IT Systems Management
12 maggio 2019, 17:49

Indice

1 Executive Support **1**
2 Organizing for Systems Management **1**
2.1 Factors to Consider in Designing IT Organizations 1
3 Staffing for System Management **1**
4 Ethics, Legislation, and Outsourcing **2**
5 Customer Service **2**
6 Availability **2**
6.1 7-Rs of availability . . . 2
6.1.1 Redundancy . . . 2
6.1.2 Reputation . . . 2
6.1.3 Reliability . . . 2
6.1.4 Repairability . . . 2
6.1.5 Recoverability . . . 2
6.1.6 Responsiveness . . . 3
6.1.7 Robustness . . . 3
7 Performance and Tuning **3**
8 Production Acceptance **3**
9 Change Management **3**
9.1 Key Steps Required in Developing a Change Management Process . . . 3
9.2 Scope . . . 4
9.2.1 Tasks in the scope of CMP . . . 4
9.2.2 Tasks that aren't part of CMP . . . 4
9.3 Workflow Tasks . . . 4
9.4 Approvals Required for Change Based on Risk Level 4
9.5 Risk Level Based Lead Times . . . 4
9.6 Change Approval Phase . . . 5
9.7 Implementation and Documentation phase . . . 5
10 Problem Management **5**
10.1 Scope of Problem Management . . . 5
10.2 Key Steps to Developing a Problem Management Process . . . 5
11 Storage Management **5**
11.1 Storage Management Capacity . . . 5
11.2 Storage Management Performance . . . 5
11.3 Storage Management Reliability . . . 5
11.4 Storage Management Recoverability . . . 5
12 Network Management **5**
12.1 Key Decisions about Network Management . . . 5
12.2 Assessing an Infrastructure's Network Management Process . . . 6
12.3 Measuring and Streamlining the Network Management Process . . . 6
13 Configuration Management **6**
13.1 Pratical Tips for Improving Config. Man. . . . 6
13.2 Assessing an Infrastructure's Configuration Management Process . . . 6
13.3 Measuring and Streamlining the Configuration Management Process . . . 6
14 Cloud Services **6**
14.1 Characteristics of a Cloud . . . 6
14.2 Cloud Services . . . 6
15 Capacity Planning **6**
15.1 4 Key Elements . . . 6
15.2 Why Capacity Planning Is Seldom Done Well . . . 6
15.3 Steps to develop an effective capacity planning process . . . 7
15.4 Additional Benefits of Capacity Planning . . . 7
15.5 Helpful Hints for Effective Capacity Planning . . . 7
15.6 Uncovering the Hidden Costs of Upgrades . . . 7
15.7 Assessing an Infrastructure's Capacity Planning Process . . . 7
15.8 Measuring and Streamlining the Capacity Planning Process . . . 7
16 Strategic Security **7**
16.1 Developing a Strategic Security Process . . . 7
16.2 Measuring and Streamlining the Security Process 7
17 Business Continuity **7**
17.1 Steps to Developing an Effective Business Continuity Process . . . 7
18 Facilities Management **8**
18.1 Major Elements . . . 8
18.2 Facilities Management Process Owner . . . 8
18.3 Evaluating the Physical Environment . . . 8
18.4 Tips to Improve the Facilities Management Process 8
18.5 Facilities Management at Outsourcing Centers . . 8
18.6 Measuring and Streamlining the Facilities Management Process . . . 8
19 IT Monitoring **8**
19.1 80% Rule . . . 8
20 CoBIT Framework **8**
20.1 Governance Objective: the value creation . . . 9
20.2 Governance and Management in COBIT5 . . . 9
20.3 ISACA . . . 9
20.4 CoBIT 5: SIEM . . . 9
20.5 6 Ways to screw up a SIEM implementation . . . 9
21 SOC **9**
21.1 High Level View . . . 10
21.2 Cobit 5 vs Cobit 4.1 . . . 10
21.3 Typical Services handled by SOC . . . 10
21.4 SOC's Team Skills - General . . . 10
21.5 SOC Options . . . 10

1 Executive Support

Crucial for SysMan. Business metrics is a good argument for Ex. Supp., continuous support should be ensured.

2 Organizing for Systems Management

2.1 Factors to Consider in Designing IT Organizations

In the case of IT, restructuring is often necessary to support company growth, increased customer demand, changing business requirements, acquisitions, mergers, buyouts, or other industry changes. Three key factors by which infrastructures can be organized: departmental responsibilities, planning orientation, and systems management processes.

