

**What to Look for in  
Mission-Critical Managed IT Services**

*What's your exposure to losing  
business capability?*

## Executive Summary

The choices from many reputable suppliers of IT managed services can appear very much alike. Yet when you have a mission-critical business process whose function must not be interrupted, you know your requirements call for something above and beyond. This paper serves as a field guide to help you identify key characteristics that set a critical managed IT service apart from even highly capable general-purpose offerings.

The discussion begins with a look at the circumstances that call for this special breed of managed service. One or more signature attributes typically identify a mission-critical capability or process that is core to the business:

- **High volume of transactions**
- **Transactions of a high value or vital nature**
- **Time-sensitive processes**
- **Virtually no tolerance for data loss**

More than any other characteristic, mission-critical managed IT services are defined by the principle that preserving business capability comes first. **Such critical managed services strive to achieve around “five nines” of availability, or 99.999% (less than 5 minutes of downtime) as opposed to conventional managed services that aim for perhaps 99% (87 hours and 36 minutes) of downtime annually.**

With that perspective in mind, four markers that distinguish mission-critical managed services will be explained:

- The importance of the **business impact analysis (BIA)** in assessing risk and determining appropriate recovery point (RPO) and recovery time objectives (RTO), business continuity (BC) measures and disaster recovery (DR) protection
- A **preventive and predictive service design** that minimizes costs and exposures identified in the BIA by protecting against failures and exposure, rather than recovering only after the business capability has been adversely affected
- **Service level agreement (SLA) metrics** that put *business capability* first (percentage of the time the critical business capability or process operates at full performance), followed by *availability capability* (percentage of the time the business capability functions with its redundancy and failover components intact)
- A **“Continuity Gene”** that flows through team members, who are specialists in the mission-critical domain; work in a do-whatever-it-takes mode; are adaptable to your organization’s key business capabilities and processes; and prepared to co-exist with traditional managed service providers

## When Do You Need Mission-Critical Managed Services?

The directive of a mission-critical managed IT service is to make sure an essential business function — or functions — will operate how, when and where needed. (As related to IT, a business capability spans the technology, the processes and the people necessary to keep a business function running. Any one business capability may depend on a number of business processes.)

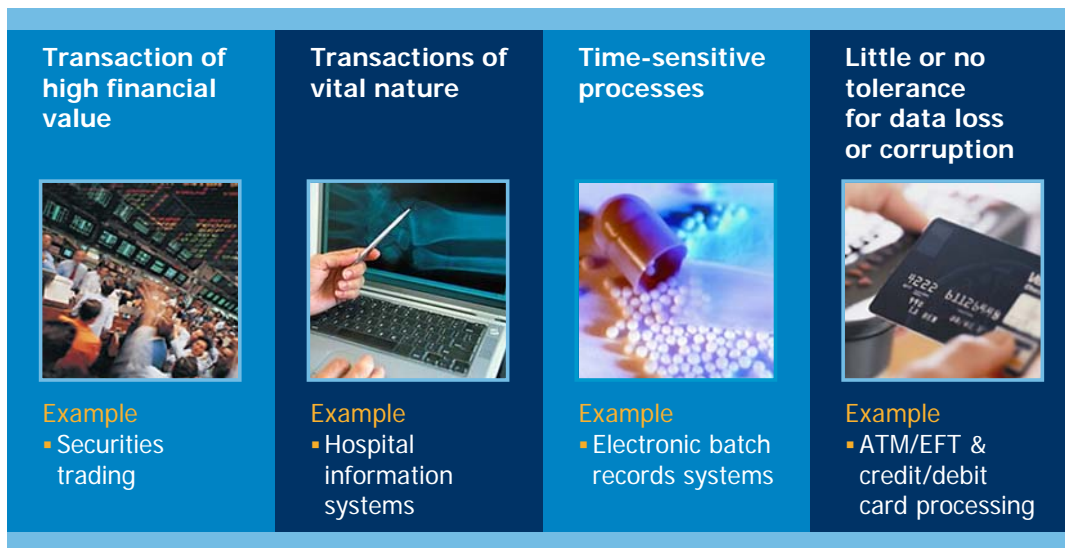
Perhaps more than any other single characteristic, mission-critical managed IT services are defined by this guiding principle: Business capability is not everything; but it's the most important thing. All other concerns are secondary to preserving business capability.

What types of situations warrant mission-critical managed services? The business capabilities and processes involved will be core to *your* business. For example, while payroll processing is necessary in all organizations, it's nothing less than a lifeblood function for a payroll-processing service bureau.

In contrast, losing access to a general or administrative function for a half an hour may be inconvenient, but your business is still able to continue when such functions are offline or if they operate at reduced capacity on occasion. Therefore these sorts of tasks would not fall under the umbrella of a mission-critical managed service.

