

Exclusive New Report



ITIL Design Guidelines

Part 2 – ITIL Service Design

Randy A. Steinberg

Robin Yearsley

ITIL Design Guidelines

Part 2 - ITIL Service Design

Paper Overview

Purpose This paper briefly describes the concept of using guidelines when designing ITIL services. It then presents a starter set of design guidelines that can be used by IT Service Management Implementation teams.

Contents This publication contains the following topics:

Topic	See Page
Paper Overview	2
Understanding Design Guidelines	3
Design Guideline Examples for ITIL Service Design	10

Understanding Design Guidelines

Overview

Introduction The following section provides some basic background on what Design Guidelines are and how to use them.

Contents This part contains the following topics:

Topic	See Page
Design Guidelines Defined	4
Components of a Design Guideline	5
Examples of Design Guidelines	7
Examples of Poorly Constructed Design Guidelines	8
Examples of Design Guideline Categories	9

Design Guidelines Defined

Introduction The following section defines Design Guidelines within an ITIL context and lists their key attributes.

Definition Design Guidelines:

- Are statements about how IT Services should operate.
- Support the IT Service Management Vision.
- Are critical statements of direction that will have major impact on how IT services should be designed and operated.
- Should be clearly understood and communicated both internally and externally to IT Services.

Derivation These Guidelines are derived from:

- Basic beliefs
- Experience
- Priorities
- Underlying culture within a business organization
- People involved with the delivery of IT Services.

Components of a Design Guideline

Introduction As an early activity in IT Service Management implementation, consider each guideline in isolation. The underlying rationale for advancing each guideline with its resulting implications and impacts should be agreed to and documented.

Describing Guidelines Each guideline has three parts, which are described below:

- Statement
- Rationale
- Implications

Statement This consists of a single sentence that states the guideline.

Example:

We will let our customers know the key services we offer them and who is accountable.

Rationale This lists reasons why the guideline should be accepted by the business.

Considerations include:

- Why should the organization do this?
- What business benefits does this guideline advance?
- What characteristics can be used to defend the guideline?

Examples:

- Will provide clear accountability for the service.
 - Will provide service clarity for the customer.
-

Continued on next page

Components of a Design Guideline, Continued

Implications This lists areas of impact to business and IT units as a result of operating with the guideline.

Considerations include:

- What needs to be done if the guideline is implemented?
- What impact will it have on business and IT units?
- What kind of behaviours, tools, data or processes need to be in place to support it?

Example:

- We will need to define each service that we offer in a Service Catalogue.
 - We will need to develop cross-organizational capabilities.
 - We will have to establish a formal communications program.
 - We will have to establish a single owner for each service.
-

Examples of Design Guidelines

- Characteristics** Well designed guidelines have the following characteristics:
- States a fundamental belief of the enterprise in one or two clearly written sentences.
 - Relevant to the IT Service Management solutions.
 - Worded directly and simply in terms understandable by both business and IT managers.
 - Widely applicable.
 - Will not be outdated quickly by advancing technology.
 - Have objective reasons for advancing it over the considered alternatives.
 - Have impacts which need to be documented.
-

- Examples** The following are examples of some well constructed design guidelines:
- External customer information will be kept strictly confidential within policies set by the organization and regulatory agencies.
 - Service Management solutions, whether purchased or developed internally, will be highly structured and modular.
-

Examples of Poorly Constructed Design Guidelines

- Characteristics** The characteristics of a poorly designed guideline are:
- The statement is difficult to dispute.
 - Is a general business or financial statement.
 - Does not support business goals.
 - Is stated at too low a level or names a product/technology.
 - May be included with "because I say so".
-

- Examples** Examples of some poorly designed guidelines are:
- The overall cost of computing must be reduced. (A business objective but not a guideline)
 - All servers will use the EISA Bus to achieve high performance. (Specifies an exact standard at a very low technical level)
 - Only Ethernet LANs will be implemented in our corporation. (Specifies a standard with a specific technology already selected)

Design Guideline Examples for ITIL Service Design

Overview

Introduction The purpose of these examples to give the reader a starting point for defining their own unique design guidelines, not to dictate or recommend them.

For purposes of clarity, the examples are grouped by key topics within the ITIL Version 3 Service Design book.

Contents This section contains the following topics:

Topic	See Page
Service Catalogue Management Examples	10
Service Level Management Examples	15
Capacity Management Examples	20
Availability Management Examples	30
IT Service Continuity Management Examples	39
Information Security Management Examples	49
Supplier Management Examples	57
Service Design Technology Examples	62
Service Design Organization Examples	69

Guideline Example #1 – Service Catalogue Management

Principle We will let our customers know the key services we offer them and who is accountable.

Sample Application For any service in our Service Catalogue, a customer can determine:

- How to access the service.
- The level of service offered.
- Agreed to quality indicators that are used to monitor service levels.
- Staff responsible for delivering service levels.

Rationale

- Clear accountability for customer service.
- Clarity for the customer.

Implications

- A service catalog that defines each service is in place.
- Cross-organizational capabilities are in place.
- Approaches and responsibilities are publicized.
- Each service has a single owner.
- Roles and responsibilities are strongly communicated.
- A process is in place to maintain information on the accountability structure and ensure this information is current for customers.
- An account management role has been established and clearly communicated.
- Conflicts between owners and account managers are managed.

Guideline Example #2 – Service Catalogue Management

Principle The Service Management services to be provided will be defined in the form of specific service package offerings.

Sample Application Each service package describes 3 service levels (minimum, normal, extended) and there will be 2 types of service packages (basic services and special services).

Rationale

- Assures affordability of services offered/received.
- Limits the number of special services by ensuring the broad application of basic services.
- Reduces the number of managed SLA's and SLA contracts.

Implications

- We have tools that allocate costs appropriately.
- We ensure only valuable services are funded.
- We consider which SLA structures and organizations to use.

Implications

- Analysis is needed to determine the business value for IT services.
- An established and agreed set of business outcomes and benefits needs to be in place
- IT needs to fully understand what services it is delivering to the business
- IT needs to articulate services in business terms

Guideline Example #3 – Service Catalogue Management

Guideline The Service Catalogue will be structured via well defined lines of services that separate IT business support services seen by the business from IT technical support services not seen by the business but used to run IT.

Sample Application The Service Catalogue has a service line called IT Business Support services that includes Accounts Payables Support, Sales Support and HR Support services. Another line of service called Operational Management services includes Job Scheduling, Backup/Restore and Event Monitoring services.

Rationale

- Makes the Catalogue easier to comprehend and manage.
- Allows IT or the business to quickly find services they are interested in without wading through long lists of services.
- Fosters a clear understanding of what IT services are seen by the business versus not seen by them.