Org. Model Know Your Business (KYB), Locating Deparments in the Infrastructure, Identify Process Owners.

3 Staffing for System Management

Skilled professionals are needed at the outset to develop plans, design processes, and evaluate technologies; then they are needed to transform these ideas from paper into realities.

Skill Set defined as technical familiarity with a particular software product, architecture, or platform.

Skill Level defined as the length of experience and depth of technical expertise and variety of platform familiarity an individual has acquired and can apply to a given technology.

Importance of the right staff Determining required skill sets and skills levels, assessing skill levels of current onboard staff (alternative sources of staffing, recruiting infra. staff from the outside [operative/consultive]), selecting the *Most Qualified Candidate*, retaining *Key Personnel*, using *Consultants and Contractors* (benefits / drawbacks are involved, steps for developing career paths for staff memebers)

4 Ethics, Legislation, and Outsourcing

Personal Ethics Set values an individual uses to influence and guide his or her personal behavior.

Business Ethics Set values an individual uses to influence and guide his or her business behavior. Business ethics tend to focus on the behaviors of an individual as it pertains to his or her work environment. The differences between personal and business ethics may be at once both subtle and far-reaching.

NPI Stands for non-public information and pertains to the private, personal information of an individual not readily available in public records. Customers typically disclose such information to private or public companies to transact business. Examples of NPI are social security numbers, unlisted telephone numbers, and credit card account numbers.

5 Customer Service

IT evolved into a service organization.

- 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 4 key elements of Good Customer Service.

6 Availability

Availability Process of optimizing the readiness of production systems by accurately measuring, analyzing, and reducing outages to those production systems.
The ratio of the total time a functional unit is capable of being used during a given interval to the length of the interval.
Mean Time To Failure (MTTF), Mean Time To Repair (MTTR)

Responsiveness Operational responsiveness is a quality of a business process or supporting IT solution, which indicates its ability to respond to changing conditions and customer interactions as they occur.

Uptime measure of the time that individual components within a production system are functionally operating. This contrasts to availability, which focuses on the production system as a whole.

Slow Response refers to unacceptably long periods of time for an online transaction to complete processing and return results to the user. The period of time deemed unacceptable varies depending on the type of transaction involved. For simple inquiries, a one-second response may seem slow; for complex computations, two- or three-second responses may be acceptable. Slow response is usually a performance and tuning problem requiring highly-trained personnel with specialized expertise

Downtime Downtime refers to the total inoperability of a hardware device, a software routine, or some other critical component of a system that results in the outage of a production application.

High Availability refers to the design of a production environment such that all single points of failure are removed through redundancy to eliminate production outages. This type of environment is often referred to as being fault tolerant.

SMART **S**pecific, *Targets should be straightforward and emphasize what you want to happen*. **M**easurable, *If a target cannot be measured then you cannot determine whether it has been achieved*. **A**chievable, *It must be possible to achieve the target with an acceptable investment of time and resources*. **R**elevant, *Achieving the target must contribute to the overall business mission*. **T**imely, *The target must be something that can be achieved and measured over the reporting period of the SLA*[1].

6.1 7-Rs of availability

These seven Rs of high availability all contribute in a unique way to extending uptime, minimizing downtime, and improving the overall level of service provided by online systems.

6.1.1 Redundancy

Power Supply, Multiple processors, Segmented Memory, Redundant Disks

6.1.2 Reputation

The reputation of key suppliers of servers, disk storage systems, database management systems, and network hardware and software plays a principle role in striving for high availability. It is always best to go with the best. Reputations can be verified in several ways, including the following: Percent of market share, Reports from industry analysts such as Gartner Group, Publications such Wall Street Journal and ComputerWorld, Track record of reliability and repairability, Customer references

6.1.3 Reliability

The reliability of the hardware and software can also be verified from customer references and industry analysts. Beyond that, you should consider performing what we call an empirical component reliability analysis. The following list describes the seven steps required to accomplish this.

1. Review and analyze problem management logs.
2. Review and analyze supplier logs.
3. Acquire feedback from operations personnel.
4. Acquire feedback from support personnel.
5. Acquire feedback from supplier repair personnel.
6. Compare experiences with other shops.
7. Study reports from industry analysts.

