Achieving ITSM Excellence Through Availability Management

Technology Concepts and Business Considerations

Abstract
This white paper outlines the motivation behind Availability Management, and describes why it is the next logical step for an organization with relatively mature Service Support processes looking to take the next step toward IT service excellence. A practical, three-phase implementation approach is outlined, which emphasizes adequate planning and also the need for integration between multiple ITIL processes.

November 2009
# Table of Contents

**Executive summary** ........................................................................................................... 4
**Introduction** .......................................................................................................................... 4
  **Audience** ............................................................................................................................... 4
**Service support isn’t enough** ............................................................................................ 4
  **Advantages of a dedicated approach to Availability Management** .................................................. 4
**Implementing Availability Management** ............................................................................... 5
  **Three phases** .......................................................................................................................... 5
**Phase 1: Understanding business needs** ................................................................................. 6
  **Understanding services** ........................................................................................................ 7
  **Underpinning services and criticality** .................................................................................... 7
  **Mapping the infrastructure** .................................................................................................. 7
  **The Availability Plan** .......................................................................................................... 8
  **Ionix Service Manager’s Availability Framework** ..................................................................... 9
  **Periodic review** .................................................................................................................... 10
**Phase 2: Monitoring the environment** ..................................................................................... 10
  **Integration between processes is critical** ............................................................................. 10
  **Unplanned outages from Incident/Problem Management** ...................................................... 10
  **Planned outages from Change Management** ....................................................................... 11
  **Relationships between CIs and services in the CMDB** .......................................................... 11
**Phase 3: Seeking improvement** ............................................................................................... 13
  **Improve Service Desk efficiency** .......................................................................................... 13
  **Rework Change Management processes** ............................................................................. 13
  **Maintain the accuracy of the CMDB** .................................................................................... 13
  **Representation of the environment** ..................................................................................... 14
  **Interdependencies** ............................................................................................................. 14
  **Ionix Service Manager’s Federated CMDB** ......................................................................... 14
  **Review the plan** ................................................................................................................. 14
**Conclusion** ........................................................................................................................... 15
**References** ............................................................................................................................. 15
Executive summary
As organizations continue to improve their levels of ITIL maturity, it is natural that interest is increasing in ways to manage the availability of services more effectively. Availability Management is an ITIL Service Delivery process aimed at maximizing the likelihood that services will be available when customers demand them. The focus on ensuring availability of services brings significant benefits in terms of customer service and cost savings to the organization.

Introduction
This white paper outlines the motivation behind Availability Management, and describes why it is the next logical step for an organization with relatively mature Service Support processes looking to take the next step toward IT service excellence. A practical, three-phase implementation approach is outlined, which emphasizes adequate planning and also the need for integration between multiple ITIL processes.

Many of the examples in this white paper refer to EMC® Ionix™ Service Manager (formerly EMC Infra™.). Ionix Service Manager is a 100 percent web-based Service Management application, verified as ITIL compatible to Pink Elephant’s highest (Service Support Enhanced) level. This signifies Ionix Service Manager’s support for seven ITIL processes, including Availability Management. Ionix Service Manager is developed and supported by EMC.

Audience
This white paper is intended for IT Service Management (ITSM) professionals interested in planning and implementing Service Support processes, those with direct responsibility and interest in Availability Management, as well as ITSM managers overseeing the overall planning and implementation of frameworks and standards used to define and deliver IT infrastructure, processes, and activities as services that align with and enable business objectives.

Service support isn’t enough
A typical path to ITIL maturity involves an initial implementation of Incident Management, followed by Problem and Configuration Management, with the introduction of Change Management to standardize error control processes. A common element shared by these processes is a focus on the support of services, with the objective of reducing the number of incidents raised due to services not being available (or behaving in unexpected ways).\(^1\) Due to this common element these processes are grouped within ITIL as Service Support.

While Service Support is essential to a successful IT service management strategy, it is not a complete solution in itself. There are many situations when more focus should be placed on how readily available services are, rather than how quickly they can be made available when they become unavailable. Many organizations rely extensively on mission-critical applications that have clearly identifiable periods in which 100 percent availability is required. In these scenarios the availability of the application itself is the issue, not how effectively it is supported when it becomes unavailable. Strategies that focus upon the effectiveness of incident/problem resolution will therefore fall short of business requirements.

