Cloud Computing

Cloud Security and Governance

Matt Stamper, VP of Managed Services
MPIA, MS, CISA, ITIL Foundation
Cloud - Evolution or Revolution?

Cloud computing can be thought of as either the logical extension of previous IT technology architectures or as a new set technologies that fundamentally reshape IT as we know it.

Evolution of Traditional IT
- Mainframe (centralized resources, remote access)
- Client Server (Ethernet & TCP/IP dominate)
- Web-centric applications (ASPs, shared hosting, colocation facilities)

Reshaping IT as we know it...
- Orchestration / Pay-as-you-go
- Consumerization of IT
- New business models
- CAPEX to OPEX
Cloud Catalysts

Cloud services leverage critical underlying technologies that have spurred rapid adoption of cloud services including:

- Enhanced chip sets that support multi-core / multi-threading technologies
- Server Virtualization
- Standards & Common Protocols (Ethernet & TCP/IP)
- Dramatic reduction in hardware costs (think China and manufacturing)
- Economics / recession (CAPEX to OPEX)
- Economies of Scale & Economies of Competencies
- Dense Wave Division Multiplexing (DWDM)
- Efficient Resource Allocation (think just-in-time IT😊)
Cloud Defined

Visual Model Of NIST Working Definition Of Cloud Computing
http://www.csrc.nist.gov/groups/SNS/cloud-computing/index.html

Essential Characteristics

Service Models

Deployment Models
Cloud Characteristics

As the NIST definition notes, cloud computing is characterized by the following characteristics:

- **Resource Pooling** – Storage, Network, Compute, Backups
- **Elasticity** – Scale up / scale down per the needs of the business
- **Measured Service** – Pay-as-you-go for what you use
- **Broadband Network Access** – Ubiquitous IP access
- **On-Demand / Self Service**

*This characteristic, as we will discuss, has important implications for governance.
There are risks, aka threat vectors, for each layer of IT, whether these are in the cloud or in traditional IT environments. Knowing the exposure for each layer is a key first step in developing a security approach that will mitigate (though never truly eliminate) security issues.

Here are the key layers to consider:

- Application (SaaS/IaaS)
- Database (SaaS/PaaS/IaaS)
- Operating System (PaaS/IaaS)
- Virtualization (SaaS/PaaS/IaaS)
- Server (Physical Hosts) (IaaS)
- Storage (PaaS/IaaS)
- Backups (SaaS/PaaS/IaaS)
- Network (SaaS/PaaS/IaaS)
- Data Center (SaaS/PaaS/IaaS)
There are important linkages between the service delivery model provided by the cloud service provider and where the user organization’s roles and responsibilities overlap. These should be well-understood and documented.
Know the Service Mix!

There is huge amount of variance between the services that are provided for each delivery model. It’s critical to know which services are in scope and how those services are provided. Detail counts!

- Know which services are being used and how they are managed:
  - Security and Monitoring
  - Application(s)
  - OS Administration
  - Servers, Storage, and Backups
  - Network
  - Data Center

- Map controls & requirements to each layer

- Validate if SSAE16 Audits provide assurance that the controls are effective in both design and operation. It’s important to carefully review the audit.
Cloud Services Rely on Data Centers

Cloud services are delivered from data centers (colocation facilities, hosting providers, central offices, etc.). Clouds services should be transparent and should be assessed for the following key controls:

**Physical Access Controls**
- Access Procedures
- Physical Security
- Capacity Management

**Staffing Controls**
- Background checks
- Staffing Levels & Competencies

**Facility Management Controls**
- Power Management
- Cooling Management
- Network Management
- Fire Suppression
Cloud Services Also Rely On IT Service Management

Key ITIL Service Management Domains that impact cloud services include the following:

- Information Security Management
- Service Level Management
- Availability Management
- Capacity Management
- Configuration Management
- Release & Deployment Management
- Change Management
- Incident Management

It’s always recommended to investigate how services are being delivered and which service management frameworks are in use.
Let’s Put the “Cloud” in a Business Context

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Balance Sheet</td>
<td>Income Statement</td>
<td>Cash Flow</td>
<td>Notes</td>
<td>Disclosures</td>
<td>AP</td>
<td>AR</td>
</tr>
<tr>
<td>Risk Management</td>
<td>Operating System</td>
<td>Database</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operations Management</td>
<td>Servers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Management</td>
<td>Storage / Backups</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Availability Management</td>
<td>Network</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Management</td>
<td>Data Center</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configuration Management</td>
<td>Data Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incident Management</td>
<td>Security Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Infrastructure Management</td>
<td>Change Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Segregation of Duties</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Configuration Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Security - Defined

The easiest way to think about security is to think about the outcome of what good security provides: **confidentiality, integrity, and availability** of information (CIA).

