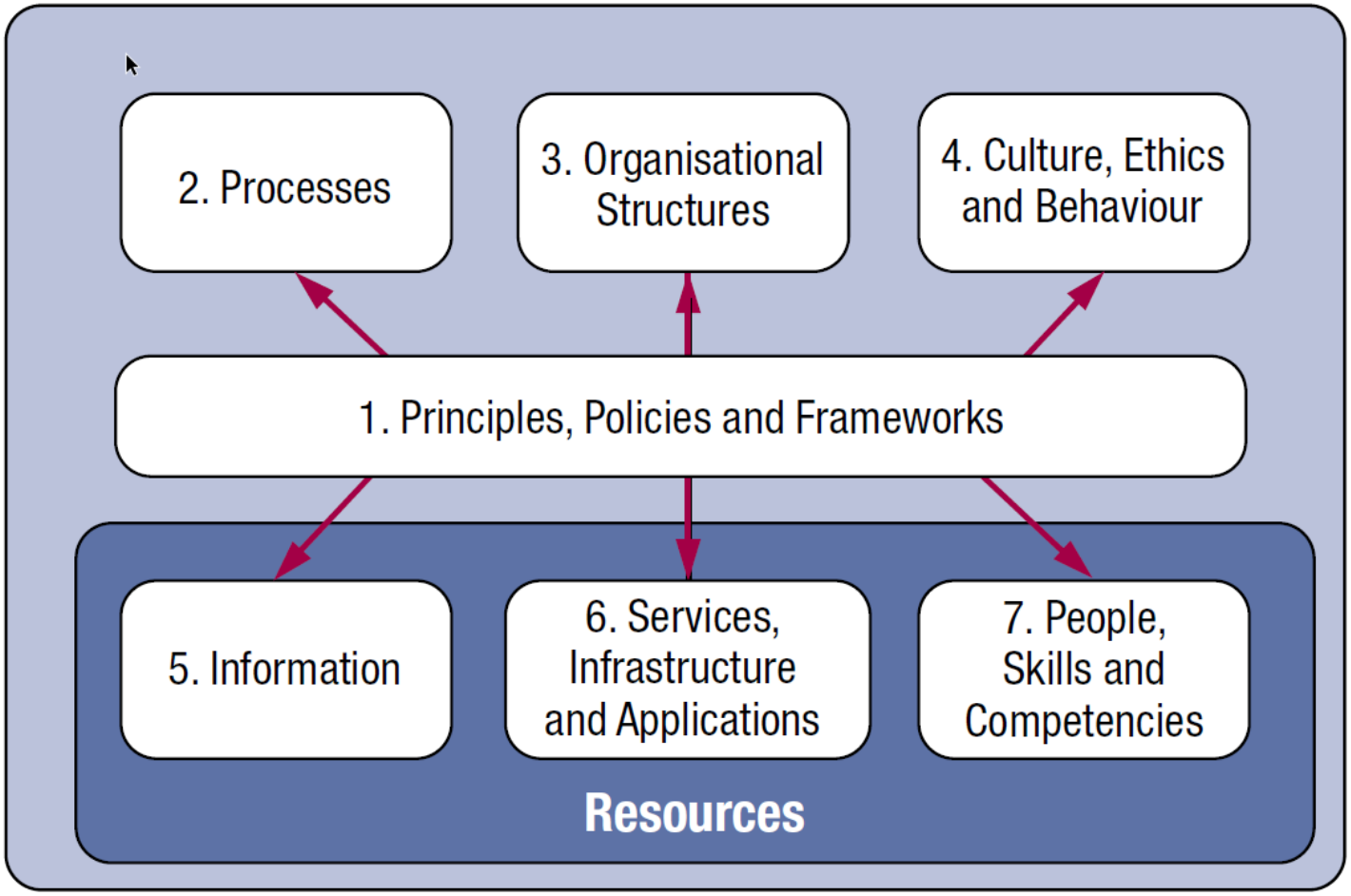
Governance and Management in COBIT5



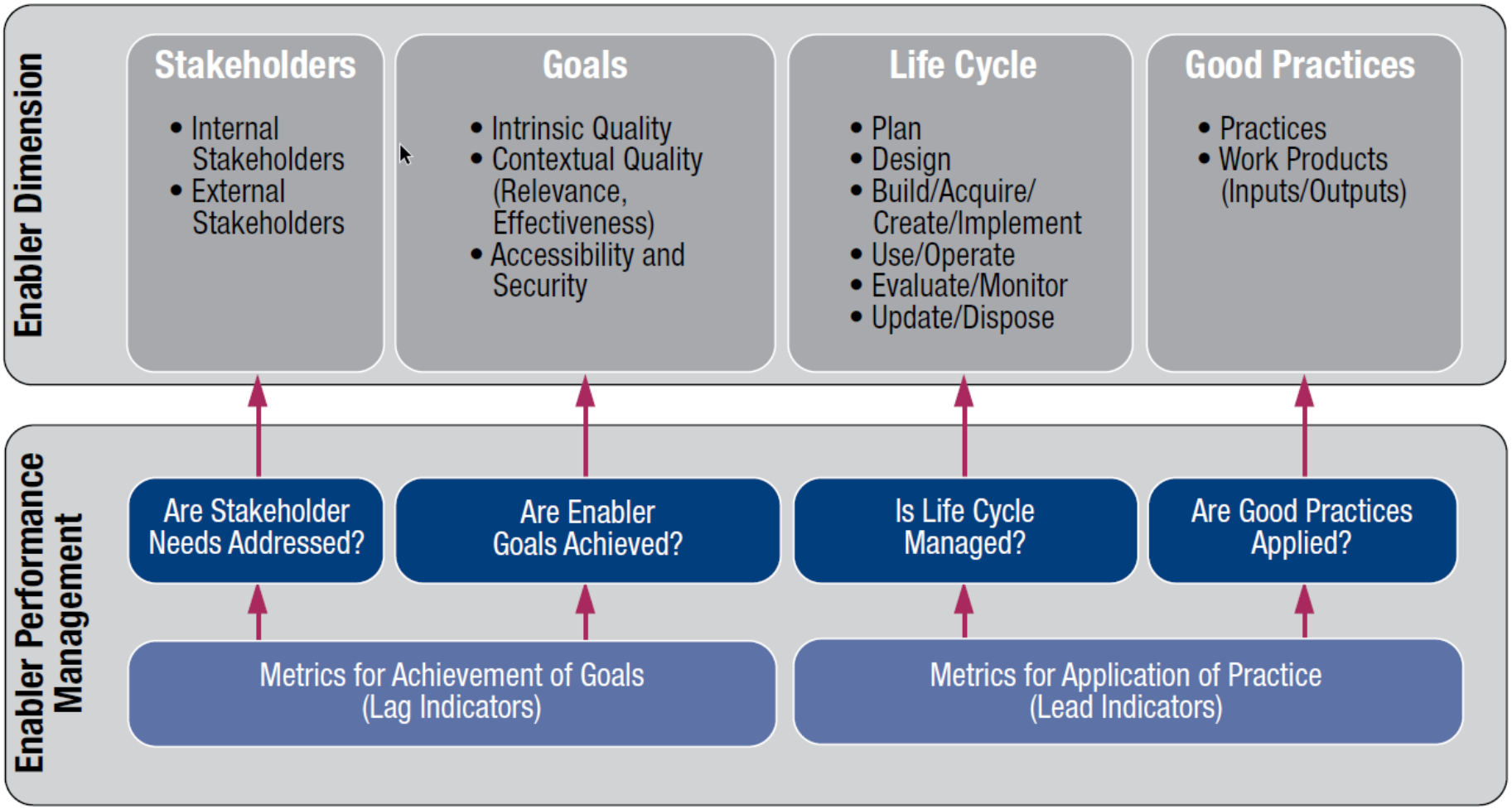
COBIT5 : Key Roles, Activities and Relationships