Implications

- A set of service lines has been defined and agreed.
- IT understands what services they are delivering to the business versus ones needed for internal management.
- The capability to describe IT services in business terms needs to be in place.

Guideline Example #4 – Service Catalogue Management

Guideline The services offered in the IT Service Catalogue will be reviewed on a periodic ongoing basis to ensure they are aligned with current business needs and objectives.

Sample Application The IT Service Catalogue is reviewed at the end of every quarter to determine:

- What new services should be added
- What services should be marked for removal
- What service delivery targets or levels may need to change
- What existing services may need to be enhanced, reduced or improved

Rationale

- Services may be offered that are not of interest to the business.
- The IT Service Catalogue will become obsolete and useless.
- Business service expectations will differ from what IT thinks it needs to deliver.

Implications

- A process is in place for reviewing and updating the IT Service Catalogue.
- Communication exists between the business and IT for identifying business plans and strategies that may require new services.
- A process is in place for formally agreeing on the contents of the IT Service Catalogue.
- Service lines and service descriptions are accurately described in the Catalogue.
- A Change Management process is in place to handle requested changes to the IT Service Catalogue.

Guideline Example #5 – Service Catalogue Management

Guideline The IT Service Catalogue will be well communicated throughout the business enterprise.

Sample Application A corporate webs site is maintained throughout the business enterprise from which users may order and receive IT services.

Rationale

- Sets business expectations about what IT can deliver.
- Quickly identifies needs for investment to support pending business requirements that are not covered by the services listed in the Catalogue.
- Prevents wasted IT labour spent on behalf of user requests for non-standard services that may not be strategic or necessary.
- Puts decisions on IT investments in hands of executive management versus IT line staff.

Implications

- Publishing capabilities are in place to publish the IT Service Catalogue.
- IT services are described in business terms.
- IT services are defined and described accurately.
- The IT Service Catalogue is maintained in a manner that keeps it current with business needs and objectives.

Guideline Example #6 – Service Level Management

Guideline

No service targets will be established that cannot be effectively delivered by our IT service organization and its suppliers.

Sample Application

The Desktop Support service will not guarantee repair of a desktop at a user location any sooner than 6 hours because the 3rd party support service will not guarantee arrival of the repair technician any sooner than 4 hours.

Rationale

- Setting service targets that can't be met will only create distrust and low satisfaction in the services IT delivers
 - The business may make costly mistakes by relying on IT services that really can't be delivered as promised
 - Wasted labor is incurred in dealing with user calls, complaints and issues when their expectations are not met
-

Implications

- A Service Catalogue is in place that clearly describes the services and service targets that customers can expect to receive
 - Capabilities are in place to measure and monitor the service targets that have been set
 - A formal agreement process is in place for agreeing the service targets from the start
 - All 3rd party suppliers have agreed and documented the services and service targets they intend to deliver
-

Guideline Example #7 – Service Level Management

Guideline No service target will become a service level unless it can be measured per methods agreed to by both the provider and the receiver of the service.

Sample Application The availability service target for the HR Support service will be considered below target if more than 5 incident calls have been logged at the Service Desk in any given month. The Service Desk has the capability to measure how many calls for that service are received. The target of less than 5 calls per month has been agreed to by both IT as well as the HR business unit.

Rationale

- What cannot be measured cannot be managed.
- Satisfaction with IT services will be low if only IT is setting the targets they think the business needs.
- IT will typically operate and manage with service levels that they feel comfortable with delivering even though they may be inadequate for the business.
- Increases business confidence in IT capabilities and services.

Implications

- Service targets are defined in business terms.
- IT has the capabilities in place to monitor and measure the targets being established at reasonable cost.
- A negotiation and agreement procedure is in place to agree on service targets and levels.
- Reporting and communications are in place to communicate how well service targets have been met.

Guideline Example #8 – Service Level Management

Guideline Services will be managed proactively to address business needs versus just reacting to business events and service issues.

Sample Application IT action is initiated when established service targets appear threatened versus delaying action until they fall below target.

Rationale

- Increases business unit satisfaction with IT services.
- Increases business unit confidence in IT capabilities.
- Lowers risk of costly service outages.
- Prevents service outages from occurring before they become visible incidents and problems.

Implications

- Clearly established and agreed service targets are in place.
- Capabilities exist to monitor threats to established service targets before they become too severe.

Guideline Example #9 – Service Level Management

Guideline No service targets will be agreed and communicated until all underpinning provider and supplier services related to those targets are formally agreed to.

Sample Application Publishing of the availability service target for the Customer Relationship Support service is being delayed pending the underpinning contract with the 3rd party application support vendor and signature on Operational Level Agreements with 2 IT technical support units.

Rationale

- May set and communicate service targets that cannot be delivered.
- Providers and suppliers will have no stake in ensuring targets are delivered as needed by the business.
- Ensures that services are managed end-to-end versus as individual technology support silos.

Implications

- Underpinning contracts and Operational Level Agreements need to be established and maintained.
- Some 3rd party vendor contracts may need to be modified if their service delivery targets are ill defined.

Guideline Example #10 – Service Level Management

Guideline Each business unit will have a single point of contact into the IT organization for all its services to address service quality, escalate service issues and communicate service changes.

Sample Application A Business Unit IT Liaison representative meets with the Marketing department once each month to review service quality, report on progress of key service issues and communicate new services needed by that department to IT.

Rationale

- Greatly increases business unit satisfaction with IT services.
- Provides business needs and a business perspective to the IT organization.
- Addresses service issues before they become too severe.
- Identifies new changes to services needed to keep up with business demands for IT on a timely basis – prevents unplanned surprises.
- Ensures IT activities are appropriately aligned to business needs.

Implications

- Investment in IT to business liaisons will be needed.
- Roles and responsibilities for liaison staff need to be clearly defined.
- Liaisons need to be aware of IT plans and activities.
- Liaisons have proper management support to get things accomplished on behalf of the business units they represent.

Guideline Example #11 - Capacity Management

Principle Business units will provide consolidated business capacity planning information.

Sample Application The Order Entry Business Unit will provide the following business capacity planning information to the capacity manager on a monthly basis:

- Number of customers
- Average number of units sold per customer per month
- Number of company retail locations

Rationale

- Promotes business unit buy-in and responsibility for influencing the capacity requirements for their services.
- Promotes a business-oriented approach to defining capacity planning information.
- Improves the reliability of the planning data.
- All capacity usage is driven by business events.

Implications

- Business units have committed to the process.
- We have a method of translating business data into IT terms.

Guideline Example #12 - Capacity Management

Guideline Every IT service must identify the business factors that drive the usage of that service and forecast volumes for those factors to estimate their future impact on capacity needs for that service.