**Confidentiality** is the end-state of ensuring that information is only viewed and acted upon by those individuals, organizations, or systems that are authorized to see such information. “A loss of confidentiality is the unauthorized disclosure of information” – FIPS 199.

**Integrity** is the end-state of information and its processing such that the information is believed to be complete, accurate, valid and subject to restricted access (CAVR)...essentially un tampered with or otherwise modified by unauthorized activity. “A loss of integrity is the unauthorized modification or destruction of information” – FIPS 199.

**Availability** is simply that...that the information is available for its required use without delay or loss. “A loss of availability is the disruption of access to or use of information or an information system” – FIPS 199.

Collectively, IT security is the set of processes that are involved with ensuring that data and information meet the confidentiality, integrity, and availability objectives of business.
Security in the Cloud

While some organizations are concerned about security in the cloud, there are many ways that cloud service providers can enhance a company’s security environment including:

✓ Physical Access Controls to data centers
✓ Reduced Access to Infrastructure (Servers, Network, Storage, Backups, etc.)
✓ Economies of process, people and infrastructure
✓ Enhanced technologies to mitigate advanced threats
✓ Standardized hardening of key system components

The bottom line is that good security practices are required in the cloud as well as on-premise. The availability of security tools and procedures may be enhanced with cloud services providers depending upon their service mix.
Cloud Layers - Orchestration Risk

The orchestration layer, given its linkages to the provisioning of system resources, metering activities, etc. is a high-value target. Orchestration layer software is also home to some of the newest code in the cloud and likely has hidden, as of yet unexposed, security issues like all software.

Orchestration Layer - Typical Risks
✓ Poor coding / complexity / linkages to underlying resources
✓ System lock-out / resource hijacking
✓ Malicious insider / elevated privileges
✓ Vendor lock-in
✓ Economic Risks (think old PBX attacks)
✓ Other considerations?
Cloud Layers - Hypervisor Risk

The hypervisor, aka a virtual machine manager (VMM), comes in two flavors: type 1 (bare metal) and type 2 (installed on top of an OS). Type 2 VMMs are inherently more risky given their dependencies upon an underlying OS.

Hypervisor- Typical Risks
✓ Rootkits that provide a hijacked or compromised OS
✓ Guest DOS attacks / system hijacking
✓ Similar issues with orchestration
✓ Other considerations?
The hypervisor and any tools used to manage services require special security attention.

- What security controls are in place to protect the hypervisor from being compromised?
- How often are these controls tested and validated?
- Who has access to the management tools used to administer the hypervisor? Are their access rights commensurate to their role with the CSP?
- How often are these access rights reviewed?
- How does our CSP mitigate the risks of internal VM-to-VM attacks?
- What security measures are in place to prevent guest-to-host attacks?
- How is resource isolation managed?
- What precludes my organization’s resources from being used by a neighboring customer?
Cloud Layers - Application Risk

Applications probably offer the widest array of risks to organizations. One of the key reasons...think about who uses applications...it’s us.

Applications - Typical Risks
✓ Human error / social networking exposure / APT attacks
✓ Segregation of duties / elevated privileges
✓ Database linkages / poor data validation
✓ Session-hacking, man-in-the-middle attacks, cross-site scripting
✓ Poor application coding
✓ Poor passwords (complexity/aging)
✓ Poor logging habits
✓ Many firewalls are not application aware (just ports 80, 443)
✓ Other considerations?
Cloud Layers - Database Risk

Databases represent the crown jewels for most organizations because they contain sensitive information (employee records, pricing schedules, IP, PCI data, health records, etc.). Databases, as a consequence, are a frequent target.