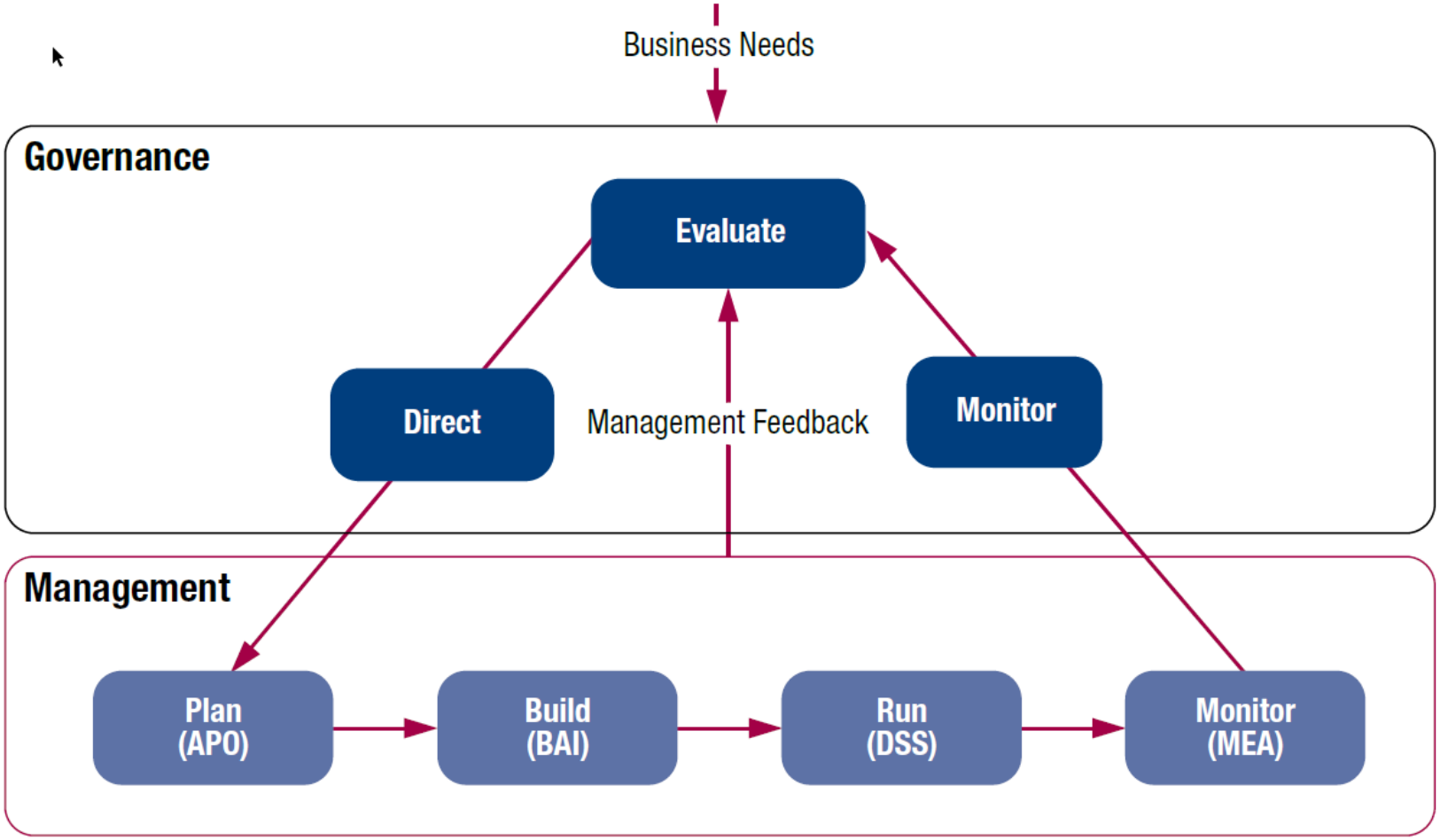
CoBIT 5: Enterprise Enablers



CoBIT 5: Enterprise Enablers



CoBIT 5: Management and Governance key areas and responsibilities



CoBIT: Table of Maturity Levels

5 Optimised—Processes have been refined to a level of good practice, based on the results of continuous improvement and maturity modelling with other enterprises. IT is used in an integrated way to automate the workflow, providing tools to improve quality and effectiveness, making the enterprise quick to adapt.

4 Managed and measurable—Management monitors and measures compliance with procedures and takes action where processes appear not to be working effectively. Processes are under constant improvement and provide good practice. Automation and tools are used in a limited or fragmented way.

3 Defined process—Procedures have been standardised and documented, and communicated through training. It is mandated that these processes should be followed; however, it is unlikely that deviations will be detected. The procedures themselves are not sophisticated, but are the formalisation of existing practices.

2 Repeatable but intuitive—Processes have developed to the stage where similar procedures are followed by different people undertaking the same task. There is no formal training or communication of standard procedures, and responsibility is left to the individual. There is a high degree of reliance on the knowledge of individuals and, therefore, errors are likely.