Sample Application The Email Messaging service capacity is driven by:

- Number of company employees
- Average size of message transmitted
- Average number of messages saved per employee

The business units provide forecasts on changes to the number of employees and IT provides information on message sizes and messages saved. The forecasts are then modelled by Capacity Management to determine needed infrastructure upgrades.

Rationale

- Ties capacity needs to actual business events.
- Results in more accurate capacity plans than using historical, trend analysis or other means of forecasting growth.
- Allows the business to see how decisions directly impact IT services.
- Provides capability to model business decisions to predict their impact on IT capacity needs before major investment has taken place.

Implications

- IT services are known and agreed.
- Business drivers that consume IT services are known and agreed.
- Capabilities exist to measure business driver volumes.
- The underpinning workload and CIs for each service are known
- Service workloads are accurately characterized for modelling.

Guideline Example #13 - Capacity Management

Guideline Capacity management must incorporate service and business activity forecasts and their impact on required capacity needs.

Sample Application The IP Telephony service requires that business units provide forecasts on number of employees that will use the service which in turn are used to model future capacity needs.

Rationale

- Cannot accurately predict future capacity for a service if the business and service plans and events are not understood.
- Aligns capacity plans with business plans and objectives.
- Promotes mutual business and IT understanding of capacity needs and issues.

Implications

- Business and service drivers for capacity usage are known.
- Business units agree to be responsible for forecasting business factors that drive capacity.
- Business units are held accountable for the accuracy of their business forecasts.

Guideline Example #14 - Capacity Management

Guideline

A Capacity Plan will be in place and kept current at all times.

Sample Application

Capacity Management produces an updated Capacity Plan at the end of each business quarter. The plan incorporates known business and IT forecasts and variances against planned capacity. It presents the current strategy and timetables for key upgrades and capacity growth tied to the forecasts.

Rationale

- Prevents unplanned expenditures due to unplanned capacity needs.
 - Capacity plans may quickly become obsolete if not kept current with changing business demand.
-

Implications

- A Capacity Management function must be in place and adequately staffed.
 - Management buy-in and support for the Capacity Plan is in place.
 - Business units provide accurate business forecasts on a timely basis.
 - A formal procedure is in place to prepare, present and review the Capacity Plan.
-

Guideline Example #15 - Capacity Management

Guideline The Capacity Management function will be the focal point for all capacity planning and performance tuning activities.

Sample Application Capacity Management functions are centralized within the IT organization. Plans and strategies are communicated through this single organization.

Rationale

- Multiple capacity strategies and plans developed by differing groups may create confusion and overlapping efforts.
- May investment more in IT infrastructure capacity needs than what might really be needed.
- Capacity impacts of one department may negatively impact capacity provided to another department.

Implications

- An organizational set of roles and responsibilities must be in place for providing Capacity Management activities.
- Senior executives adequately support the centralized Capacity Management function.
- Input to the Capacity Plan may need to be provided by individual IT and business units and then integrated into an overall plan.

Guideline Example #16 - Capacity Management

Guideline Capacity recommendations will include financial impacts of capacity strategies as well as technical strategies.

Sample Application The capacity strategy to handle a 30% increase in the number of employees using the Email Messaging Service not only shows options in upgrades to provide needed capacity for that increase, but also an estimate for the level of investment needed for each option.

Rationale

- Capacity needs have to be provided at acceptable costs to the business.
- Many times, a technical strategy will be rejected if it is discovered that its costs are unacceptable.

Implications

- Financial Management activities need to be in place enough to support Capacity Management.
- Agreement exists as to how estimates for costs and upgrades are derived.

Guideline Example #17 - Capacity Management

Guideline All changes to services and the IT infrastructure will be assessed in terms of their impacts on current capacity plans and strategies.

Sample Application Capacity Management has representation on the company CAB (Change Advisory Board). In this role, they review each change brought before the board in terms of its potential impact on current capacity, performance and planned capacity strategies and upgrades.

Rationale

- Prevents changes from corrupting planned capacity strategies and activities.
- Prevents service outages that might be caused by unexpected capacity failures related to changes.

Implications

- A formalized Change Management process is in place.
- Capabilities exist to inform Capacity Management of what changes are being requested.
- There is enterprise agreement and recognition that changes may be rejected due to their capacity impacts.

Guideline Example #18 - Capacity Management

Guideline Capacity plans, forecasting assumptions, workload models and performance data will be safely stored and readily accessible to IT staff and management.

Sample Application All Capacity Plan documents, forecasts, forecast assumptions, workload descriptions, models, performance data and business demand factor volumes are stored in a Capacity Management Database which is linked to a CMDB (Configuration Management Database).

Rationale

- Provides an authorized source for capacity and performance information and assets.
- Makes capacity and performance information readily available to other service support and delivery processes.
- Speeds the process by which Capacity forecasts and plans are developed.

Implications

- Technologies are in place to store Capacity information and relate it to Configuration Items.
- Schemas and Meta data strategies have been developed for how Capacity information will be stored and accessed.

Guideline Example #19 - Capacity Management

Guideline

Capacity Management activities will manage capacity and performance proactively wherever possible.

Sample Application

Each day, a capacity analyst checks key resource monitoring indicators to check current performance and utilization levels against thresholds. In addition, the analyst also examines capacity and performance results for changes in trends against what was predicted in the Capacity Plan. Any variations found are escalated to the Capacity Manager.

Rationale

- Prevents service outages that are capacity related.
 - Prevents unplanned labour related to dealing with sudden unexpected capacity issues.
 - Prevents unplanned costs related to emergency capacity expenditures not previously foreseen.
-

Implications

- A set of Key Performance Indicators (KPIs) must be in place to monitor effectiveness of Capacity Management activities.
 - Capabilities must be in place to monitor key performance and capacity levels for services effectively and with a minimum amount of labor cost.
 - Capacity thresholds related to each service must be defined to determine whether capacity issues may be starting to appear.
-

Guideline Example #20 – Capacity Management

Guideline The scope of Capacity Management activities will include capacity impacts and needs for Availability and Service Continuity Plans.

Sample Application The Capacity Plan includes planned upgrades for 30 additional servers to accommodate redundant data stores for the Sales Management service. These stores were specified in the Availability Plan for that service as a way to quickly provide failover capabilities in case the main production data stores encounter failures.

Rationale

- Availability and Service Continuity strategies both require enough capacity to be in place to make them successful.
- In the event a major business disruption occurs, there may not be enough capacity to support vital business functions.
- Predicted costs for an availability strategy may be under estimated if the capacity needs for that strategy are not considered.

Implications

- Capacity Management needs to be tightly integrated with Availability and Service Continuity planning activities.
- Availability and Service Continuity strategies must be able to be characterized as IT workloads.
- Availability and Service Continuity plans must not be considered complete until their capacity implications have been considered.