Advantages of a dedicated approach to Availability Management
Availability Management is defined under ITIL as follows: “Availability Management is concerned with the design, implementation, measurement and management of IT services to ensure the stated business

\(^1\) At higher levels of maturity some of the focus will shift to proactive approaches via Problem Management. However, even with relatively mature proactive Problem Management in place the primary motivator remains a desire to reduce both the number and impact of incidents that are logged against IT services.
requirements for availability are consistently met. Availability Management requires an understanding of the reasons why IT service failures occur and the time taken to resume service. Incident Management and Problem Management provide a key input to ensure the appropriate corrective actions are being progressed.²

While Service Support processes undeniably contribute indirectly to availability, the implementation of a dedicated Availability Management approach allows an organization to plan for, improve, and expand upon service availability itself. This brings advantages on three fronts:

- **Customer service.** While customers certainly benefit from improvements in support, an even better outcome is for services to work in the first place so the customer does not have to engage with the Service Desk at all. The availability of a service when it is needed is the primary concern of a customer, and having a set of processes clearly aligned to improving availability has a significant impact on customer satisfaction.

- **Cost effectiveness.** Due to constraints on resources, allocating staff and time to increase the availability of one service often requires that they be removed from another service. Availability Management, therefore, requires that resources be allocated according to service priority – the objective being the highest levels of service availability (as required by the customer) possible within budgetary constraints. Furthermore, because high availability means fewer incidents, the resource demands on the Service Desk are lowered considerably.

- **Reputation of IT.** A focus on availability can be viewed as a shift in focus from repairing services when they stop functioning, to ensuring that they remain functioning. This proactive approach can be viewed very positively by the organization and is an obvious departure from the reactive “firefighting” so often associated with IT.

**Implementing Availability Management**

Achieving effective Availability Management can be a daunting task. Availability Management requires input from Service Support processes to function – particularly Incident, Problem, and Configuration Management. This has two implications:

- A degree of ITIL maturity is required before attempting Availability Management.
- Availability Management software solutions require a high level of integration with components supporting other ITIL processes. Smooth integration between Availability Management and other ITIL processes – both from an operational and a software perspective – is critical, and must be a major focus of any implementation effort.

**Three phases**

This white paper advocates an approach to implementing Availability Management with a strong emphasis on aligning availability practices to the objectives of the business, while ensuring that other ITIL processes integrate effectively with Availability Management. This is realized in three distinct phases, which are summarized below and described in more detail in the following sections:

- **Phase 1: Understanding business needs.** Prior to addressing availability issues it is important to gain an understanding of the objectives of a business and the services that support these objectives. It is then possible to determine the services that should be prioritized to achieve optimal and realistic levels of availability. An element of this phase is often the development of Service Level Agreements (SLAs) on availability³. The key deliverable from this first phase is the production of an Availability Plan.

---

² *Achieving Best Practice with Service Desk Automation*, EMC white paper

³ It is not always necessary to implement a complete SLA immediately. Many organizations will initially develop Service Level Intentions (SLIs) – less formal statements of intended service levels that may be converted to full SLAs later. SLIs can, if desired, still be entered into automated Service Level Management tools, such as Ionix Service Manager’s SLM functionality.
- **Phase 2: Monitoring and gathering information.** Once a credible and realistic Availability Plan is established it will be possible to monitor performance against the plan. Availability performance monitoring involves input from several ITIL processes, and from specialized availability metrics and tools.

- **Phase 3: Seeking improvement.** At this point, the performance data gathered in Phase 2 is analyzed and areas of improvement are identified. The process for implementing availability improvements should be defined in the Availability Plan (and will likely interface with Change Management).

## Phase 1: Understanding business needs

IT departments enhance their value proposition considerably when their activities are aligned to business objectives. A key element in this alignment is a shift from defining IT infrastructure in terms of hardware and software components, toward an approach emphasizing the services provided by IT. Availability Management concerns itself with the degree to which services provided by IT are available to the business. Before availability targets can be set and prioritized, the needs and objectives of the business must be understood.

**Example**

Consider the following: A business runs an intranet service from a server that has a 2 percent chance of failure over 24 hours. If staff is available when there is a system failure, outages tend to average approximately one hour. When staff are unavailable, outages average around three hours, due to the fact that a support officer must be paged from home, travel to work, and then perform the necessary fix. This scenario would likely result in an availability profile similar to that displayed in Figure 1, with a reduction in availability outside of business hours.