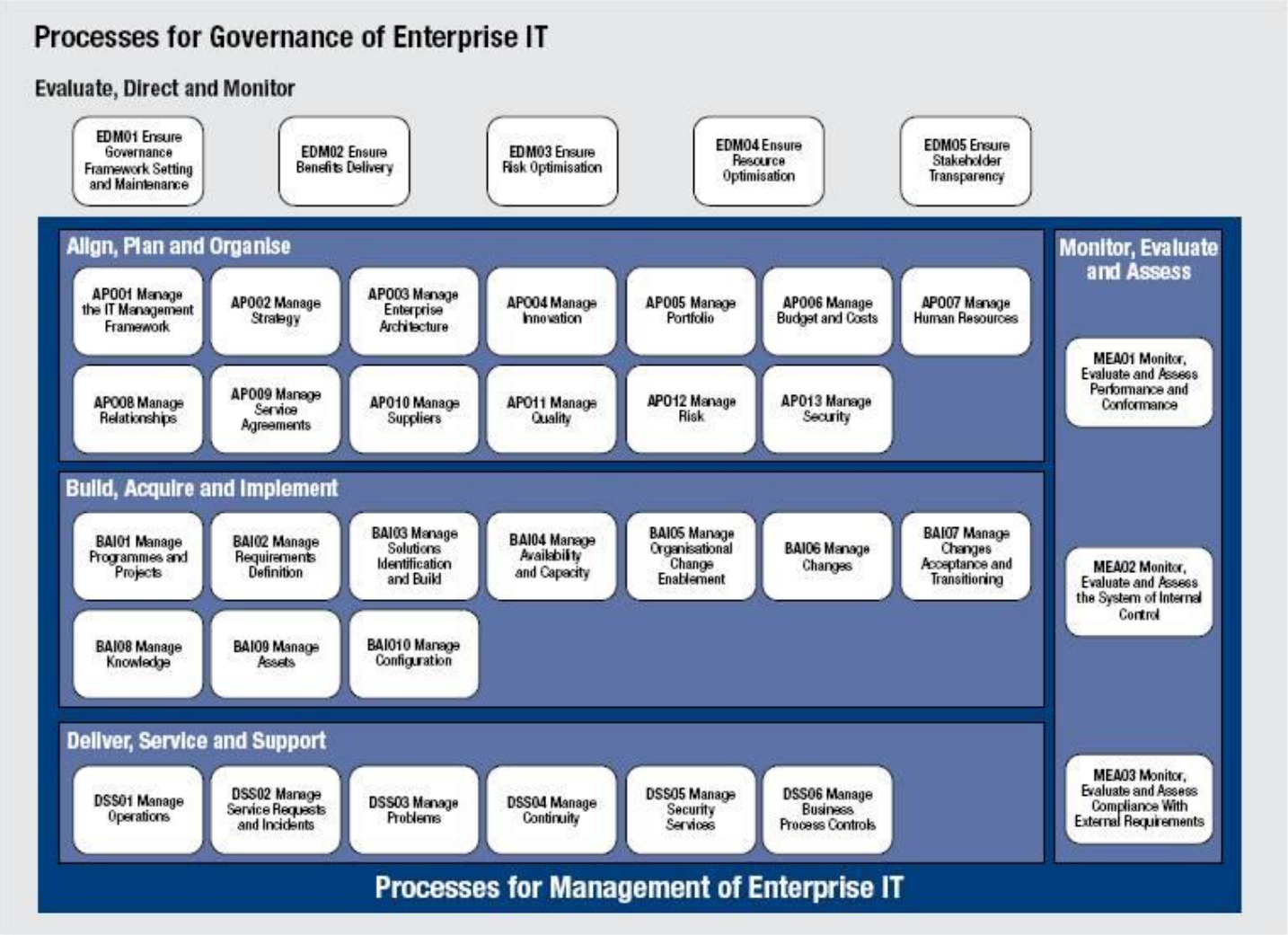
1 Initial/*Ad hoc*—There is evidence that the enterprise has recognised that the issues exist and need to be addressed. There are, however, no standardised processes; instead, there are *ad hoc* approaches that tend to be applied on an individual or case-by-case basis. The overall approach to management is disorganised.

0 Non-existent—Complete lack of any recognisable processes. The enterprise has not even recognised that there is an issue to be addressed.

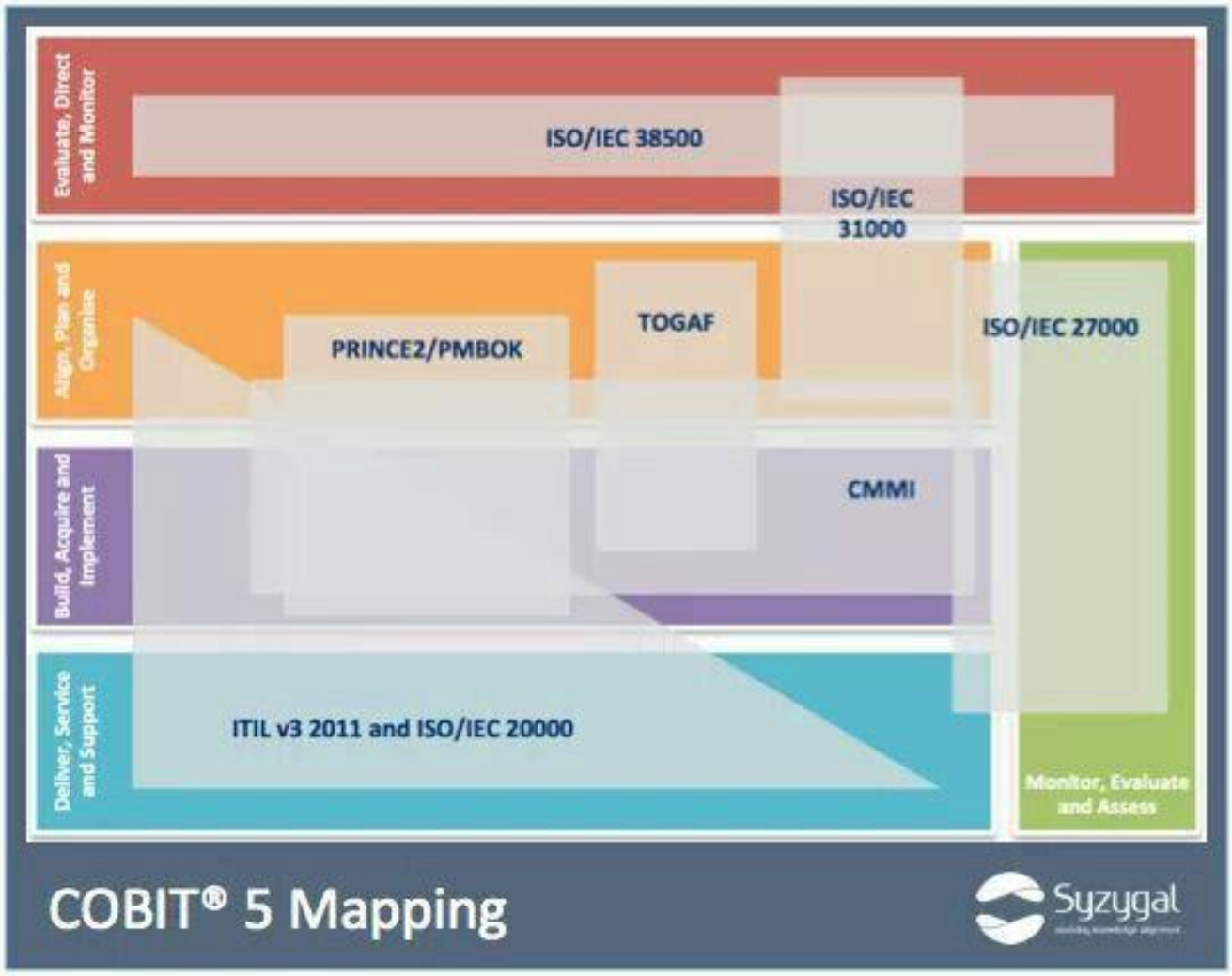
CoBIT 5 vs. CoBIT 4.1: Comparison of maturity attributes