Guideline Example #21 - Availability Management

Principle We will provide consistent, robust, secure and cost effective IT assets and services through a centralized services function.

Sample Application All server equipment, while located at various places within the organisation, will be centrally managed, utilising remote management tools and capabilities.

Rationale

- Manages distributed resources cost-effectively.
- Enables resources to be assembled in the most effective location.

Implications

- Tool capabilities have been confirmed and deployed.
- Effective communication channels to remote systems are in place.
- Application and infrastructure platforms are capable of remote, unattended management.
- A mechanism to define the most effective location of IT assets and services is in place.
- A review of existing and legacy systems has been done and a transition plan has been developed.
- We have qualified ownership of development, test and production environments.

Guideline Example #22 - Availability Management

Principle We will be the guardians of IT systems and services, ensuring they are available in-line with business needs at acceptable costs.

Sample Application IT availability plans are built on the basis of business needs for system availability and with a clear understanding of the business value of system uptime.

Rationale

- IT Supported systems are key business enablers.
- System availability is the way that IT adds value to the business.
- Without IT systems the business data is inaccessible.
- There is a direct cost to business for unplanned downtime.

Implications

- The business is enshrined in our SLA's.
- We are prepared to enable rather than inhibit business change.
- We have aligned our planning with the business calendar.
- We fully understand the business requirements.
- Our organization is focused on availability.

Guideline Example #23 - Availability Management

Guideline Availability strategies must take a holistic view of the services they support versus only technologies.

Sample Application Availability strategies for the company's product logistics IT support service include support staff, skills awareness, training, physical plant, security processes and Service Desk as well as the hardware, software and networking technologies that underpin it.

Rationale

- The business cares about the overall services they receive and not the technologies that underpin them.
- May provide high availability for technology platforms but still provide poor levels of service.
- May overspend on IT infrastructure hardware and software to overcome an availability issue that could have been solved with a better process, communication or more training.

Implications

- IT services are known and agreed.
- The underpinning IT infrastructure for each service must be known and understood.
- Availability strategies must look beyond the technical solutions when being developed.
- Availability strategies will include non-technical recommendations as well as technical ones.

Guideline Example #24 - Availability Management

Guideline Every IT service must identify the risk factors that exist with that service and assess those risks to that service.

Sample Application The Sales Support IT Support Service has identified 2 severe infrastructure risks and 3 moderate level risks to its successful operation. The likelihood of one of the sever risks is high. Therefore, the current availability plan will highlight this risk and include recommended strategies and actions to mitigate it.

Rationale

- Allows the business to see how threats and risks will directly impact IT services.
- Ensures availability plans, strategies and activities are appropriately aligned to the business.
- Focuses priority and investment on mitigating those risks with the greatest likelihood of disrupting the business.

Implications

- IT services are known and agreed.
- Risk factors for IT services are known and agreed.
- The likelihood of risks occurring must be known and estimated in a manner that everyone agrees to.
- Availability plans must clearly identify risks, their likelihood of occurring and the actions needed to mitigate them for each IT service.
- The impact of executing availability activities in the plan must show how they will reduce the likelihood of risks occurring.

Guideline Example #25 - Availability Management

Guideline	An Availability Plan will be in place and kept current at all times.
Sample Application	Availability Management produces an updated Availability Plan at the end of each business quarter. The plan incorporates all known changes to IT availability plans and activities based on changes in business need and changes made to the IT infrastructure.
Rationale	<ul style="list-style-type: none">• Prevents unplanned expenditures due to unplanned availability needs.• Availability plans may quickly become obsolete if not kept current with changing business demand or changes to the IT infrastructure.
Implications	<ul style="list-style-type: none">• An Availability Management function must be in place and adequately staffed.• Management buy-in and support for the Availability Plan is in place.• A formal procedure is in place to prepare, present and review the Availability Plan.• Availability Management must be made aware of changes to the IT infrastructure since the last plan was produced.

Guideline Example #26 - Availability Management

Guideline The Availability Management function will be the focal point for all key availability plans and strategies.

Sample Application Availability Management functions are centralized within the IT organization. Plans and strategies are communicated through this single organization.

Rationale

- Multiple availability strategies and plans developed by differing groups may create confusion and overlapping efforts.
- May invest more in IT infrastructure availability needs and solutions than what might really be needed.
- Availability actions of one department may negatively impact availability actions of another department.

Implications

- An organizational set of roles and responsibilities must be in place for providing Availability Management activities.
- Senior executives adequately support the centralized Availability Management function.
- Input to the Availability Plan may need to be provided by individual IT and business units and then integrated into an overall plan.

Guideline Example #27 - Availability Management

Guideline	Availability recommendations will include financial impacts of availability strategies as well as technical strategies.
Sample Application	The IT Availability Plan associates each availability strategy in the plan with its costs.
Rationale	<ul style="list-style-type: none">• Availability needs have to be provided at acceptable costs to the business.• Many times, a technical strategy will be rejected if it is discovered that its costs are unacceptable.
Implications	<ul style="list-style-type: none">• Financial Management activities need to be in place enough to support Availability Management.• Agreement exists as to how estimates for costs are derived.• Costs for availability strategies must take a holistic view of all hardware, software, network, people, facilities, license and other related costs when building availability strategies.

Guideline Example #28 - Availability Management

Guideline All changes to services and the IT infrastructure will be assessed in terms of their impacts on current availability plans and strategies.

Sample Application Availability Management has representation on the company CAB (Change Advisory Board). In this role, they review each change brought before the board in terms of its potential impact on current availability plans, strategies and activities.

Rationale

- Prevents changes from corrupting availability plans, strategies and activities.
- Prevents service outages that might be caused by unexpected availability failures related to changes.

Implications

- A formalized Change Management process is in place.
- Capabilities exist to inform Availability Management of what changes are being requested.
- There is enterprise agreement and recognition that changes may be rejected due to their impact on availability plans and strategies.

Guideline Example #29 - Availability Management

Guideline Availability Management activities will manage availability proactively wherever possible.

Sample Application Each day, an availability analyst checks key resource monitoring indicators, problem and incident trends to determine availability levels against thresholds. In addition, the analyst also examines these to proactively identify impending availability issues. Any issues found are escalated to the Availability Manager.

Rationale

- Prevents frequent or unstable service outages before they happen.
- Prevents unplanned labour related to dealing with sudden unexpected availability issues.
- Prevents unplanned costs related to emergency expenditures to increase availability not previously foreseen.

Implications

- A set of Key Performance Indicators (KPIs) must be in place to monitor effectiveness of Availability Management activities.
- Capabilities must be in place to monitor key availability levels for services effectively and with a minimum amount of labor cost.
- Availability thresholds related to each service must be defined to determine whether availability issues may be starting to appear.
- Problem and incident reporting must be in place to support trending and analysis activities.