6.1.4 Repairability

This refers to is the relative ease with which service technicians can resolve or replace failing components. A common metric used to evaluate this trait is the average or mean time to repair (MTTR). MTTR is sometimes interpreted as the mean time to recover, the mean time to restore, or the mean time to resolve. It measures the average time it takes to do the actual repair. $\text{MTTR} = \frac{\text{sum of repair times}}{\text{\# of failures}}$

6.1.5 Recoverability

This refers to the ability to overcome a momentary failure in such a way that there is no impact on end-user availability. It could be as small as a portion of main memory recovering from a single-bit memory error; it can be as large as having an entire server system switch over to its standby system with no loss of data or transactions. Recoverability also includes retries of attempted reads and writes out to disk or tape, as well as the retrying of transmissions down

[1] SLA is short for service level agreement and refers to a documented, negotiated agreement between a representative from an IT department and a representative from an end-user department concerning the quality of service delivered. Common SLA metrics include percent uptime availability, average response times, and escalation procedures for problems.

network lines.

6.1.6 Responsiveness

This trait is the sense of urgency all people involved with high availability need to exhibit. This includes having well-trained suppliers and in-house support personnel who can respond to problems quickly and efficiently. It also pertains to how quickly the automated recovery of resources such as disks or servers can be enacted. Escalation is another aspect of responsiveness that ensures higher levels of technical expertise and management support are involved to restore availability as quickly as possible. Escalation guidelines are usually documented in service-level agreements between IT and business customers.

6.1.7 Robustness

A robust process will be able to withstand a variety of forces—both internal and external—that could easily disrupt and undermine availability in a weaker environment. Robustness puts a high premium on documentation and training to withstand the following:

Technical Changes as they relate to Platforms, Products, Services, Customers

Personnel Changes as they relate to Turnover, Expansion, Rotation

Business changes as they relate to New direction, Acquisitions, Mergers
Defining a process to measure and monitor Infrastructure's Availability: Committed Hours of Availability (A), Outage hours (B), Achieved Availability: $\frac{A-B}{A} \cdot 100\%$.

7 Performance and Tuning

Methodology to maximize throughput and minimize response times of batch jobs, online transactions, and Internet activities. The five infrastructure areas most impacted by performance and tuning are:

- Servers
- Disk storage
- Databases
- Networks
- Desktop Computers

8 Production Acceptance

Methodology used to consistently and successfully deploy application systems into a production environment regardless of platform.

Consistent methodology While the methodology is consistent, it is not necessarily identical across all platforms. This means there are essential steps of the process that need to be done for every production deployment, and then there are other steps that can be added, omitted, or modified depending on the type of platform selected for production use.

Deploying into a production environment This implies that the process is not complete until all users are fully up and running on the new system. For large applications, this could involve thousands of users phased in over several months.

Application system This refers to any group of software programs necessary for conducting a company's business—the end-users of which are primarily, but not necessarily, in departments outside of IT. This excludes software still in development, as well as software used as tools for IT support groups.

Production Acceptance Process

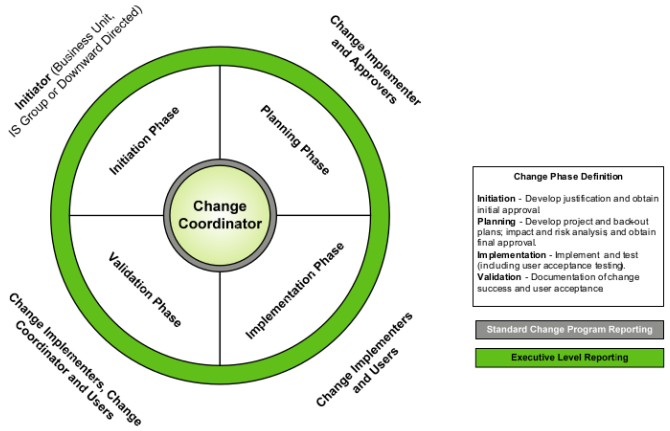
1. Identify an Executive Sponsor
2. Select a Process Owner
3. Solicit Executive Support
4. Assemble a Production Acceptance Team
5. Identify and Prioritize Requirements
6. Develop Policy Statements
7. Nominate a Pilot System
8. Design Appropriate Forms
9. Document updates, extension and new procedures
10. Run field tests and a solid pilot phase
11. Revise Policies, Procedures, and Forms
12. Define an adequate marketing strategy (if applicable)
13. Conduct a lessons-learned sessions
14. Follow-up with continuous improvements

Pay attention:

- Production Acceptance is not Change Management
- New Applications vs. New Versions of Existing Applications

9 Change Management

Change Management is the process to control and coordinate all changes to an IT production environment. Control involves requesting, prioritizing, and approving changes; coordination involves collaborating, scheduling, communicating, and implementing changes.
A change is defined as any modification that could impact the stability or responsiveness of an IT production environment.