Database - Typical Risks
✓ Ill-defined linkages with applications and the web (segmentation)
✓ Promiscuous trust relationships
✓ SQL Injection / input validation
✓ Poor database management (logging, patching, access, etc.)
✓ Backup procedures (non-encrypted backups / off-site vaulting)
✓ Other considerations?
Security - Patch / Kernel

Depending upon the CSP, there may be important variances around patch management and system hardening.

✓ What are the processes to harden the environment?
✓ Are these processes ubiquitously applied?
✓ What are the procedures to harden operating systems?
✓ What if exceptions are required?
✓ Do my applications have kernel-level dependencies that could be impacted by system-wide changes?
Cloud Layers - OS Risk

Operating Systems, especially in Windows environments, are extraordinarily complex and the code typically requires frequent updates (aka patching) to address security fixes or performance issues.

Operating Systems - Typical Risks
✓ Poor patch management practices
✓ Domain / user management
✓ Generic & anonymous accounts
✓ Unnecessary services still enabled
✓ Default settings / permissions (file systems, registries, etc.)
✓ Log settings / sizing (security, system, application)
✓ Other considerations?
Physical servers do not face as many security risks as other layers within cloud computing but there are factors to consider.

Server Center - Typical Risks
✓ Remote management tools (DRAC, ILO)
✓ Poor configuration
✓ Physical access / social engineering / USBs
✓ System Failure (non-malicious DOS)
✓ Other considerations?
Cloud Layers - Network Risk

Despite numerous breaches and social engineering attacks that exploit other layers, IT security efforts have historically focused on the network layer. The analogy is to have dead-bolted the front door while leaving the garage, backdoor, and windows (no pun) opened.

Network - Typical Risks
✓ Port 80 (Web)
✓ Port 443 (SSL)
✓ Limited application awareness with traditional firewalls
✓ DDoS attacks (network saturation)
✓ IP address blacklisting
✓ IP address spoofing
✓ Other considerations?
Cloud Security - Defense in Depth

As we reviewed, security vulnerabilities can be found at numerous layers within an environment. As a consequence, it’s important to have a broad context to security.

Key areas of concentration should include:
✓ Elevated privileges, system administration roles / SOD
✓ Data management / classification
✓ Social network / social engineering attacks
✓ Physical access
✓ Basic *housekeeping* (logging, patch management)
✓ Shared-resource management
Cloud Security - What’s different

Given that cloud computing represents a logical extension of previous IT advancements, what else should we be aware of?

How is security in the cloud different?

✓ Multi-tenancy (servers, storage, backups, network)
✓ Abstraction of many components (the complexity did not go away)
✓ Obfuscation of infrastructure / location of data
✓ 3rd-party service management / availability of information (e.g. logs)
✓ Massive scale and resources to leverage
✓ Chain-of-custody
✓ Other considerations?
Cloud Security - CSPs as Targets

Large, well-known public clouds are the hackers dream come true.

✓ What type of target does my CSP present to the hacking community?
✓ Has my CSP been hacked before?
✓ How often is my provider the target of DDoS attacks?
✓ How effectively are these mitigated?
✓ Are there prominent targets (e.g. other clients) receiving similar services from my CSP? How well do you know your neighbors?
✓ Has my CSP’s IP space been black-listed?
Security - CSP Management

Using a CSP to support IT infrastructure does not eliminate the requirement to ensure controls are effective in design and operation.

✓ What policies and procedures does the CSP employ?
✓ Are these policies and procedures appropriate for my organization’s requirements and risk-mitigation strategies?
✓ Which controls have been outsourced to the cloud provider?
✓ How will these controls be assessed and how frequently?
A cornerstone to developing a control environment to mitigate security risks is to have data appropriately classified.

- Will the CSP provide services that transmit, process, or store personally-identifiable information (PII) or personal-health information (PHI)?
- Will the CSP provide services that contain or store credit card information? Cardholder data includes:
  - Primary account number
  - Expiration date
  - Name on the card
  - CCV / CVV2
  - Magnetic strip
- Will human resource / employment records be part of the data used in the cloud?
Security - Data Location

Where data physically resides is important given certain regulatory requirements and jurisdictional nuances to data management.