Guideline Example #30 - IT Service Continuity Management

Principle We will ensure that vital IT service functions are recoverable in-line with business needs on a timely basis and at acceptable costs.

Sample Application IT Service Continuity plans are built on the basis of business needs for system availability and with a clear understanding of the business value of system uptime.

Rationale

- Without IT systems, the business data is inaccessible.
- There are major costs to business for extended downtime.

Implications

- We have aligned our planning with the business continuity plan
- We understand that IT continuity planning is about more than IT systems.
- We fully understand the vital business functions and their requirements.

Guideline Example #31 - IT Service Continuity Management

Principle There will be an annual test of IT Service Continuity recovery processes.

Sample Application A complete recovery test for application ABC services will be scheduled annually for the last week in October.

Rationale

- Ensures that critical data and systems can be quickly recovered in the event of a major outage.
- Ensures that services recovered match those currently in production.
- Ensures that capacities for recovery are truly effective.

Implications

- Management is committed to the yearly test.
- We understand testing expenses.
- We perform ongoing analysis of what is critical to the business.

Guideline Example #32 – IT Service Continuity Management

Guideline IT recovery plans must recover services – not just technologies.

Sample Application The plans for recovering the company’s Email services include all Email applications, mailboxes, support staff, supporting hardware, software and networking infrastructure as well as the LANs and PC access to Email functions to ensure that end-to-end Email services can be restored in the event of a major business disruption.

Rationale

- Recovering specific technologies is useless if the services they underpin still won’t operate.
- Services will still be down even though technologies were successfully recovered.
- Costs for recovery strategies may be greatly under estimated.

Implications

- IT services are known and agreed.
- Recovery plans must take a holistic service view when creating recovery strategies and detailing recovery activities.

Guideline Example #33 – IT Service Continuity Management

Guideline Every IT service must identify the vital business functions that it provides which must be adequately provided for in the IT Service Continuity Plan.

Sample Application Insurance Company ABC has formalized the following as vital business functions:

- Processing claims
- Paying employees and claim agents
- Processing payments from premiums
- Disbursing payments to customers for claims

Without these, the company will go out of business. IT continuity plans prioritize recovery of all applications, hardware, software and networking infrastructure to ensure these functions will continue in the event of a major business disruption.

Rationale

- Ties recovery needs to actual business events.
- Ensures recovery activities meet the critical needs of the business in the event of a major business disruption.
- Ensures recovery activities are properly focused and prioritized in line with real business needs.

Implications

- IT services are known and agreed.
- Vital business functions are known and agreed.
- Recovery plans are prioritized by vital business function.

Guideline Example #34 - IT Service Continuity Management

Guideline An IT Service Continuity Plan will be in place and kept current at all times.

Sample Application IT Service Continuity Management produces an updated IT Continuity Plan at the end of each business quarter. The plan incorporates all changes to vital business functions that may have occurred since the last time the plan was produced.

Rationale

- Prevents unplanned expenditures due to unplanned recovery needs.
- Continuity plans may quickly become obsolete if not kept current with changing business demand.

Implications

- An IT Service Continuity Management function must be in place and adequately staffed.
- Management buy-in and support for the IT Continuity Plan is in place.

Guideline Example #35 - IT Service Continuity Management

Guideline The IT Service Continuity Management function will be the focal point for all continuity planning and testing activities.

Sample Application IT Service Continuity Management functions are centralized within the IT organization. Plans and strategies are communicated through this single organization.

Rationale

- Multiple continuity strategies and plans developed by differing groups may create confusion and overlapping efforts.
- Key recovery actions may get missed.
- May invest more in IT infrastructure recovery needs than what might really be needed.
- Recovery actions of one department may negatively impact recovery actions of another department.

Implications

- An organizational set of roles and responsibilities must be in place for providing IT Service Continuity Management activities.
- Senior executives adequately support the centralized IT Service Continuity Management function.
- Input to the IT Service Continuity Plan may need to be provided by individual IT and business units and then integrated into an overall recovery plan.

Guideline Example #36 - IT Service Continuity Management

Guideline IT Service Continuity strategies and recommendations will include financial impacts of those strategies as well as recovery strategy details.

Sample Application IT Service Continuity strategies and recommendations come with associated costs and charges. The costs and charges are balanced against the risks and likelihood of a major business disruption.

Rationale

- May over or under spend on continuity plans and activities.
- May incur unplanned costs and charges once recovery activities have begun.
- Will not be able to balance the investment made against the risks that are being mitigated.

Implications

- Financial Management activities need to be in place enough to support IT Service Continuity Management.
- Agreement exists as to how estimates for costs are derived.
- IT Service Continuity Management must be prepared to provide recovery alternatives if costs are deemed as too high.

Guideline Example #37 - IT Service Continuity Management

Guideline All changes to services and the IT infrastructure will be assessed in terms of their impacts on current IT service continuity plans and strategies.

Sample Application IT Service Continuity Management has representation on the company CAB (Change Advisory Board). In this role, they review each change brought before the board in terms of its potential impact on current plans and strategies for IT recovery.

Rationale

- Prevents changes from corrupting planned continuity strategies and activities.
- May jeopardize the company's ability to recover services if the target infrastructure to be recovered is different from the production infrastructure running currently.

Implications

- A formalized Change Management process is in place.
- Capabilities exist to inform IT Service Continuity Management of what changes are being requested.
- There is enterprise agreement and recognition that changes may be rejected due to their impacts of IT Service Continuity plans and strategies.

Guideline Example #38 - IT Service Continuity Management

Guideline The IT Service Continuity plan, continuity test plans and testing results will be safely stored and readily accessible to IT staff and management.

Sample Application A copy of the IT Service Continuity Plan and all associated documents is maintained at an offsite location in the event of a major business disruption.

Rationale

- In the event of a major business disruption, the Service Continuity Plan may not be able to be accessed at the company's IT processing location.
- At least one location for which the plan can be found will be known to those responsible for IT recovery activities.
- Greatly lowers the risk that continuity plans may get lost or destroyed beyond recovery.

Implications

- A redundant copy of continuity plans and associated documents will need to be synchronized with their originals.
- An offsite location to store the redundant plans must be acquired and made known to all IT staff.

Guideline Example #39 - IT Service Continuity Management

Guideline The scope of IT Service Continuity Management activities will include capacity needs for proper continuation of vital business services in the event of a major business disruption.

Sample Application The Capacity Plan includes planned upgrades for 30 additional servers to accommodate redundant data stores for the Sales Management service. These stores were specified in the Availability Plan for that service as a way to quickly provide failover capabilities in case the main production data stores encounter failures.