9.1 Key Steps Required in Developing a Change Management Process

1. Identify an executive sponsor.
2. Assign a process owner.
3. Select a cross-functional process design team.
4. Arrange for meetings of the cross-functional process design team.
5. Establish roles and responsibilities for members supporting the design team.
6. Identify the benefits of a change management process.
7. If change metrics exist, collect and analyze them; if not, set up a process to do so.
8. Identify and prioritize requirements.
9. Develop definitions of key terms.
10. Design the initial change management process.
11. Develop policy statements.
12. Develop a charter for a Change Advisory Board (CAB).

13. Use the CAB to continually refine and improve the change management process.

9.2 Scope

Because the Change Management Process deals with the management of changes in the production environment, it is imperative that both customers and the company's change organization understand the events that are considered within the scope of the process. In this section, the scope is described and includes areas which are both within and outside of the change management process scope.

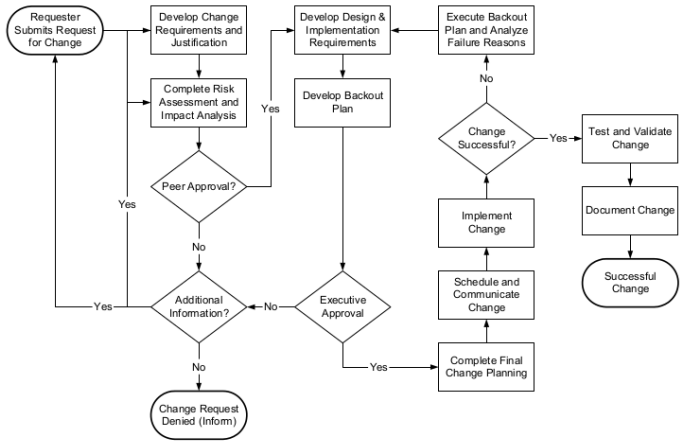
9.2.1 Tasks in the scope of CMP

- SDLC – Changes handled through the formal software development life cycle will be included within the company's change management program.
- 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.
- 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.
- Moves, Adds, Changes and Deletes – Changes to system configuration.
- Scheduled Changes - Requests for creation, deletion, or revision to job schedules, back-up schedules or other regularly scheduled jobs managed by the IT department.
- Telephony – Installation, modification, de-installation, or relocation of PBX/VOIP equipment and services.
- Desktop – Any modification or relocation of desktop equipment and services for users or classroom labs.
- Generic and Miscellaneous Changes – Any changes that are required to complete tasks associated with normal job requirements.

9.2.2 Tasks that aren't part of CMP

- Contingency/Disaster Recovery
- BCM related activities
- Changes to non-production elements or resources
- Changes made within the daily administrative process.
  - 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

9.3 Workflow Tasks



Basic Change Managment Workflow

9.4 Approvals Required for Change Based on Risk Level

Change Category	Risk Level	Priority			
		Emergency	Urgent	Routine	Low
Production Migration	No Risk	Assignment group	Assignment group	Assignment group	Assignment group
	No Risk	Mgr of Assignment group	Mgr of Assignment group	Mgr of Assignment group	Mgr of Assignment group

Change Category	Risk Level	Priority			
		Emergency	Urgent	Routine	Low
Hardware	High	Assignment group based on subcategory, Peer Review, CAB	Assignment group based on subcategory, Peer Review, CAB	Assignment group based on subcategory, Peer Review, CAB	Assignment group based on subcategory, Peer Review, CAB
	Moderate	Assignment group based on subcategory, Peer Review	Assignment group based on subcategory, Peer Review	Assignment group based on subcategory, Peer Review	Assignment group based on subcategory, Peer Review
	Low	Assignment group based on subcategory, Peer Review	Assignment group based on subcategory, Peer Review	Assignment group based on subcategory, Peer Review	Assignment group based on subcategory, Peer Review
	No Risk	Assignment group based on subcategory, Peer Review	Assignment group based on subcategory, Peer Review	Assignment group based on subcategory, Peer Review	Assignment group based on subcategory, Peer Review

Change Category	Risk Level	Priority			
		Emergency	Urgent	Routine	Low
Software	High	Assignment group based on subcategory, Peer Review, CAB	Assignment group based on subcategory, Peer Review, CAB	Assignment group based on subcategory, Peer Review, CAB	Assignment group based on subcategory, Peer Review, CAB