**Data-in-Motion (DIM)**

- How is data protected as it migrates to/from the cloud?
- How is data protected within the cloud as it migrates between virtual machines and shared storage arrays?

**Data-at-Rest (DAR)**

- How is data protected in cloud-storage environments?
- What levels of encryption are being employed?
- Who is managing the encryption keys?
- Is data encrypted when it is backed up to tape or other media?
Security - Data Migration

There is a challenging relationship with cloud services: they are generally easy to deploy to but challenging to migrate away from.

✓ How can you migrate sensitive data from one provider to another?
✓ What controls are in place to ensure security over data-in-motion?
✓ Does my provider have documented procedures/APIs in place to facilitate the migration of data/business logic out of its services?
Access, Authentication, and Authorization: Access management, coupled with data classification, is the foundation for good security practices.

- What are the access procedures employed within the organization?
- How are these procedures impacted by migrating services and data to the cloud?
- Do my CSP’s access procedures map to our internal requirements? If not, what are the mitigating controls?
- Is strong authentication being employed between the various components in the environment? Are security domains employed and how are they being used?
- Who has elevated privileges in the cloud environment? Are there any system-wide accounts? If so, who has these accounts? How were there privileges established?
- What type of background checks are performed on those individuals employed by the service provider?
- How does the provider procure access credentials? Are multiple-factors of authentication employed?
Security - Audits & Certifications

Public clouds, by definition, involve services provided by third parties. This necessitates audits of the CSP’s controls, procedures, and operations.

✓ What audits has our CSP completed?
✓ What certifications has our CSP achieve?
✓ How meaningful are these audits and certifications to my organization’s control requirements?
✓ Have the service provider’s controls been mapped to our internal controls? Are there gaps that need to be filled by mitigating controls?
✓ How willing is my provider to disclose the status of their audits (e.g. exceptions, scope, etc.) and the extent of their certifications?
Security - Personnel & Staffing

Organizations that leverage CSPs to support their IT infrastructure have effectively “outsourced” certain functions but have not delegated ultimate responsibility.

- What assurances are in place that the CSP’s staff are adequately trained?
- What assurances are in place that there are adequate segregation of duties between provider’s staff?
- Have adequate background checks been performed?
- Does my organization have the ability to know who is working on my organization’s infrastructure?
- Do personnel from my organization’s provider have access to our environment? If so, is this monitored and logged?
- How many personnel have been dismissed within the last year? For cause?
Security - Vulnerability Scans

For a variety of reasons, many CSPs do not allow scanning of their infrastructure. This can create challenges for CSP clients subject to regulations and standards such as PCI-DSS.

✓ Does my CSP allow scanning? If so, how are these scans scheduled? Do we need to notify the provider of the scan? Will this change behavior?

✓ Will my organization be subject to shutdown if we affect a scan without notifying the provider?

✓ What about internal scans?

✓ What happens if my “neighbor” conducts scans that impact my operations?
Log management and event correlation are quickly becoming key tools to help mitigate risk and understand security exposures.

- What information is logged by the provider?
- How can logs be obtained in a multi-tenant environment?
- How can logs be disaggregated to our organization only?
- How can an effective chain of custody be established over important system logs?
- What controls are in place to ensure that logs are unaltered?
- What is the standard retention period for logs? What happens if a distinct period is required?
- What if we require logs that the cloud services provider will not provide?
Security - Resource Scaling

The Hidden DOS: One of the notable benefits of cloud computing is the ability to rapidly scale services and infrastructure to reflect the needs of the business.

- What happens if resources are unavailable?
- What happens if my CSP has not managed its capacity planning correctly and there are degradations in service?
- Do my organization’s workloads map well to cloud-type services?
- Latency/distance issues
- Processing/storage latency
- Client-side/browser latency
- How would spikes from other clients impact the responsiveness/performance of my organization’s infrastructure?
- Is my organization at risk from a friendly DOS attack?
- Is there a policy on resource capping?
Security - CSP Dependencies

There are important differences from one provider to another. These differences cover numerous risk considerations.