Rationale

- Availability and Service Continuity strategies both require enough capacity to be in place to make them successful.
- In the event a major business disruption occurs, there may not be enough capacity to support vital business functions.
- Predicted costs for an availability strategy may be under estimated if the capacity needs for that strategy are not considered.

Implications

- Capacity Management needs to be tightly integrated with Availability and Service Continuity planning activities.
- Availability and Service Continuity strategies must be able to be characterized as IT workloads.
- Availability and Service Continuity plans must not be considered complete until their capacity implications have been considered.

Guideline Example #40 - Information Security Management

Principle We will be the custodians of all company data, ensuring it is correctly stored, readily available, secure and recoverable.

Sample Application All data stored on company servers will be managed by IT services, so that it is available and recoverable for customers. Local data on personal drives will not be managed.

Rationale

- Customers feel secure that their business data is secure and stored in backups, ready for recovery.
- Data is a critical asset with high monetary and business value.

Implications

- We have clear definitions of company and personal data.
- Supported platforms are published with guidelines for where data is stored.
- We are clear on integrity.
- We have implemented security guidelines.
- Data management guidelines have been put into place.

Guideline Example #41 - Information Security Management

Principle

No sensitive data will reside on client workstations.

Sample Application

Customer information for application ABC will reside on corporate server databases and will be read-only at the workstation level.

Rationale

- Minimizes exposures of data being compromised or lost.
 - Reduces security, backup and recovery complexity and costs.
-

Implications

- We perform regular workstation audits.
 - We have simplified backup procedures and given proper data staging rules.
 - We have identified where to stage and locate sensitive data.
-

Guideline Example #42 - Information Security Management

Principle IT is responsible for the integrity of data associated with IT services, irrespective of technical platform.

Sample Application IT has implemented services and controls to ensure that data is secure and reliable.

Rationale

- Data is a corporate asset which IT is mandated to manage.
- Users will not do it.
- There needs to be separation between producers of data and those managing it.

Implications

- We make users aware of what data management IT will and will not provide through SLA's.
- We are able to handle increasingly complex data management requirements driven through increased business demands and regulations.

Guideline Example #43 - Information Security Management

Principle The IT infrastructure used to underpin internal company services will be logically isolated from the DMZ, enterprise business network, and business partners.

Sample Application The systems management tooling infrastructure uses a separate network logically isolated from company business servers and the company DMZ.

Rationale

- Security threats are not just external, the greater threat is often internal.
- Business partners should not have capability of access to the company's networking infrastructure and systems.
- Need to remove risks of "backdoor" security exposures to the greatest extent possible.

Implications

- All servers will need to have their data secured, and both the subsidiary and partner networks will require strong "trusted partner" evaluations to ensure they don't create "backdoor" security exposures.
- Security monitoring of internal connections will be required, both inbound and outbound from the IT infrastructure.
- There may be need for additional hardware/software for access control and intrusion detection.
- Planning for secure performance monitoring of network and server platforms will become more complex.

Guideline Example #44 - Information Security Management

Principle Everything in the DMZ is to be considered disposable.

Sample Application The company has an IT policy that states that no IT supported business services will run on IT infrastructure considered within the company DMZ.

Rationale

- Web sites are commonly attacked and/or vandalized.
- Services will be exposed to security attacks and threats.
- It is nearly impossible to guarantee security for parts of the IT infrastructure exposed directly to the outside world.

Implications

- Server integrity must be monitored and unauthorized alterations prevented or identified and corrected.
- Backup and restore processes must be in place to quickly rebuild the DMZ servers.
- Security recovery will require an isolated alternate path to load/restore servers, secure from the internal network so that recovery does not impact the production network or violate the interior security requirements.

Guideline Example #45 - Information Security Management

Principle IT number of IT infrastructure access points will be minimized for security while balancing availability requirements.

Sample Application The company's main portal service is handled by two different ISP service providers. This ensures that the portal service will still be available even if one of the ISPs encounters a service outage. The security management group carefully administers company firewalls and IP addresses to ensure that a conflict does not arise between the two ISPs and that no security exposures exist by using both ISPs.

Rationale

- Exposure to the outside world must be limited to preserve security.
- Alternate Internet service providers (ISPs) and alternate paths are necessary to maintain service availability.

Implications

- A formal risk analysis will be needed to select designs and carriers.
- Internal network visibility must be controlled and the network isolated from unauthorized access.
- The process of coordinating/selecting multiple ISPs will have to include the administration of router and firewall filtering (addresses, routes, applications, etc.).
- Private networking addresses may be needed so they will be portable across carriers.
- Extra coordination of network address plans with carriers may be needed, as will the need for diverse routes so that a path failure does not disrupt services.
- Web-sites that are mission critical will need a plan for managing multiple-site-access strategies. These multi-site strategies will also have to include both operations and IT service continuity planning.

Guideline Example #46 - Information Security Management

Principle	Client and customer information is sensitive and confidential. Access to that information will be limited to those that need it to perform their job.
Sample Application	Security profiles and access lists are carefully tailored and mapped against corporate job roles and descriptions. Each employee can only access data and services allowed by their job position and description.
Rationale	<ul style="list-style-type: none">• Reduces security vulnerability by attacks from within the company.• May be required for regulatory compliance or audit requirements.
Implications	<ul style="list-style-type: none">• Will require close coordination with company HR functions and processes.• Some company job descriptions may specify multiple job roles with conflicting security requirements.• All infrastructure configuration items that require secure access will need to be controlled through access lists and security controls.

Guideline Example #47 - Information Security Management

Principle IT will take a holistic view of security including physical security access, regulatory controls, audits, people and process in addition to security technologies.

Sample Application The Information Security Management function oversees all physical access operations such as security badges, cameras and facilities access to IT secured areas in addition to monitoring the IT infrastructure for security violations.

Rationale

- Provides a single point of accountability for all of IT security.
- May operate with key entry points for security threats and risks that were not considered.

Implications

- IT needs to understand the full spectrum of security management services.
- There is recognition that a single point of contact and accountability exists for all IT security management activities.

Guideline Example #48 - Supplier Management

Guideline Each supplier will have a single point of contact into the IT organization for all its services to address service quality, escalate service issues and communicate service changes.

Sample Application An IT Liaison representative meets with the 3rd party vendor that supplies server hardware and software each month to review service quality, report on progress of key service issues and communicate new services needed from that supplier to support IT services.

Rationale

- Greatly increases business unit satisfaction with IT services.
- Establishes a win-win relationship between IT and its suppliers.
- Addresses supplier service issues before they become too severe.
- Identifies new changes to supplier services needed to keep up with business demands for IT on a timely basis – prevents unplanned surprises for both IT as well as its suppliers.
- Ensures supplier activities are appropriately aligned to company IT and business needs.