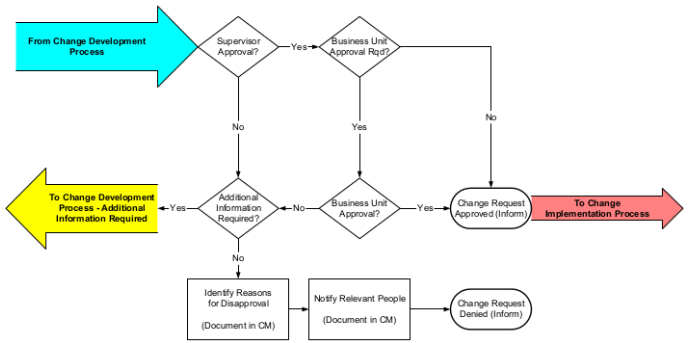
9.5 Risk Level Based Lead Times

It is essential that requests for change are submitted and approved in a timely manner. This will allow completion of accurate documentation, change processing and obtaining the approvals in sufficient time prior to the requested implementation date. Lead times are the number of days an action (Initiation or Approval) must be completed prior to the requested implementation date. The number of days will vary, depending on the priority and the risk level.

		Lead Time by Change Phase	
Priority	Risk Level	Initiation	Approval
Emergency	High	3	3
	Moderate	2	2
	Low	1	1
	No Risk	1	1
Urgent	High	6	3
	Moderate	4	2
	Low	2	1
	No Risk	1	1
Routine	High	20	10
	Moderate	15	7
	Low	10	5
	No Risk	5	3
Low	High	25	15
	Moderate	20	10
	Low	15	7
	No Risk	10	5

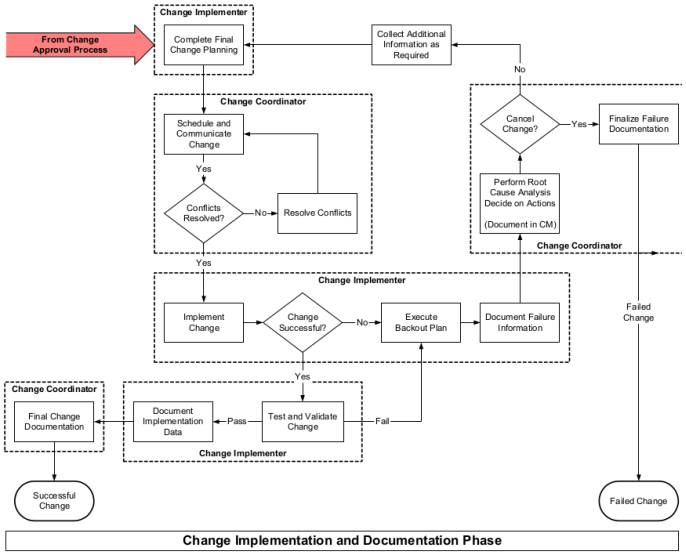
9.6 Change Approval Phase

After a minor, major or significant change has been correctly prioritized, categorized, and analyzed by the Change Coordinator and been through the Peer Review process, the change must be authorized for implementation. The diagram below identifies the workflow associated with change management approval at the company:



Change Approval Phase

9.7 Implementation and Documentation phase



Change Implementation and Documentation Phase

10 Problem Management

Problem management is a process used to identify, log, track, resolve, and analyze problems impacting IT services.

10.1 Scope of Problem Management

Many infrastructures do agree that first-level problem handling, commonly referred to as tier 1, is the minimum basis for problem management.

10.2 Key Steps to Developing a Problem Management Process

1. Select an executive sponsor.
2. Assign a process owner.
3. Assemble a cross-functional team.
4. Identify and prioritize requirements.
5. Establish a priority and escalation scheme.
6. Identify alternative call-tracking tools.
7. Negotiate service levels.
8. Develop service and process metrics.
9. Design the call-handling process.
10. Evaluate, select, and implement the call-tracking tool.
11. Review metrics to continually improve the process.

11 Storage Management

Storage management is a process used to optimize the use of storage devices and to protect the integrity of data for any media on which it resides.

11.1 Storage Management Capacity

Storage management capacity consists of providing sufficient data storage to authorized users at a reasonable cost.

11.2 Storage Management Performance

The first performance consideration is the size and type of main memory.