![Mean % Uptime for Corporate Intranet Service](Image)

**Figure 1. Mean uptime for a corporate intranet service over the last 12 months**

The question is whether or not this availability profile is acceptable and it is here that an understanding of business needs is important. If no one is using the intranet outside of business hours, then a small drop in availability at those times is unlikely to be an issue; however, if the intranet performs a mission-critical function (such as providing access to a CRM application for a heavily sales-driven organization) and is accessed across multiple time zones, loss of availability may represent a significant issue for the business.
Understanding services
When determining a suitable availability profile we can be guided by consideration of cost to the business of failing to meet demand for a particular service. This cost is directly related to two main factors:

- How critical the service is in supporting particular business objectives
- The importance/priority of those objectives themselves

Underpinning services and criticality
A good understanding of both of these factors is important. It is often the case, however, that the relationship between services and business objectives is not a simple one-to-one mapping. Many services (for example, mail) underpin multiple business objectives. In these situations it is important to consider the most critical objective that a service supports in order to set the criticality of the service.

Demand
Real world data can be invaluable in validating assumptions drawn from analysis of business objectives. Patterns of demand can provide a useful early source of information into what services are actually being consumed by users and, by extension, are likely to have some importance for the business.

Obvious sources of demand-based data include access logs and network monitoring tools. Additional data (available to any IT department with incident management in place) can be sourced from incident patterns. Among the more than 100 standard reports that ship with Ionix Service Manager are several incident trend analysis reports. Figure 2 is taken from the Ionix Service Manager “Call Hourly Logging Rate” trend report, which details the mean number of calls logged against a particular Configuration Item (CI) by time of day. If incidents are being logged against a CI, this indicates that users are attempting to make use of that CI. This in turn indicates demand.

Figure 2. Example of a report detailing incidents logged against a CI by time of day
Some caution is warranted when drawing conclusions from incident statistics. If incidents are not being logged against a CI it may simply mean that the CI is functioning well – and is still in demand. Incident patterns, therefore, are most useful for comparing variations in demand for the same CI at specific times of day, rather than for making judgments about overall demand between different CIs.

Mapping the infrastructure
IT services do not exist in a vacuum – they are created, supported, and improved upon within the IT infrastructure. A service-oriented approach must therefore still maintain an underlying CI-based view; because CIs support services, our view of the infrastructure should include the CIs and CI interdependencies that support the services (this is the approach taken by Ionix Service Manager as shown in Figure 3).
Figure 3. Ionix Service Manager allows for availability tracking against both services and the CIs that underpin them

CI-to-service relationships are important
It is important to be aware that within a service-oriented architecture a strict one-to-one relationship may not exist between CIs and services. A service may, in many cases, be supported by many CIs (for example, a web farm). Similarly, a single CI may provide many services (for example, a server hosting a web server and a database). Each service failure may not be the direct result of a CI failure. Similarly, a CI failure may not result in a service failure. For this reason, it is good practice to track and set availability targets on both services and CIs.

Physical, organizational, and human resources
As well as having a good understanding of the IT infrastructure and its relationship to services, we must take stock of other factors that may or may not be recorded in the CMDB. These include:

- Staff skills
- Internal processes, particularly those employed to manage Requests for Change
- Organizational factors, such as siloing or turnover issues, which may impact upon the ability to support a service or CI

The Availability Plan
The Availability Plan is the final element in the business analysis process. At this point, the business objectives, service criticality, demand factors, and a deep understanding of the infrastructure are drawn together and availability targets set.
Ionix Service Manager’s Availability Framework

The Availability Framework within Ionix Service Manager provides an extremely useful structure for defining periods of availability, which maps directly to the capabilities of the tool. This provides users of Ionix Service Manager the opportunity to develop their Availability Plan in line with the framework, and ensures the plan can be implemented and automated successfully.

The Availability Framework divides availability broadly between Scheduled Availability (the plan) and Outages (the reality).

---

**Figure 4. Ionix Service Manager Availability Framework**

**Scheduled Availability**

Scheduled Availability refers to any period of time in which a CI or service is available. This may be further broken down to Availability Contracted and No Availability Contracted:

- **Availability Contracted** refers to times that the CI is under some agreement to be available at this time. Note that this does not necessarily mean it will be available the entire time – the agreement might state that it only needs to be available for a proportion of this time. Availability will be tracked during this period to ascertain whether the target availability is met.

- **No Availability Contracted** refers to times that the CI is not under any agreement to be available. While the CI may be available during this time, if it is for any reason unavailable the outage will not be counted in the availability targets for the CI.

During Scheduled Activity times planned activities occur such as backups, restarts, or maintenance. These planned activities would conflict with changes, so periods of scheduled activity constitute change blackouts. Scheduled Activity can occur during both contracted and non-contracted availability periods.

**Outages**

Outages refer to periods of time in which a CI or service is unavailable.