Comparison Table of Maturity Attributes (COBIT 4.1) and Process Attributes (COBIT 5)									
	COBIT 5 Process Capability Attribute								
COBIT 4.1 Maturity Attribute	Process Performance	Performance Management	Work Product Management	Process Definition	Process Deployment	Process Measurement	Process Control	Process Innovation	Process Optimisation
Awareness and communication				■	■	■			
Policies, plans and procedures							■		
Tools and automation				■					
Skills and expertise				■	■				
Responsibility and accountability				■					
Goals setting and measurement		■				■			

CoBIT 5: Management and Governance



CoBIT 5: Management and Governance

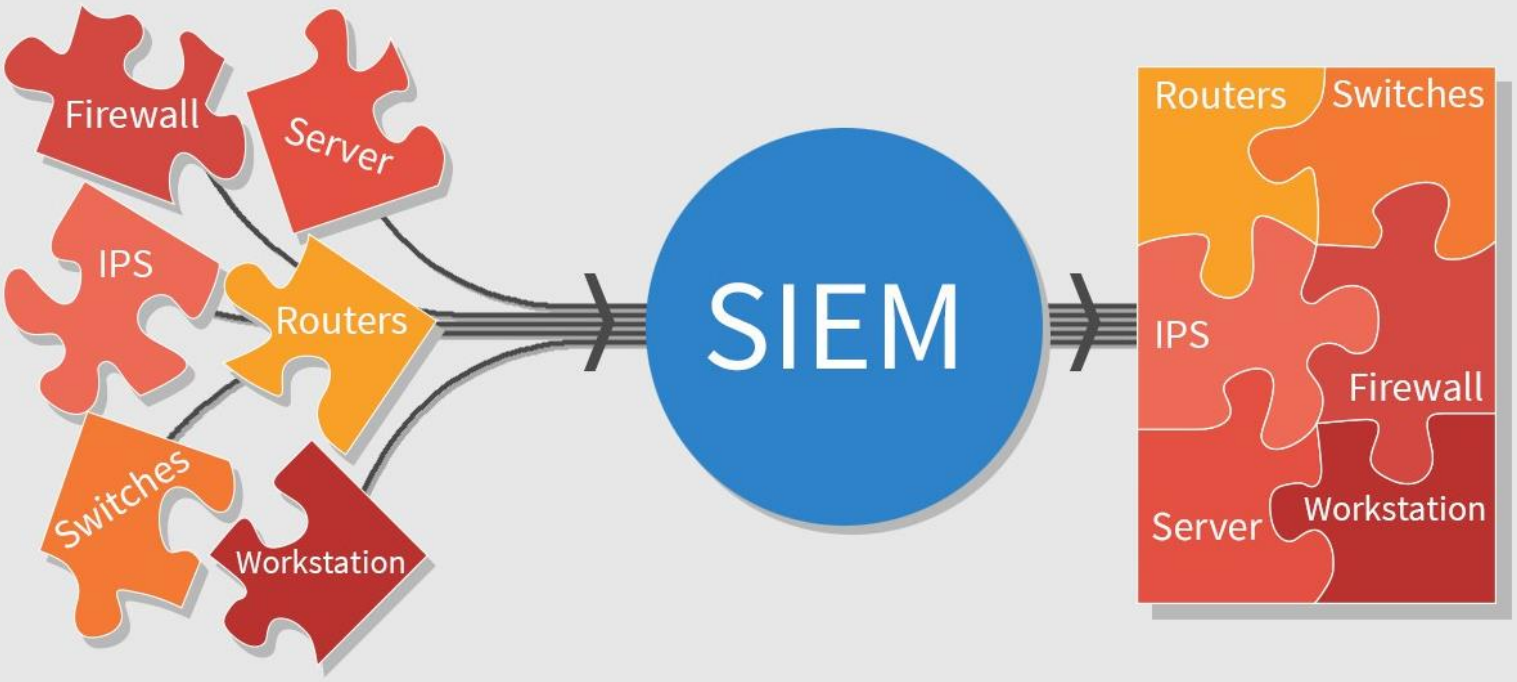


SIEM

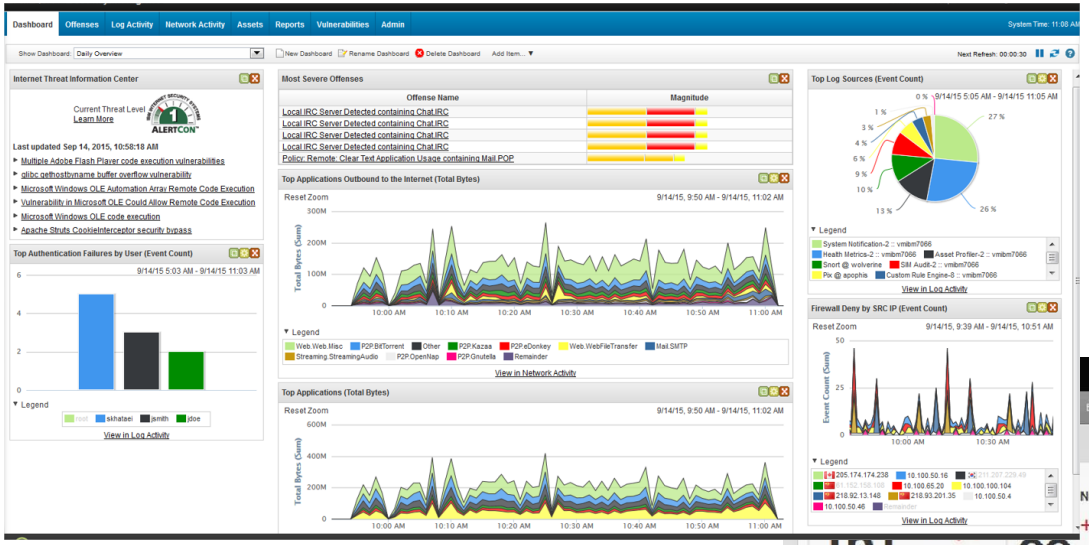
- Security information and event management (SIEM)
- A solution enterprise security professionals both insight into and a track record of the activities within their IT environment.
- Real time analysis of log and event data, to provide:
  - threat monitoring,
  - event correlation and
  - incident response

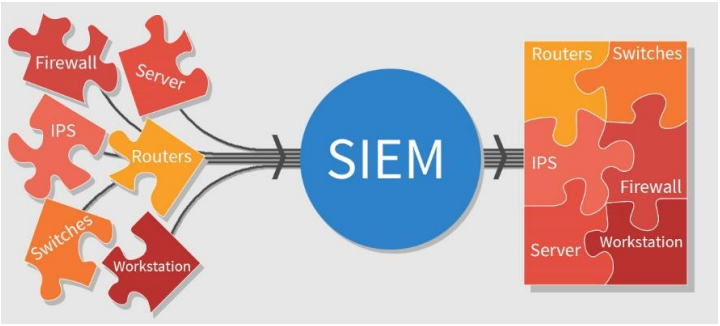
- Collects and aggregates log data generated throughout the organization's technology infrastructure:
  - servers
  - host systems
  - applications
  - network and
  - security devices such as firewalls and antivirus filters.

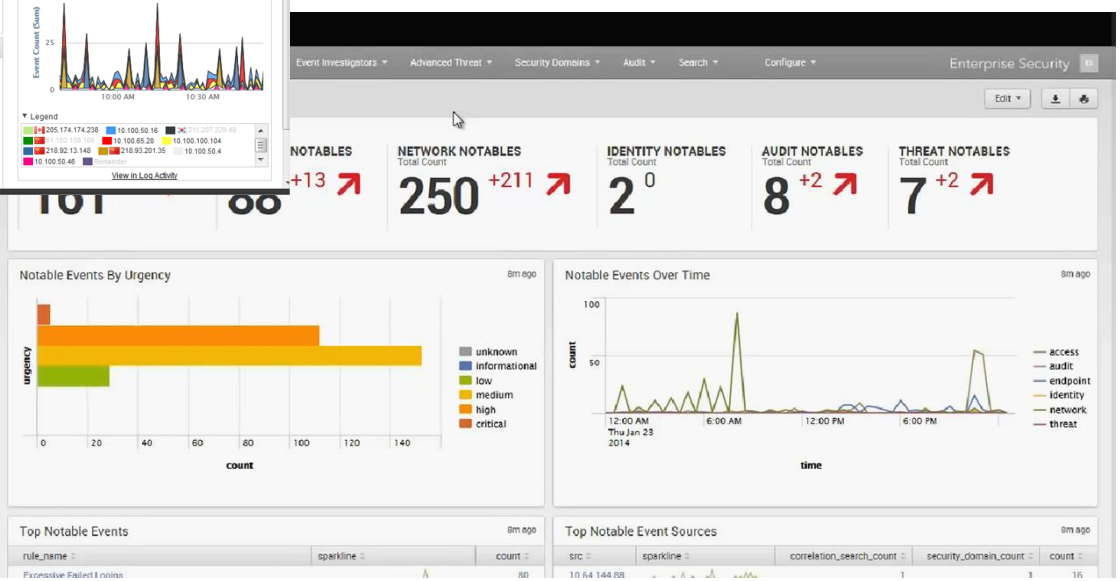
SIEM


Firewall
Server
IPS
Routers
Switches
Workstation
SIEM
Routers
Switches
IPS
Firewall
Server
Workstation

SIEM security information & event management







SIEM

Essential Capabilities of an Analytics-Driven SIEM	
Real-Time Monitoring	Threats can move quickly, and IT needs the ability to monitor threats and correlate events in real time to find and stop threats faster.
Incident Response	IT needs an organized way to address and manage potential breach as well as the aftermath of a security breach or attack in order to limit damage and reduce recovery time and cost.
User Monitoring	Monitoring user activity with context is critical to pinpoint breaches and uncover misuse. Privileged user monitoring is a common requirement for compliance reporting.
Threat Intelligence	Threat intelligence can help IT recognize abnormal activity, assess the risk to the business, and prioritize the response.
Advanced Analytics	Analytics are key to producing insights from mountains of data, and machine learning can automate this analysis to identify hidden threats.
Advanced Threat Detection	Security professionals need specialized tools to monitor, analyze and detect threats across the kill chain.
Use Case Library	Understanding and responding to threats in real time is imperative for organizations to reduce their risk.

SIEM: Magic Quadrant for Security Information and Event Management

SIEM

- SIEM software **identifies** and **categorizes incidents and events**, as well as analyzes them.

- SIEM has 2 main objectives:
  - providing reports on security-related incidents and events, such as successful and failed logins, malware activity and other possible malicious activities
  - sending alerts if the event analysis discovers an activity that runs against predetermined rulesets, indicating a potential security issue.