11.3 Storage Management Reliability

Fault tolerance w/ RAID Systems

RAID Level	Explanation
0	Disk striping for performance
1	Mirroring for total redundancy
0 + 1	Combination of striping and mirroring
3	Striping and fault tolerance with parity on totally dedicated parity drives
5	Striping and fault tolerance with parity on nonassociated data drives

11.4 Storage Management Recoverability

several methods available for recovering data that has been altered, deleted, damaged, or otherwise made inaccessible. Determining the correct recovery technique depends on the manner in which the data was backed up.

12 Network Management

Process to maximize the reliability and utilization of network components in order to optimize network availability and responsiveness.

12.1 Key Decisions about Network Management

1. What will be managed by this process?
2. Who will manage it?
3. How much authority will this person be given?
4. What types of tools and support will be provided?
5. To what extent will other processes be integrated with this process?
6. What levels of service and quality will be expected?

12.2 Assessing an Infrastructure's Network Management Process

12.3 Measuring and Streamlining the Network Management Process

We can measure the effectiveness of a network management process with service metrics such as network availability, network response times, and elapsed time to logon.

13 Configuration Management

Process to ensure that the interrelationships of varying versions of infrastructure hardware and software are documented accurately and efficiently.

Configuration management refers to coordinating and documenting the different levels of hardware, firmware, and software that comprise mainframes, servers, desktops, databases, and various network devices such as routers, hubs, and switches. It does not refer to application software systems or to the verification of various levels of application software in different stages of development, testing, and deployment—these activities are commonly referred to as versioning control and are normally managed by the applications development group or by a software quality assurance group within applications development.

13.1 Pratical Tips for Improving Config. Man.

1. Select a qualified process owner.
2. Acquire the assistance of a technical writer or a documentation 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.

13.2 Assessing an Infrastructure's Configuration Management Process

13.3 Measuring and Streamlining the Configuration Management Process

We can measure the effectiveness of a configuration management process with service metrics such as the number of times analysts, auditors, or repair technicians find out-of-date configuration documentation. Process metrics, such as the elapsed time between altering the physical or logical configuration and noting it on configuration diagrams, help us gauge the efficiency of this process. And we can streamline the configuration management process by automating certain actions—the updating of multiple pieces of documentation requiring the same update, for example.

14 Cloud Services

14.1 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.

14.2 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.

15 Capacity Planning

As its name implies, the systems management discipline of capacity planning involves the planning of various kinds of resource capacities for an infrastructure.
Capacity planning is a process to predict the types, quantities, and timing of critical resource capacities that are needed within an infrastructure to meet accurately forecasted workloads.

15.1 4 Key Elements

1. The type of resource capacities required, such as servers, disk space, or bandwidth
2. The size or quantities of the resource in question
3. The exact timing of when the additional capacity is needed
4. Decisions about capacity that are based on sound, thorough forecasts of anticipated workload demands

15.2 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

15.3 Steps to develop an effective capacity planning process

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

15.4 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

15.5 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

15.6 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

15.7 Assessing an Infrastructure's Capacity Planning Process

15.8 Measuring and Streamlining the Capacity Planning Process

We can measure the effectiveness of a capacity planning process with service metrics such as the number of instances of poor response due to inadequate capacity on servers, disk devices, or the network. Process metrics—such as the number of instances of poor response due to inadequate capacity on servers, disk devices, or the network—help us gauge the efficiency of this process. We can be streamline the capacity planning process by automating certain actions—the notification to analysts when utilization thresholds are exceeded, the submittal of user forecasts, and the conversion of user-workload forecasts into capacity requirements, for example.

16 Strategic Security

Strategic security is designed to safeguard the availability, integrity, and confidentiality of designated data and programs against unauthorized access, modification, or destruction.

16.1 Developing a Strategic Security Process

1. Identify an executive sponsor.
2. Select a process owner.
3. Define goals of strategic security.
4. Establish review boards.
5. Identify, categorize, and prioritize requirements.
6. Inventory current state of security.
7. Establish security organization.
8. Develop security policies.
9. Assemble planning teams.
10. Review and approve plans.
11. Evaluate technical feasibility of plans.
12. Assign and schedule the implementation of plans.

16.2 Measuring and Streamlining the Security Process

We can measure the effectiveness of a security process with service metrics such as the number of outages caused by security breaches and the amount of data altered, damaged, or deleted due to security violations. Process metrics, such as the number of password resets requested and granted and the number of multiple sign-ons processed over time, help us gauge the efficiency of this process. Finally, we can streamline the security process by automating certain actions—for example, the analysis of password resets, network violations, or virus protection invocations.