- Does my CSP rely upon any specific technology or vendor that may impact our service?
- Are these dependencies disclosed?
- Are the risks around these dependencies fully-captured?
- Are there work-around procedures in the event of a technology failure?
- How standardized are the APIs used to interact and work with the CSP’s fabric?
- Will my organization be effectively locked into this provider?
Security - Change Management

One of the benefits of cloud computing is the ability to quickly turn-up and turn-down resources. For highly-regulated industries, this “flexibility” can result in a compliance nightmare.

- For PCI-DSS environments, vulnerability scans must take place after major changes.
- How does the CSP manage changes to its infrastructure?
- How are my organization’s change-management practices altered by migrating to the cloud?
- Just because change is easy, does not meant that changes should take place.
Security - Provider Concerns

In an effort to make the delivery of services as automated as possible, CSPs have invested significant resources into self-service portals and other provisioning tools. A compromise to these tools, similar to compromising the hypervisor, would generate notable security risks.

- How has the CSP secured its provisioning platform?
- Who has system administrator rights to these tools?
- How are these rights reviewed?
CSPs vary notably and each has its own unique risk profile.

- What is the financial status of my organization’s provider?
- What is the average tenure of their employees?
- Are there third-parties that are required to deliver the services that my CSP provides?
- What exceptions were part of my CSP’s SAS 70 Type II audit (now SSAE 16)? How will these exceptions change our assessment of the provider’s risk profile?
- How reliable has our provider been? What types of outages have occurred? Have there been security breaches? Would they say?
- How transparent is my CSP?
Security - Security Devices

Many CSPs offer security services with embedded appliances connected directly to the cloud fabric.

✓ According to Gartner “Keeping security separate from the infrastructure will always be the most secure approach as long as software is involved.”
✓ What security devices are part of my infrastructure?
✓ Which security devices are shared?
✓ How readily can rules and policies be changed to my organization’s security infrastructure?
✓ How easily can we use dedicated, stand-alone security devices?
Why Does Governance Matter?

With so many regulations and compliance requirements, good governance is critical. Governance affects all organizations...private, public, academic, non-profit, and closely-held.

No organization is exempt from regulatory oversight. In short, IT Governance is no longer optional.

Some of the forces driving an emphasis on governance include:

- Sarbanes-Oxley (Financial Reporting Controls)
- SB 1386 (Uniquely Identifiable Data Custodianship)
- HIPAA (Uniquely Identifiable Health Records)
- SEC 17a-3/4 (e-mail & IM retention requirements)
- NASD 3010 & NYSE 342 (similar to SEC 17a-3/4 - records retention)
- Gramm-Leach-Bliley Act (Uniquely Identifiable Data Custodianship)
Who’s Responsible?

‘IT governance is the responsibility of the Board of Directors and Executive Management.

It is an integral part of enterprise governance and consists of the leadership and organizational structures and process that ensure that the organization’s IT sustains and extends the organization’s strategy and objectives.’

(IT Governance Institute - Board Briefing on IT Governance - 2003)
 Responsible, Accountable, Consulted & Informed (RACI)

IT activity is not isolated from the rest of the organization. The COBIT framework offers guidance on who the key participants should be for a given IT process. Key participants include the following roles within an organization:

- Board of Directors
- CEO
- CFO
- Business Executives
- Business Process Owners
- CIO / CTO
- IT Operational Staff
- Compliance Staff
- 3rd Party Service Providers
<table>
<thead>
<tr>
<th>Control Objective</th>
<th>Assertions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Activity</td>
<td>Completeness</td>
</tr>
<tr>
<td>Control Classification</td>
<td>Existence or Occurrence</td>
</tr>
<tr>
<td>Preventative</td>
<td>Presentation and Disclosure</td>
</tr>
<tr>
<td>Detective</td>
<td>Rights and Obligations</td>
</tr>
<tr>
<td>Corrective</td>
<td>Valuation or Occurrence</td>
</tr>
<tr>
<td>Control Type</td>
<td>Risk (Magnitude &amp; Likelihood)</td>
</tr>
<tr>
<td>Manual</td>
<td>High</td>
</tr>
<tr>
<td>Automated</td>
<td>Medium</td>
</tr>
<tr>
<td>Hybrid</td>
<td>Low</td>
</tr>
<tr>
<td>Control Effectiveness</td>
<td>Control Failures</td>
</tr>
<tr>
<td>Adequate</td>
<td>By Design</td>
</tr>
<tr>
<td>Inadequate</td>
<td>In Operation</td>
</tr>
</tbody>
</table>

**The Language of Governance**
COBIT’s Structure

COBIT has four governance domains with 34 IT processes with a total of 210 control objectives (excluding application controls).