SIEM: 10 Priorities for System Management

- Priority 01 - *Operating System Performance and Availability*
- Priority 02 - *Server Hardware Status*
- Priority 03 - *Data and Storage Availability*
- Priority 04 - *Directory Services*
- Priority 05 - *Patches and Updates*
- Priority 06 - *Virtualization Infrastructure Performance*
- Priority 07 - *Problem and Incident Alarming and Reporting* **!!!**
- Priority 08 - *Change Detection*
- Priority 09 - *Capacity Planning*
- Priority 10 - *Email Server Monitoring*

*The key to effective incident management is **prompt identification** of the failure.*

SIEM: 7 Priorities for Network Management

- Priority 01 - *Get the Network Under Management*
- Priority 02 - *Define Device Groupings*
  - Device Type
  - Geographical
  - Organizational
- Priority 03 - *Prioritized Availability Monitoring*
- Priority 04 - *Add Device-level Performance Monitoring*
  - Monitoring device resources
  - Monitoring ports/interfaces
  - Setting performance thresholds
  - Identifying trends
- Priority 05 - *Get Change Under Control*
- Priority 06 - *Add Application Awareness*
- Priority 07 - *Integrate and Communicate*
  - Help desk and trouble ticketing
  - Systems and application monitoring
  - Security monitoring and management
  - Line of business and end users

SIEM: 5 Priorities for Network Security

- Priority 01 - *Identity and Access Management (IAM)*
- Priority 02 - *Vulnerability Management*
- Priority 03 - *Change Monitoring*
- Priority 04 - *Correlated, Centralized Event Management and Analysis*
- Priority 05 - *Incident Response*

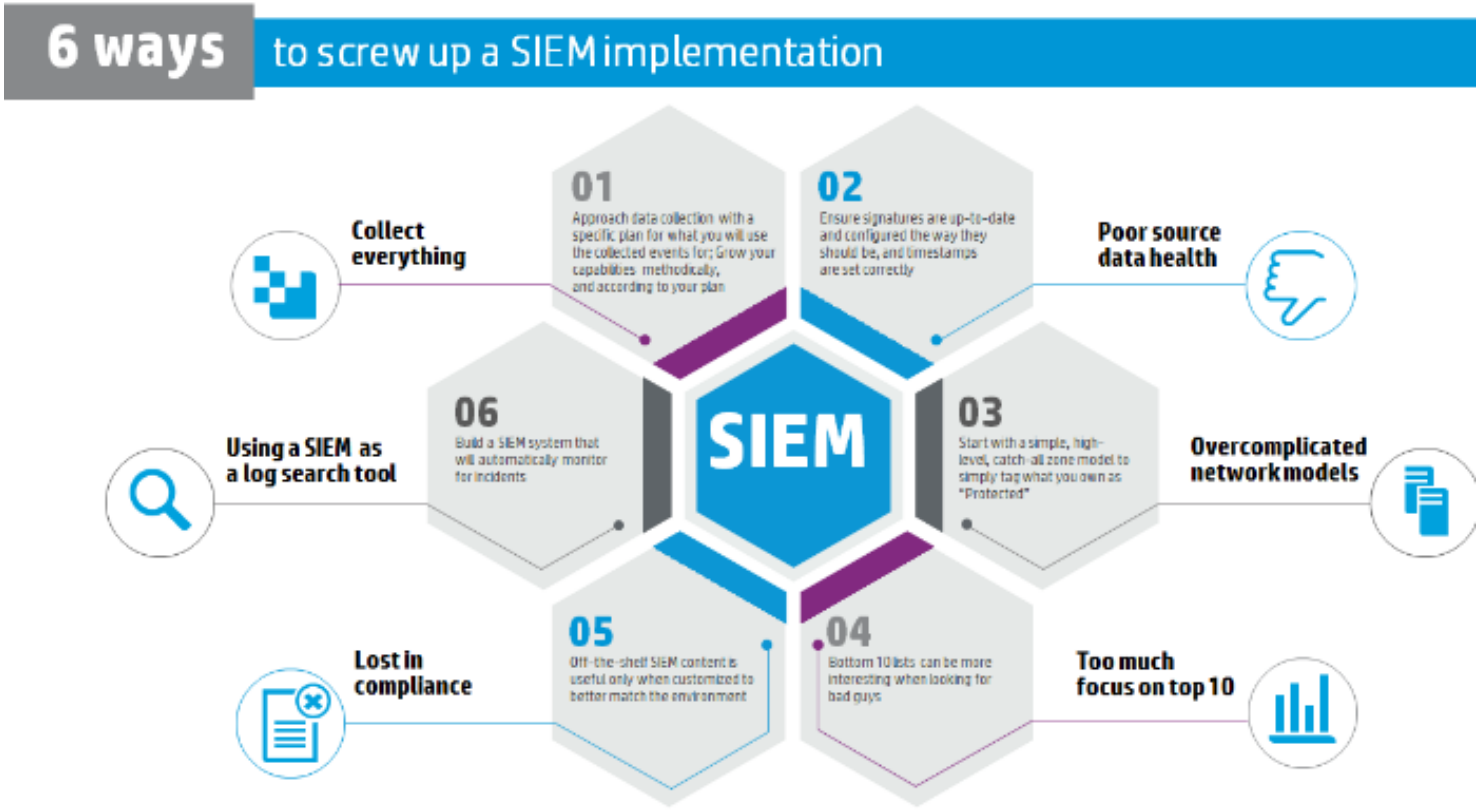
SIEM

- SIEM is implemented via software, systems, appliances, or some combination of these items. There are, generally speaking, six main attributes of an SIEM system:

- **Retention**: Storing data for long periods so that decisions can be made off of more complete data sets.
- **Dashboards**: Used to analyze (and visualize) data in an attempt to recognize patterns or target activity or data that does not fit into a normal pattern.
- **Correlation**: Sorts data into packets that are meaningful, similar and share common traits. The goal is to turn data into useful information.
- **Alerting**: When data is gathered or identified that trigger certain responses - such as alerts or potential security problems - SIEM tools can activate certain protocols to alert users, like notifications sent to the dashboard, an automated email or text message.
- **Data Aggregation**: Data can be gathered from any number of sites once SIEM is introduced, including servers, networks, databases, software and email systems. The aggregator also serves as a consolidating resource before data is sent to be correlated or retained.
- **Compliance**: Protocols in a SIEM can be established that automatically collect data necessary for compliance with company, organizational or government policies.