17 Business Continuity

Business continuity is a methodology to ensure the continuous operation of critical business systems in the event of widespread or localized disasters to an infrastructure environment.

17.1 Steps to Developing an Effective Business Continuity Process

1. Acquire executive support.
2. Select a process owner.
3. Assemble a cross-functional team.
4. Conduct a business impact analysis.
5. Identify and prioritize requirements.
6. Assess possible business continuity recovery strategies.
7. Develop a request for proposal (RFP) for outside services.

8. Evaluate proposals and select the best offering.
9. Choose participants and clarify their roles on the recovery team.
10. Document the business continuity plan.
11. Plan and execute regularly scheduled tests of the plan.
12. Conduct a lessons-learned postmortem after each test.
13. Continually maintain, update, and improve the plan.

18 Facilities Management

Facilities management is a process to ensure that an appropriate physical environment is consistently supplied to enable the continuous operation of all critical infrastructure equipment.

18.1 Major Elements

UPS uninterruptible power supply and is a temporary battery backup in the event of commercial power loss. UPS units are normally used to power data centers for 15-20 minutes until such time that commercial power is restored or until longer term backup generators come online. Portable UPS units are now available for servers, workstations and desktops outside of a data center.

18.2 Facilities Management Process Owner

- Determining the Scope of Responsibilities of a Facilities Management Process Owner
- Desired Traits of a Facilities Management Process Owner

The owner of the facilities management process almost always resides in the computer operations department.

18.3 Evaluating the Physical Environment

- Major Physical Exposures Common to a Data Center
- Keeping Physical Layouts Efficient and Effective

If the problem-management system includes a robust database, it should be easy to analyze trouble tickets caused by facilities issues and highlight trends, repeat incidents, and root causes.

18.4 Tips to Improve the Facilities Management Process

1. Nurture relationships with facilities department.
2. Establish relationships with local government inspecting agencies, especially if you are considering major physical upgrades to the data center.
3. Consider using video cameras to enhance physical security.
4. Analyze environmental monitoring reports to identify trends, patterns, and relationships.
5. Design adequate cooling for hot spots due to concentrated equipment.
6. Check on effectiveness of water and fire detection and suppression systems.
7. Remove all tripping hazards in the computer center.
8. Check on earthquake preparedness of data center (devices anchored down, training of personnel, and tie-in to disaster recovery).

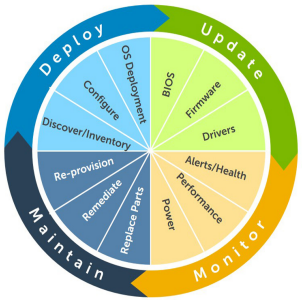
18.5 Facilities Management at Outsourcing Centers

Shops that outsource portions of their infrastructure services—co-location of servers is an example—often feel that the responsibility for the facilities management process is also outsourced and no longer of their concern. While outsourcers have direct responsibilities for providing stable physical environments, the client has an indirect responsibility to ensure this will occur. During the evaluation of bids and in contract negotiations, appropriate infrastructure personnel should ask the same types of questions about the outsourcer's physical environment that they would ask if it were their own computer center.

18.6 Measuring and Streamlining the Facilities Management Process

We can measure the effectiveness of a facilities management process with service metrics such as the number of outages due to facilities management issues and the number of employee safety issues measured over time. Process metrics—for example, the frequency of preventative maintenance and inspections of air conditioning, smoke detection, and fire suppression systems and the testing of uninterruptible power supplies and backup generators—help us gauge the efficiency of this process. And we can streamline the facilities management process by automating actions such as notifying facilities personnel when environmental monitoring thresholds are exceeded for air conditioning, smoke detection, and fire suppression.

19 IT Monitoring



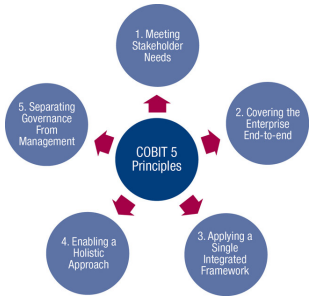
Monitoring Priorities for Systems Management

- 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

19.1 80% Rule

When servers regularly exceed about 80% of their capacity – in terms of CPU utilization, memory performance, and storage availability – they should be upgraded or replaced.