The domains are:

- **Plan & Organize (PO)** - 10 Processes
- **Acquire & Implement (AI)** - 7 Processes
- **Deliver & Service (DS)** - 13 Processes
- **Monitor & Evaluate (MS)** - 4 Processes

COBIT provides guidance on control activities, control accountability & ownership, and a maturity model to baseline process maturity.
COBIT’s Maturity Model

The maturity model allows organizations to baseline their process maturity against well-defined standards.

0 = Management processes are not applied at all
1 = Processes are ad hoc and disorganized
2 = Processes follow a regular pattern
3 = Processes are documented and communicated
4 = Processes are monitored and measured
5 = Good practices are followed and automated

Source COBIT 4.1 (IT Governance Institute)
15 Key IT Management Domains

1. Risk Management
2. IT Planning
3. Acquire, Implement & Test Technology
4. Policies & Procedures Management
5. Data Management
6. Availability & Recoverability Management
7. Security Management
8. Change Management
9. Configuration Management
10. Incident Management
11. IT Infrastructure Management
12. Operations & Staffing Management
13. Third-Party Service Provider Management
14. End-User Application Management (i.e. Excel)
15. Application Management
IT Risk Assessment

Business Environment
• Linkage to Business Processes
• Complexity
• Service Provider Relationships

Operational Management
• Data Management
• Availability & Recoverability Management
• Security Management
• Change Management
• Configuration Management
• Incident Management
• Server Management
• Network Management
• System Monitoring

Infrastructure
• Application
• Database
• Operating System
• Servers
• Storage
• Network
• Data Center
Effective management of an organization’s information assets (data) represents a linchpin to good IT Governance. There are some important considerations as they relate to data (i.e. storage) management:

1. Data Classification
2. Data Custodianship
3. Data Retention
4. Data Location
5. Data Source
6. Data Structure
7. Data Availability
8. Data Integrity
9. Data Backup & Restore
10. Media Labeling & Custodianship
Data Classification

Data classification is one of the foundations of IT governance. Good classification techniques help organizations structure IT architectures, determine security requirements, and determine data management requirements.

Key classification guidelines include:

Classification Labels (Samples below)
- Restricted
- Company Confidential
- Proprietary & Confidential
- Public

Data Custodianship
- Data Owner
- Data Users
- Data Custodians

Data Mapping
ITIL Lifecycle

ITIL has specific processes, with guidance, that map to one or more of five domains:

• Service Strategy
• Service Design
• Service Transition
• Service Operation
• Continual Service Improvement
ITIL - Service Strategy

The Service Strategy stage within ITIL consists of the following processes:

- Business Relationship Management
- Service Portfolio Management
- Financial Management
The Service Design stage within ITIL consists of the following processes:

- Design Coordination
- Supplier Management
- Information Security Management
- Service Catalog Management
- Service Level Management
- IT Service Continuity Management
- Availability Management
- Capacity Management
ITIL - Service Transition

The Service Transition stage of the ITIL framework consists of the following processes:

- Transition Planning and Support
- Knowledge Management
- Release & Deployment Management
- Service Asset & Configuration Management
- Change Management
ITIL - Service Operation

The Service Operation stage of ITIL consists of the following processes:
✓ Service Desk Function
✓ IT Operations Management Function
✓ Application Management Function
✓ Technical Management Function
✓ Event Management
✓ Request Fulfillment Management
✓ Access Management
✓ Problem Management
✓ Incident Management
ITIL - Continual Service Improvement

The Continual Service Improvement is ubiquitous throughout all processes and leverages a seven-step process to improve service delivery:

1. Identify the strategy for improvement
2. Define what is measured
3. Gather data
4. Process data
5. Analyze information and data
6. Present and use the information
7. Implement Improvement
Thank you!

Matt Stamper, MPIA, MS, CISA, ITIL Foundation
858-836-0224 / 760-809-2164 (Mobile)
matt.stamper@redit.com