Schema alto livello

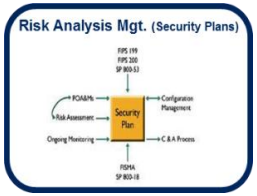
Errori comuni



Tipici Servizi gestiti dal SOC

Security Monitoring & Incident Handling

Operational Security Management



Technical Operational Processes

Technical Security Analysis

Security Infrastructures Management

Technical Infrastructure monitoring and maintenance Processes

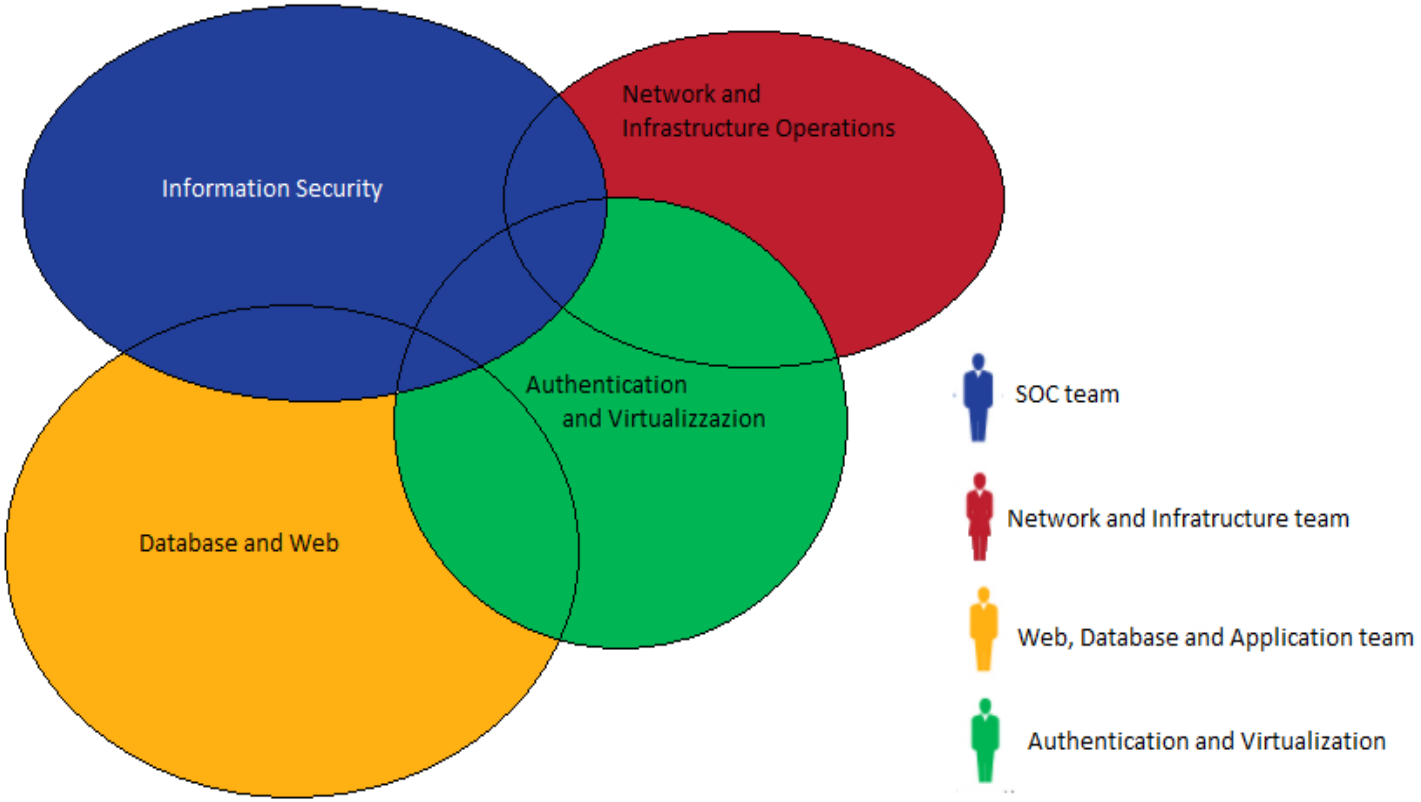
SOC's modular design enables adding/removing different services depending on organization requirements and InfoSec maturity

SOC Team Skills - General

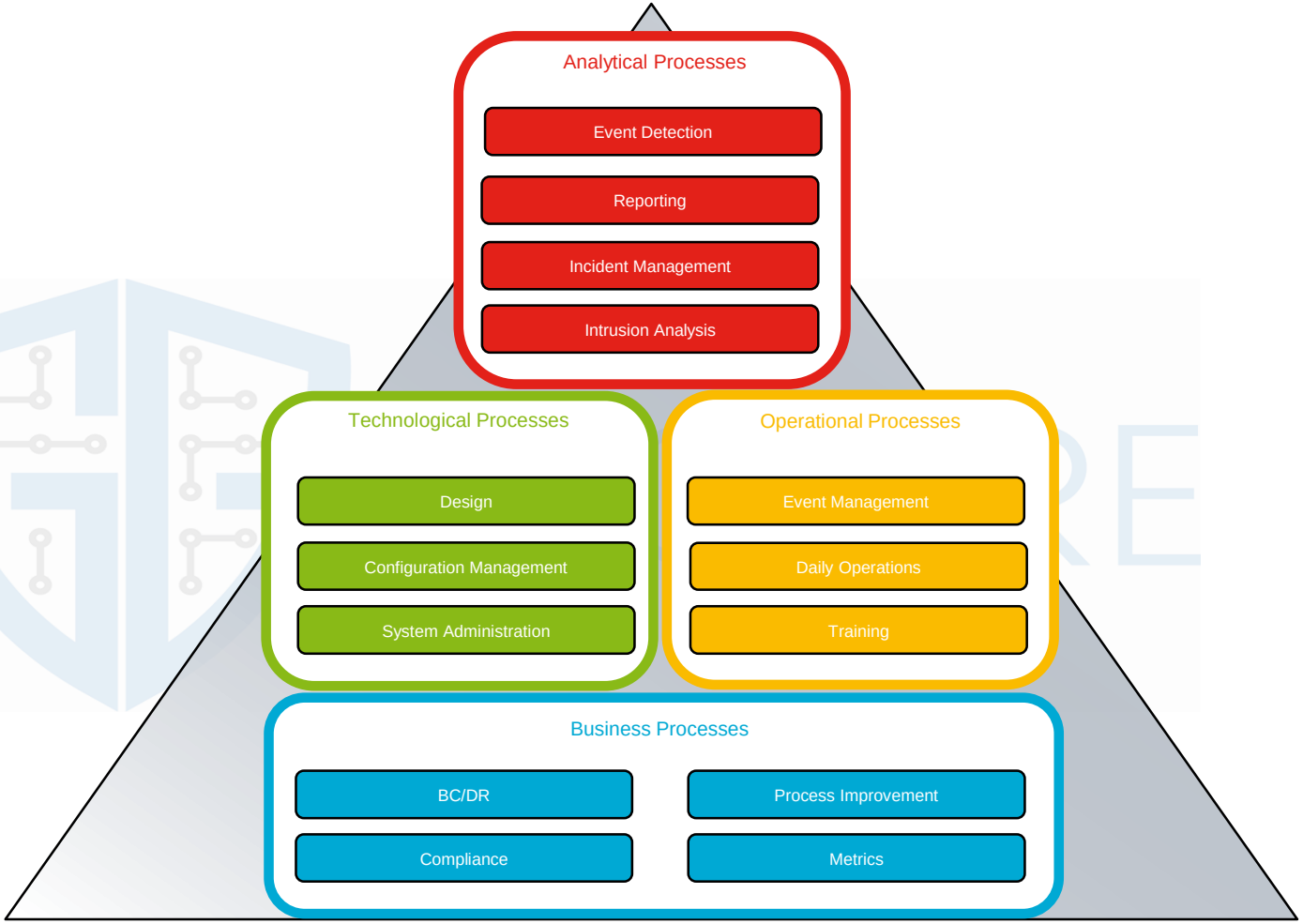
- Synthetically, the SOC team manages and prevents security issues and defines all security instructions/guidelines for IT teams and therefore requires a diverse and very high level of expertise grouped into 4 distinct areas of expertise.