Implications

- Investment in IT to supplier liaisons will be needed.
- Roles and responsibilities for liaison staff need to be clearly defined.
- Liaisons need to be aware of IT plans and activities.
- Liaisons need to be aware of supplier services and capabilities.
- Liaisons have proper management support to negotiate and deal with supplier issues.
- Supplier contracts may need to be modified to accommodate the liaison relationship..

Guideline Example #49 - Supplier Management

Guideline	An underpinning contract must exist with each supplier that underpins IT services. This contract should clearly identify the services and products being provided along with key performance indicators and service targets that can be measured to monitor successful delivery from each supplier.
Sample Application	Service Desk services supplier by a 3 rd party vendor are formally listed as part of a formal contract with that vendor. In addition, the vendor must supply call waiting, call abandon, call transfer, and call closure rates to the IT organization. These metrics have specifically been written into the contract with that vendor.
Rationale	<ul style="list-style-type: none">• Greatly increases business unit satisfaction with IT services.• Ensures clear communication between IT, the business and the supplier.• Ensures the supplier is meeting stated service requirements.• Clearly identifies whether the supplier is meeting its contracted obligations.• Provides a record of supplier performance to company procurement functions.
Implications	<ul style="list-style-type: none">• Investment in IT to supplier liaisons will be needed.• Supplier services need to be fully understood.• Supplier metrics will need to be created and monitored.• Third party contracts may need to be rewritten or modified to accommodate service and metric descriptions.• Supplier performance reports will need to be developed and put into place.

Guideline Example #50 – Supplier Management

Guideline Supplier service and product delivery quality will be examined and reviewed on a periodic basis with each supplier and actions taken to correct and resolve any deficiencies found.

Sample Application An IT Liaison representative meets with the 3rd party vendor that supplies server hardware and software each month to review service quality, report on progress of key service issues and communicate new services needed from that supplier to support IT services.

Rationale

- Greatly increases business unit satisfaction with IT services.
- Fosters a win-win relationship between IT and its suppliers.
- Addresses supplier service issues before they become too severe.
- Ensures supplier activities are appropriately aligned to company IT and business needs.

Implications

- Investment in IT to supplier liaisons will be needed.
- Liaisons need to be aware of supplier services and capabilities.
- Liaisons are made aware of supplier issues and problems on a timely basis.
- Liaisons have proper management support to negotiate and deal with supplier issues.
- Supplier contracts may need to be modified to accommodate the liaison relationship..

Guideline Example #51 – Supplier Management

Guideline Lead suppliers that directly contract with IT must demonstrate that their subcontractors also operate within the same service targets and controls contracted by that lead supplier.

Sample Application Each month, the supplier representative provides the IT Supplier Liaison a report that lists all its services being subcontracted along with required service targets and quality measurement metrics.

Rationale

- Ensures supplier truly has capability to meet its service obligations.
- Mitigates service risks that might be due to poor sub-contractor performance.
- Holds supplier fully responsible for the services they are delivering.
- Avoids finger-pointing between supplier and sub-contractor organizations when service issues occur.

Implications

- Investment in IT to supplier liaisons will be needed.
- Liaisons need to be aware of supplier services and capabilities.
- Suppliers may not be comfortable exposing service quality issues with their subcontractor relationships.
- Supplier contracts may need to be modified to accommodate the requirements for reporting on their subcontractor performance.
- Suppliers and/or subcontractors may not typically operate with adequate controls and service reporting activities.

Guideline Example #52 – Supplier Management

Guideline Outsourcing services or sub-functions to a supplier will not remove the responsibility for delivery quality of those services or sub-functions from the company IT organization.

Sample Application An IT Liaison representative periodically audits supplier service delivery quality metrics to ensure they are produced accurately and result in values that meet established targets and objectives. The liaison also signs off on delivered quality reports from the supplier.

Rationale

- Outsourcing a service or function does not remove the responsibility for it from IT.
- Unknown threats and risks to service delivery quality may exist without IT being aware of them until outages occur.
- Regulatory regulations or audits may require that delivery controls need to be in place irregardless of who is providing the service.

Implications

- Service quality metrics need to be in place with each supplier.
- Metrics need to be examined, reviewed and audited on an ongoing basis.
- IT must be held accountable for all IT services no matter who delivers them.
- Supplier contracts may need to be rewritten or modified to accommodate service quality metrics and key performance indicators.

Guideline Example #53 - Service Design Technology

Principle IT Service Management processes must use common data wherever possible.

Sample Application All incident history and service events will be located in the Incident Management Database.

Rationale

- Promotes integration and correlation of data.
- Reduces the need for re-entry and chance for error.
- Simpler to administer the data.

Implications

- We utilize powerful automated management systems.
- We strive to obtain availability of integrated data solutions whenever possible.
- Data design and normalization activities are done to accomplish this goal.
- Data is interfaced or ported between different automation solutions.

Guideline Example #54 - Service Design Technology

Principle Where significant server to backend host traffic occurs, servers will be collocated with the backend hosts.

Sample Application The trading system IT support service must provide trading prices to regional servers from a centralized mainframe in near real time. As a result, the regional servers will be co-located at the mainframe location since high volumes of update traffic is expected to occur.

Rationale

- Response time will be improved by eliminating unnecessary hops across the network.
- Consistent physical security can be maintained.
- Overhead is greatly reduced as there will be no need for encrypted traffic within the secured data center.
- Operations staff are always available 24/7 to provide real time support.
- Significantly less networking bandwidth and resources will be needed.
- Service transaction performance times can be much better managed and controlled to business need.

Implications

- Additional skills may be required in the data center to support additional servers.
- There will be a need for workload characterization / application profiling to decide which servers should be collocated.
- Politics of “my systems” vs. “enterprise systems” can be an issue, but will have to be over-ruled.

Guideline Example #55 - Service Design Technology

Principle Site engineering will include construction of alternate paths, load balancing, and redundancy to improve availability and scalability wherever possible.

Sample Application The trading system IT support service must provide trading prices to regional servers from a centralized mainframe in near real time. As a result, the regional servers will be co-located at the mainframe location since high volumes of update traffic is expected to occur.

Rationale

- Services typically require high availability and scalability.
- Proactively provides for delivery of high quality services.
- Provides more flexibility for upgrading and maintaining the IT infrastructure that supports services while minimizing disruptions to those services.

Implications

- Redundant components that are needed to provide alternate paths will add costs.
- The topology and technology alternatives add to the complexity of fault isolation, routing designs, recoverability scenarios, administration, and security planning.
- There may be measurable performance impacts because of additional components in the data path.
- Load balancing architectures will need to be mapped to the application requirements for persistence. These may force solutions that have multiple paths and strategies for different application work flows.