20 CoBIT Framework



The COBIT 5 framework defines 7 categories of enablers:

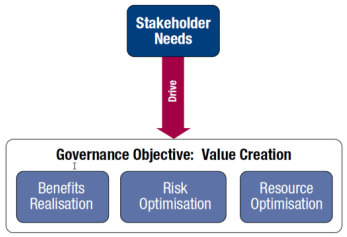
- Principles, Policies and Frameworks
- Processes
- Organisational Structures
- Culture, Ethics and Behaviour

- Information
- Services, Infrastructure and Applications
- People, Skills and Competencies

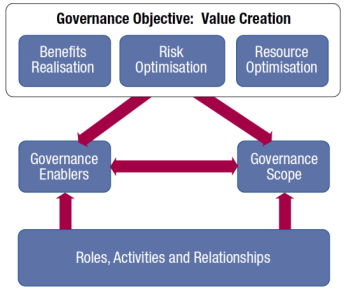
The COBIT 5 framework makes a clear distinction between governance and management. These two disciplines encompass different types of activities, require different organisational structures and serve different purposes. COBIT 5's view on this key distinction between governance and management is:

- 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).

20.1 Governance Objective: the value creation



20.2 Governance and Management in COBIT5



20.3 ISACA

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

20.4 CoBIT 5: SIEM

Security information and event management (SIEM), it is a solution enterprise security professionals both insight into and a track record of the activities within their IT environment. It provides 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.

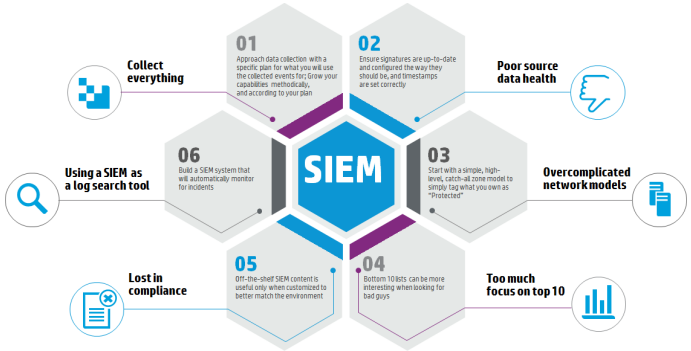
SIEM software identifies and categorizes incidents and events, as well as analyzes them.
SIEM has 2 main objectives:

- 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 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.

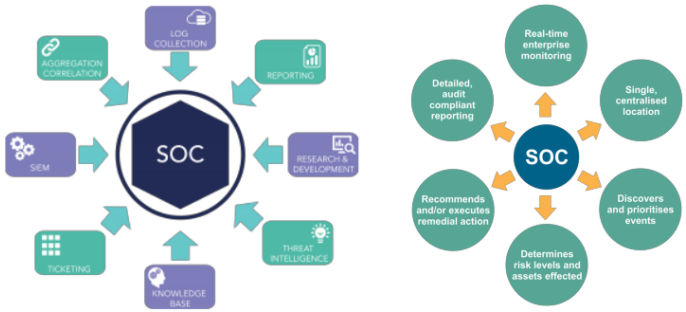
20.5 6 Ways to screw up a SIEM implementation



21 SOC

An information security operations center (”ISOC” or ”SOC”) is a facility where enterprise information systems (web sites, applications, databases, data centers and servers, networks, desktops and other endpoints) are monitored, assessed, and defended.

21.1 High Level View



21.2 Cobit 5 vs Cobit 4.1

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		■				■			

21.3 Typical Services handled by SOC

- Security Monitoring & Incident Handling
  - Security Incident Handling
  - New Threats Management
- Operational Security Management
  - Risk Analysisy Management (Security Plans)
  - Remediation Plans
  - Operational Security
- Technical Security Analysis
  - Vulnerability Assessment
  - Security Baseline Compliance Assessment
  - Forensics Analysis Services
- Security Infrastructures Management
  - Operational Security

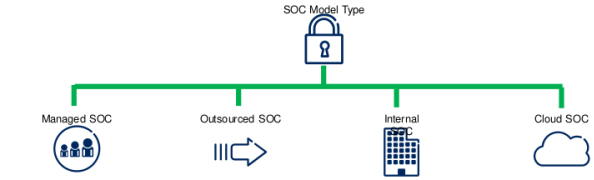
SOC's modular design enables adding/removing different services depending on organization requirements and InfoSec maturity.

21.4 SOC's 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

21.5 SOC Options



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