- **The SOC general skill-set are:**
  - Security Skills
  - Network Skills
  - Infrastructure Skills
  - Governance & Compliance Skills

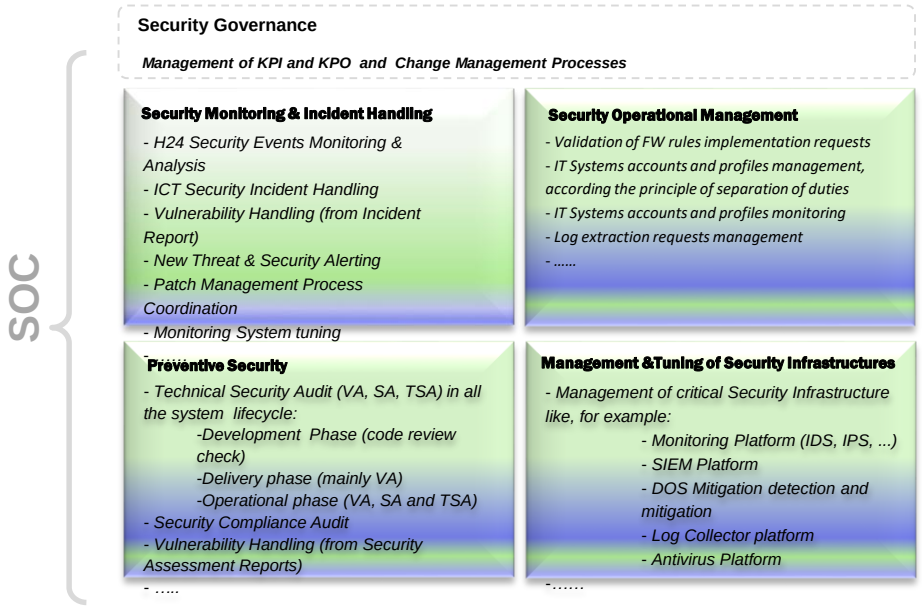
Teams Skills Map



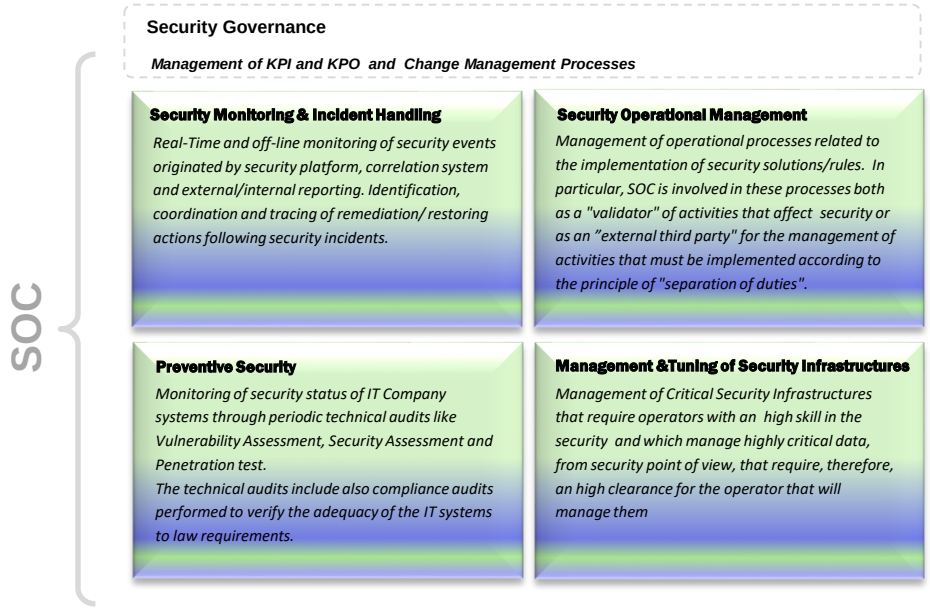
SOC - Processes



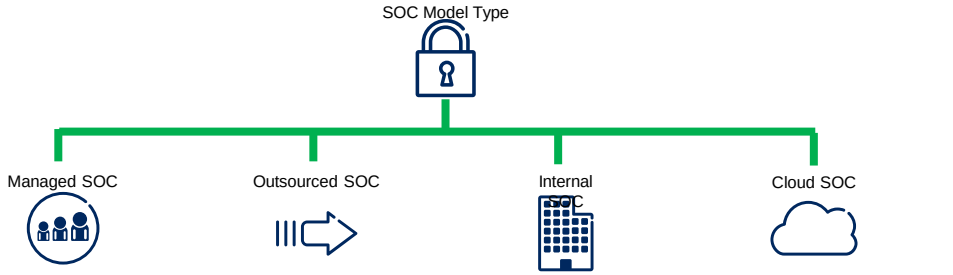
SOC - Activities/Processes Model



Organizational Functional Model



SOC Options: ragioniamo …



The SOC is located at Client's premises	The SOC is located at supplier premises	The SOC is located at Client's premises	The SOC is located on supplier's cloud
Client provides the tools and equipment (based on supplier's recommendations)	Supplier provides the standard SOC tools and equipment	Client provides the tools and equipment (based on supplier's recommendations)	The tools are cloud based. Equipment are part of supplier standard cloud
The skills are provided by supplier (possibly)	The skills are provided by the supplier	Client provides the skills that are trained by the supplier	The skills are provided by suppliers
The processes are collaboratively developed by Client and the supplier	The processes are collaboratively developed by Client and the supplier	The processes are collaboratively developed by Client and supplier	The processes are collaboratively developed by Client and supplier
The processes are managed by the supplier	The processes are produced/managed by supplier	Processes management is transferred to Client's SOC employees	The processes are managed by supplier

Thank you for the attention!