Guideline Example #56 - Service Design Technology

Principle The IT infrastructure that underpins services will be engineered to be scalable by being designed to run on multiple, simultaneous servers (web, application, database).

Sample Application The Sales Management IT Support Service has implemented Sales Support applications across smaller servers versus a large mainframe. Databases and web sales portal functions also reside on separate smaller servers.

Rationale

- Horizontal scalability lessens 'box' architecture dependencies and allows for load balancing across systems.
- Allows for site-independence of data and processing.
- Allows for growth in demand of services with much less risk of significant infrastructure upgrades.

Implications

- Performance and capacity planning disciplines need to be in place for the network and the servers.
- Vendor hardware / software architectures may inhibit cross system communications by only being vertically scaleable.
- In some cases, additional management agents may have to be installed within the infrastructure to communicate with load balancing components.
- Some parts of the IT infrastructure may have hard coded links between systems that will require significant changes to overcome.

Guideline Example #57 - Service Design Technology

Principle Primary data will be structured to represent the business entity (e.g., provider, patient, benefit, etc.). The structure of primary data is independent of the applications. Data will conform to defined data models and common data formats and will be accessed using standard data base and file management facilities. Services which create and maintain proprietary data structures and formats will be avoided.

Sample Application The Business Intelligence and Data Warehousing service maintains all needed data infrastructures in a common format that can be accessed by any service.

Rationale

- Ensures company data can be accessed by multiple services as needed both now and in the future.
- Provides greatest flexibility for sharing and reuse of data across all the IT services.
- Prevents additional costs and overhead for maintaining redundant stores of data.
- Reduces complexity of the IT infrastructure.

Implications

- Data structures and relationships must be fully understood by those supporting IT services.
- Some service solutions provided by outside suppliers may come with proprietary formats.
- An enterprise data model will have to be maintained and administered.

Guideline Example #58 – Service Design Technology

Principle	All service design technology solutions must adhere to company IT architecture and infrastructure standards.
Sample Application	Product selection of the Incident Management tool was driven by the supplier who most closely matched company technical standards.
Rationale	<ul style="list-style-type: none">• Reduces costs for maintaining the IT infrastructure by providing consistency of technology.• Reduces risk of service outages related to conflicting standards and products.
Implications	<ul style="list-style-type: none">• An IT architecture governance process must be in place to review changes and new services from an architectural compliance perspective.• IT standards must exist and be well communicated.• Some supplier technology solutions may not match corporate IT architecture standards.• A process needs to exist to deal effectively with architectural exceptions.• Agreement needs to exist between IT and the business to balance need for architectural fit with cost and functionality objectives.

Guideline Example #59 - Service Design Technology

Principle Service technology solutions should be designed with off-the-shelf technology solutions with as minimal customization as possible.

Sample Application The Order Processing IT support service is underpinned by a version of the SAP application that has been implemented with the barest minimum of custom code changes.

Rationale

- Although somewhat greater functionality can be made possible by custom coding solutions, these have proven to be more costly in the long term and create bottlenecks to company growth.
- Places the costs for developing upgrades and staying current with technology on the supplier.
- Ensures that infrastructure knowledge will not become captive to only a few individuals.

Implications

- Might introduce conflicts with the business to live with some processes that might differ from what the company has done in the past.
- May have to be willing to forgo some functionality not deemed as necessary.
- Will need to establish guidelines for when custom solutions might become necessary.
- Will need to communicate cost and support implications if the business wants to move forward with a custom solution.

Guideline Example #60 – Service Design Organization

Principle Our people are our primary asset - we will motivate, develop and retain them.

Sample Application We will ensure that our people have up-to-date objectives and regular performance reviews. There will be opportunities for everyone to develop toward their personal and career aspirations.

Rationale

- Staff retention is much more cost-effective than staff recruitment.
- Business awareness is grown, not taught.
- No amount of documentation can replace experience.
- Motivated staff tends to be loyal staff.
- Personal development is key to motivation.

Implications

- Objective HR measures are in place.
- We understand what motivates our people.
- Staff development costs are understood.
- We increase performance management; we do not accept mediocrity.

Guideline Example #61 – Service Design Organization

Principle IT Configuration items will have identified owners, corporate and regional, responsible for their management, administration and accurate inventory and configuration information.

Sample Application Each configuration item type (e.g. server, pc, mainframe, SLA, policy, etc.) within the IT infrastructure has a named owner assigned to it responsible for its upkeep, inventory and configuration information.

Rationale

- Ensures no part of the IT infrastructure is operating with no one truly responsible for it.
- Quickly pinpoints who should be called in the event of an incident or problem.
- Easily identifies who needs to be consulted for changes and IT projects.

Implications

- Staff responsibilities will have to be assigned for each part of the IT infrastructure.
- Owner roles and responsibilities need to be clearly communicated.
- Owners must need to recognize that they have a substantial role in reviewing infrastructure changes and supporting incident and problem resolution activities.

Guideline Example #62 – Service Design Organization

Principle Those responsible for IT services need to be adequately trained with the right skills to do so.

Sample Application A skills profile is developed for each role that underpins IT services. Periodic audits are performed to ensure support staff has the appropriate skills for the roles they are responsible for. Deficiencies are resolved with additional training.

Rationale

- Cannot adequately support high quality services if resources do not have the skills to do so.
- Greatly increases the risks of service outages.
- Lack of needed skills and training creates low morale among support staff.
- Poor skills are easily seen by the business as a negative reflection of IT capabilities.

Implications

- Roles and responsibilities that underpin services need to be clearly defined.
- Skill profiles will need to be developed for each role.
- Staff will have to be continually assessed on their skills versus the roles they are responsible for.
- Training programs may need to be implemented, maintained and administered.

Guideline Example #63 – Service Design Organization

Guideline An organizational role will exist to provide IT service liaisons to every business unit.

Sample Application John Doe is the IT Service Liaison for the Sales and Manufacturing business units. In his role, he reviews the IT Service catalogue with key unit executives to communicate available services and obtain feedback for new services. He also manages provided services and acts as the first line of contact for resolving key service issues related to those business units. He also negotiates service targets and reviews service quality with unit executives once every month.

Rationale

- Provides a single point of contact to a business unit for all the IT services it is using.
- Increases customer satisfaction with IT services.
- Advocates business plans and objectives for IT to continuously improve and adapt their service offerings to business needs.
- Controls and simplifies communication between IT and the business units it serves.

Implications

- A business liaison role needs to be clearly defined and communicated.
- Investment needs to be made in assigning people resources to the IT Service Liaison role.
- Personnel assigned to the role are adequately authorized and supported.
- Accommodations need to be in place in the event a business unit does not like the liaison assigned to them.