In Stratus Technologies' almost three decades of providing continuously available servers and services that enable the world's most demanding IT environments, we have observed that mission-critical settings are identifiable by one or more signature attributes. These include high transaction volumes, transactions of a high value or vital nature, time-sensitive processes and virtually no tolerance for data loss.

**Figure 1: Attributes of a Mission-Critical Environment**



*The consequences can be severe when an essential business process is impaired or unavailable: millions of dollars can be lost and lives may be in peril.*

For business capabilities and processes where these attributes are present, protecting the interests of stakeholders dictates more rigorous practices than average. For non-mission-critical functions, for instance, pushing out certain software updates to the corporate environment without extensive pre-testing may be the typical procedure. When a critical business function is involved, it becomes imperative to first verify that any software update will not precipitate downtime or degrade service.

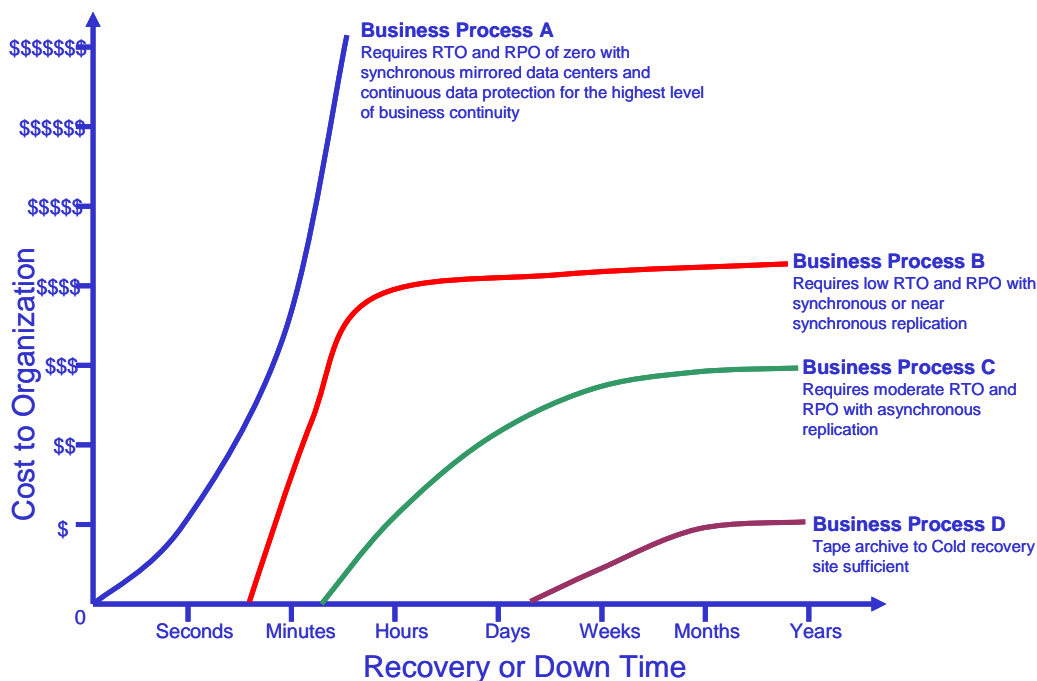
A current evaluation of critical business capabilities is the first step in understanding exactly what is at stake, identifying risks and designing an IT managed service that is capable of providing the right level of protection for the business capability at an appropriate cost.

### The Role of the BIA

Because mission-critical managed IT services exist for the express purpose of ensuring business capability, they are based on a business impact analysis (BIA) that assesses the direct and indirect effects if a vital capability were to be impaired. The BIA will identify the key technology, process and people elements that support the business capability, including all the dependencies involved. Situation-specific factors, including peak periods of activity and time-sensitive processing, are taken into account.

That BIA then drives decisions including which recovery point (RPO) and recovery time objectives (RTO) are suitable, and the extent to which business continuity (BC) and disaster recovery (DR) elements should be put in place.

**Figure 2: Business Impact Analysis Dynamics**



Source: Burton Group. *Building a Business Impact Analysis: The Keystone to Effective Business Continuity Planning*. Richard Jones, v1, July 30, 2008.

### Business Impacts

Financial loss and damage to brand reputation are among the consequences when a vital business process is hindered or unavailable. A credit/debit card authorization processor, for instance, could expect to lose tens of thousands of dollars per minute during an outage. Afterward, its cardholder customers could also decide to use another card with better reliability.

Some businesses are in addition bound by regulations that mandate complete and auditable data, which makes any data loss a serious concern. A pharmaceutical company cannot afford gaps in the data related to manufacturing a prescription drug, or risk having to destroy a batch of product valued at millions.