- **Planned Outages**, by definition, are outages that have been preplanned as part of a Change Management process. Within Ionix Service Manager, Planned Outages are raised from a Request for Change and managed using Ionix Service Manager’s workflow engine. Change windows can be associated with CIs or services, so that workflows that impact that CI or service can be scheduled to occur within an approximate change window.

- **Unplanned Outages** are periods during which CIs become unavailable unexpectedly. As with Planned Outages, this may occur during either a period of contracted or uncontracted Availability. Within Ionix Service Manager, Unplanned Outages are created as part of the Incident Management process.
Periodic review
The purpose of the Availability Plan is to drive improvements in availability outcomes; however, the value of the availability of a service is directly related to its criticality to the business. As business objectives change, the importance of particular services can change too. For this reason, the Availability Plan should be periodically reviewed to ensure that the assumptions it makes with regard to service priorities remain valid.

Phase 2: Monitoring the environment
The second phase in developing an Availability Management strategy is to gather information from the environment and ascertain how the infrastructure is actually performing in relation to the plan. While listed as a discrete project phase monitoring should be conducted as an ongoing process.

Integration between processes is critical
The Availability Plan, developed during the first phase, will make reference to relationships between ITIL processes at an organizational level. During the monitoring phase, these relationships take on an additional dimension as data is fed from various ITIL processes directly into availability statistics. It is at this point that software solutions that provide a high level of integration between processes can be highly advantageous, as they will automate the aggregation of data from a variety of sources, including:

- Unplanned outages raised from Incident and Problem Management
- Planned outages from Change Management
- Relationships between CIs and services to determine the impact of an individual outage

Unplanned outages from Incident/Problem Management
Incident Management is made aware of unplanned service outages, either as incidents are raised by customers, or via automated incident logging tools. This data can then be passed into a Configuration Management Database to collate availability data on individual CIs and the services supported by those CIs.

Tools that provide tight integration between Incident Management and the CMDB can automatically apply this outage information to CIs and (if the CMDB supports it) service records. Within Ionix Service Manager, for example, it is possible to set an outage against both the CI and the service supported by the CI when logging an incident (see Figure 5).

![Diagram](image)

Figure 5. Users can create an outage directly from the Incident screen within Infra
Problem Management identifies underlying errors in the IT infrastructure that are causing services to fail. Often, an incident is logged against a particular service or CIs, but subsequent analysis finds that the real source is an outage on a CI elsewhere in the infrastructure. This outage data can also be fed directly into the CMDB.

Planned outages from Change Management
Change Management workflows often require that a CI (or service) be temporarily taken offline, resulting in planned outages. Because they can be anticipated, the impact of planned outages is generally lower in comparison to those that are unplanned; however, planned outages still impact upon availability. They should therefore be fed into availability statistics.

To automate the relationship between Change and Availability Management, Ionix Service Manager allows CIs and services to be linked to workflows and automatically updated as the workflow proceeds. Changes made to CIs as Change Management workflows proceed are immediately reflected both in the CMDB and availability metrics.

Figure 6. Change Management workflows should ensure that changes to CI availability arising from change processes are reflected in the CMDB

Relationships between CIs and services in the CMDB
Up to this point we have described the CMDB in terms of its ability to collate data from outages (planned and unplanned) against individual CIs or services for use in Availability Management monitoring (see Figure 7). However, this is only part of the role that a CMDB plays in availability monitoring.
Figure 7. The CMDB links Availability Management to Incident and Change Management

In addition to tracking data on individual CIs, an effective CMDB will maintain representations of relationships and dependencies between CIs (see Figure 8). This dependency information provides an understanding of the effects that an outage on one CI will have on the rest of the IT environment. Within Ionix Service Manager, for example, as outages are logged against CIs (either from Incident, Problem or Change Management) they can be cascaded to dependent CIs or services. This presents a realistic picture of the impact of an outage and, correspondingly, accurate reliability data.

Figure 8. The Ionix Service Manager CMDB represents not only CIs, but also their relationships and linkages
Phase 3: Seeking improvement

Once we have set our availability targets in line with business objectives and monitored our performance against those targets, the next step is to seek necessary improvement against availability targets. The initial response to availability issues is often to address the physical infrastructure, and sometimes replacing a faulty router is the correct course of action. It is important to remember, however, that IT environments depend upon a complex interplay between technology and human factors. The following are examples of non-hardware related improvements that yield improvements in availability performance:

- Improve Service Desk efficiency
- Rework Change Management processes
- Maintain the accuracy of the CMDB