The essential nature of the business capabilities they ensure mean that mission-critical IT managed services strive to achieve around “five nines” of availability, or 99.999%, or 5 minutes of downtime annually which is known as continuous availability. A typical availability target for general-purpose managed services would be in the range of 99%, or 87 hours and 36 minutes of downtime annually.

The following table shows the difference in the availability that each incremental nine signifies to the business capability. For instance, about 99% availability may appear acceptable without a BIA that sets the proper context. More than 87 hours of annual downtime would be unacceptable for the trading capability of an international stock exchange, a service capability of a telecommunications provider or the dispatch capability of an emergency medical services organization.

**Figure 3: Availability by the Numbers**

Availability Level	Average Yearly Downtime
99%	87 hours, 36 minutes
99.9%	8 hours, 46 minutes
99.95%	4 hours, 23 minutes
99.99%	~52 minutes
99.999%	~5 minutes
99.9999%	~32 seconds

*Each additional nine of availability represents a measurable difference that has an impact on the business capability.*

Given that IT has become inseparable from essential business capabilities and processes today, an up-to-date BIA can be an eye opener even for experienced organizations that may not have taken the time to assess the impact of a business capability since it was first rolled out. A formerly non-mission-critical capability or process may have expanded to a scope that turns it into a heartbeat function.

## **Predictive and Preventive Design**

Mission-critical managed IT services are grounded in the same best practices and governance principles — such as those defined by ITIL®, COBIT®, Six Sigma® and ISO 9001 — that have been adopted by the best of their general-purpose counterparts. IT monitoring capabilities and automation tools are also part of the package for keeping watch over the health of the relevant systems and networks.

The difference is that while building on these frameworks and tools, the BIAs for vital business capabilities prescribe that mission-critical managed services have to use predictive and preventive measures beyond the norm.

Let's assume a business impact analysis indicates an RTO for a capability approaching zero and its RPO permits virtually no transaction loss. In this situation quickly restarting servers or redirecting network traffic after a failure has happened is not good enough. Higher levels of prediction and prevention must be planned into the managed service design.

For example, a disk drive whose block error rate starts creeping up is likely to crash. Under most circumstances, having duplicate hardware in place to ride through the failure without interruption would provide ample protection. But a company with an extremely high-volume transaction load may opt against being exposed to the remote possibility of two disks failing at the same time. Keeping full redundancy intact becomes important in this particular case, so engineers would monitor for errors to proactively replace an ailing disk before the component in question has a chance to fail.

Mission-critical managed services don't only attend to the "hard" areas of vulnerability that involve technology components. Like more general IT managed services, they also address "soft" areas where people and human interaction come into play: policies and procedures. The distinction is that critical managed services must be more stringent in these areas.

Change management is a prime example. Having testing and back-out procedures in place before implementing a hardware or a software change is part of the playbook for many IT environments, not just critical ones. However, a round or two of testing will not suffice when business capability could be devastated by a glitch.

Risk-appropriate change management may demand multiple levels of testing outside of the production environment to reveal potential problems and uncover hidden interdependencies over a period of time. Then load testing may be called for to simulate how the change will behave under a production workload. After the change is fully validated and deemed ready for production, traffic may need to be transferred to an alternate processing path so that users will not be affected while the primary resources are upgraded.

## **SLA Metrics and Priorities**

We have said that ensuring business capability takes precedence in a mission-critical managed service. As a result, the most important measurement is the percentage of the time the critical business capability or process is operating at full performance.

The second most important measure is availability capability, which is the percentage of the time the business capability is functioning with all redundancy and failover components intact. The managed service architecture may be designed to fail over so that users are unaffected in the event

of a single outage, or even if an entire data center goes offline. Such conditions might still breach a service level agreement (SLA) because the failsafe protection will be at less than 100%.

By keeping the focus on business capability and availability capability, mission-critical managed services ensure that attention is paid to meaningful results. Significant incidents and conditions do not get lost in a fog of minor issues that pose little or no consequence.

Other key performance indicators (KPIs) are still relevant although secondary to the first two metrics. Examples of other non-critical KPIs include properly documenting incident management, how long it takes to respond to a user request, following agreed-upon approval processes, providing timely reporting and the like.

Overall, the KPIs will be stricter than in general-purpose managed services. Example: A critical managed service provider could be obligated to meet an SLA that specifies 15-minute resolution for a Severity 1 problem; the Severity 1 time-to-resolution under a general-purpose service might be four hours.

### **The “Continuity Gene”**

The human factor in managed services is a make-or-break aspect that should not be underestimated. A services provider with core competency in the mission-critical domain ought to demonstrate a focus on maintaining business capability.

A provider with mission-critical DNA will grasp the significance of adapting to your key business capabilities and processes instead of insisting you conform to them. For example, expect them to be willing to interface to your existing internal systems as required for effective service delivery. Having identified as specialists, they should be prepared to co-exist with broad-based traditional managed service providers as well. Where necessary and reasonable the co-existence may entail integration with the trouble ticketing, change management and service request mechanisms already present in your environment.

Team members have the mindset, the discipline, the attention to detail the job requires. A do-whatever-it-takes attitude will be prevalent. Their experience and orientation will not be the same as technical generalists, who perhaps have administered internal systems that can withstand being down for a few hours while being restored from a backup tape.

Continuous improvement is a major emphasis, unlike more general offerings where meeting the SLAs is success in itself. The end-to-end performance of the environment will be examined. Is everything healthy? Could things be better? Could network latency be a threat? Performance statistics will also be archived and analyzed for trends and thresholds.

**Figure 4: Comparing Non-Critical and Critical IT Managed Services**

Characteristic	General-Purpose Emphasis	Mission-Critical Emphasis
<b>Business process domain</b>	<ul style="list-style-type: none"> <li>Includes general and administrative capabilities</li> </ul>	<ul style="list-style-type: none"> <li>Dedicated focus on core business capabilities and processes</li> </ul>
<b>Recovery time objective/ Recovery point objective</b>	<ul style="list-style-type: none"> <li>RTO of hours may be acceptable; RPO may allow in-process transactions to be backed out</li> </ul>	<ul style="list-style-type: none"> <li>As determined by the business impact analysis, RTO may approach zero; RPO may specify that data loss is unacceptable</li> </ul>
<b>Uptime objective</b>	<ul style="list-style-type: none"> <li>In the 99% range</li> </ul>	<ul style="list-style-type: none"> <li>99.999% or greater</li> </ul>
<b>Problem resolution emphasis</b>	<ul style="list-style-type: none"> <li>Quick recovery; break/fix</li> </ul>	<ul style="list-style-type: none"> <li>Preventive, predictive</li> </ul>
<b>Principal service delivery metrics</b>	<ul style="list-style-type: none"> <li>Range of KPIs</li> </ul>	<ul style="list-style-type: none"> <li>Business capability is first</li> <li>Availability capability is second</li> <li>Then other KPIs</li> </ul>
<b>Service delivery approach</b>	<ul style="list-style-type: none"> <li>One-size-fits-all orientation; may require customer to adapt to service provider's preferred tools and systems</li> </ul>	<ul style="list-style-type: none"> <li>Oriented to adapt to existing business processes as well as tools and systems already in place; co-existence with other managed service providers</li> </ul>
<b>IT support coverage</b>	<ul style="list-style-type: none"> <li>Typically during business hours</li> </ul>	<ul style="list-style-type: none"> <li>24/7, follow-the-sun support to provide seamless global coverage</li> </ul>
<b>Focus on continuous improvement</b>	<ul style="list-style-type: none"> <li>Meeting SLAs is sufficient</li> </ul>	<ul style="list-style-type: none"> <li>Continuous improvement approach augments SLAs to ensure business capability and availability capability goals are met long-term</li> </ul>

*Non-critical managed services and services that are hardwired to sustain business capability may appear roughly similar, but have a different emphasis that becomes evident in their characteristics.*

## Conclusion

Most IT managed services may appear to be birds of a feather, but on closer evaluation the mission-critical services will distinguish themselves as a breed apart. Look deeper for must-have traits from your IT managed service provider to make sure the availability and performance you need will be ensured by design. Start with a business impact analysis to bring essential capabilities and processes into focus, and to specify a risk-appropriate, cost-effective managed service architecture that fits your specific situation.

## About Stratus Technologies

Stratus Technologies focuses exclusively on helping its customers keep critical business operations online without interruption. Business continuity requires resiliency and superior availability throughout the IT infrastructure, including virtual environments. Stratus delivers a range of solutions that includes software-based high availability, fault-tolerant servers, availability consulting and assessment, and remote systems management services. Based on its 28 years of expertise in product and services technology for total availability, Stratus is a trusted solutions provider to customers in manufacturing, health care, financial services, public safety, transportation & logistics, and other industries. **For more information, visit [www.stratus.com](http://www.stratus.com).**

Specifications and descriptions are summary in nature and subject to change without notice.

Stratus is a registered trademark and the Stratus Technologies logo is a trademark of Stratus Technologies Bermuda Ltd. ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office. Six Sigma is a registered trademark of Motorola, Inc. COBIT is a registered trademark of the IT Governance Institute. All other trademarks and registered trademarks are the property of their respective holders.

© 2008 Stratus Technologies Bermuda Ltd. All rights reserved.  
X977