Improve Service Desk efficiency

The amount of time that it takes the Service Desk to provide a workaround in response to incidents directly impacts upon availability performance. The longer it takes a Service Desk to develop a workaround, the longer an outage will last, increasing the likelihood of a service level breach. Many factors can affect the ability of the Service Desk to provide effective workarounds, such as:

- **Staffing and skill levels.** A Service Desk needs to be staffed adequately and supplied with the necessary training.
- **Staff turnover.** High turnover Service Desks have to devote more resources to training new staff and can therefore allocate fewer resources to maintaining services.
- **A Knowledge Management strategy** ensures that previous solutions can be reused to resolve incidents faster and mitigate the effects of staff turnover.
- **Communication from customers.** Having a strategy in place to ensure that customers adequately describe their issues the first time they contact the Service Desk can greatly reduce the time to resolution.

Rework Change Management processes

Change Management processes often involve a planned outage on a CI or service. Excessively lengthy or complex change processes may result in unnecessarily lengthy outages, impacting negatively on availability. Issues to consider in relation to this include:

- **Efficiency of change processes.** Processes can, in many cases, be refined and simplified. The fewer steps and decisions that are required to make a change, the faster the change will occur. Simpler change processes also reduce the potential for error and are more likely to be followed (driving compliance).
- **Compliance** with Change Management processes ensures that changes are visible, standardized, and easier to roll back should issues arise that affect availability.
- **Relationship with CMDB.** Change Management workflows must update the status of the CIs they affect so that accurate availability data can be gathered. Providing links into the CMDB also allows for accurate risk assessments to be performed against the CIs affected by changes.

Maintain the accuracy of the CMDB

The CMDB acts as a central source for availability data, and also as a key component in Incident, Problem, and Change Management. An inaccurate CMDB is particularly damaging to Availability Management efforts because it provides inaccurate data while simultaneously hindering Service Support efforts.
Representation of the environment
Out-of-date or inaccurate data undermines the CMDB’s status as the definitive representation of the IT environment. The status of a CI must reflect its real-world status for outage tracking to have any meaning. As CI statuses change in the real world, these changes must be reflected in an updated CMDB.

Interdependencies
The statuses of individual CIs are not the only aspect of a CMDB that is subject to change. As the IT environment evolves the interdependencies between CIs themselves, the relations that CIs have with services can also change.

These interdependencies need to be accurate so that the CMDB is capable of realistic impact analysis. Poor representation of impact can have potentially damaging consequences, both for the accuracy of availability data itself, and also for Problem Management activities that may otherwise drive improvements in availability.

Ionix Service Manager's Federated CMDB
Keeping a traditional CMDB up to date (particularly in a rapidly changing environment) can be extremely resource-intensive. Ionix Service Manager addresses this through the implementation of a Federated CMDB, in which data from the IT environment is captured by automated monitoring tools, and integrated into the CMDB. As the environment changes, the CMDB is automatically updated, ensuring an accurate representation is maintained. This has a positive flow on benefits for Availability Management, as CI statuses and interdependencies can be automatically factored into availability data.

Review the plan
Finally, it is important that the Availability Plan itself is an element in the improvement cycle. The Availability Plan is a function of the objectives of the business and the way that IT services are provided and aligned to those objectives. It is important to regularly revise the plan in light of the following:

- Changes in the business objectives
- Shifts in demand for services
- Changes in technology and processes that alter the ways that services are provided
Conclusion

Availability Management offers organizations solid benefits in customer service and cost effectiveness. It represents an opportunity for an IT department to adopt a positive approach centered upon providing services when people need them, rather than just supporting services when things go wrong.

While a degree of ITIL maturity is undoubtedly required, Availability Management should be of interest to organizations at all levels of maturity. Availability is a highly effective end goal as it provides a roadmap for how ITIL processes should be organized and integrated. Indeed, it is this integration between ITIL processes that is the key to effective Availability Management. The three-phase plan outlined in this white paper serves to illustrate this, with inputs from multiple ITIL sources forming the basis of the planning, monitoring, and improvement phases. The importance of tight integration between ITIL processes is a key consideration when selecting a software solution. Solutions such as Ionix Service Manager that provide end-to-end, out-of-the-box integration between ITIL processes will provide significant benefits.

References

For further information please contact your local Ionix Service Manager office:

**Europe**
Phone: +44 (0)870 608 7777  
Fax: +44 (0)208 758 6013  
www.infra.co.uk

**USA**
Phone: +1 562 384 5200  
Fax: +1 562 384 5201  
www.infra-corp.com

**Asia Pacific**
Phone: +61 2 8908 7100  
Fax: +61 2 8908 7199  
www.infra.com.au