Safe Systems

Disaster Recovery & Strategic Planning: How alignment can reduce risk and cost

Thomas Hinkel, Director of Compliance

Introduction

If it's been done correctly, your business continuity program has been developed to support your Banks' strategic plan. The capabilities of your hardware and software have been carefully selected to coincide with the needs of your target market. Your financial projections are based on your ability to successfully penetrate your target market, and your DR program provides assurance that your critical business processes will continue functioning to serve your customers in the event of a disaster. In short, the objectives of your strategic plan should be reflected in the priorities of your DR plan (specifically in the business impact analysis and the risk assessment phases), and your recovery procedures will assure process recovery within the pre-defined limits.

The Challenge

In the real world, things are rarely in perfect alignment. More often than not strategic planning, DR planning, and recovery procedures are mutually exclusive exercises that only converge coincidentally. But, there are three reasons why you might want to want to revisit these three concepts with an eye towards bringing them into alignment with one another.

Overview

Although the prospect may seem daunting, there are three compelling reasons why you should consider re-visiting your existing policies and procedures with an eye towards aligning your strategic plan with your disaster recovery program and its recovery procedures:

- Regulatory Overlap
- Cost Efficiency
- Risk Reduction

Details

Regulatory Overlap:

According to the FFIEC Audit Handbook,

> *"The board or its audit committee should be aware of, and understand, significant risks and control issues associated with the institution's operations, including risks in new products, emerging technologies, information systems, and electronic banking. Control issues and risks associated with reliance on technology can include…*
>
> - *Inadequate alignment between IT systems and business objectives,*
> - *Ineffective or inadequate business continuity plans, and*

- *Financial losses and loss of reputation related to systems outage.[1]"*

Similarly, the FFIEC Business Continuity Planning Handbook states when addressing the importance of the business impact analysis:

> *"This phase may initially prioritize business processes based on their importance to the institution's achievement of strategic goals and the maintenance of safe and sound practices.[2]"*

And,

> *"The BCP should be based on the size and complexity of the institution and should be consistent with the financial institution's overall business strategy.[3]"*

So proper audit procedure of technology requires consideration of business continuity, and business continuity planning requires consideration of strategic goals and objectives. But perhaps the most compelling reason comes from the most recent FDIC Winter 2009 Supervisory Insights newsletter, in an article titled "Customer Information Risk Assessments: Moving Toward Enterprise-wide Assessments of Business Risk". Although information security risk assessments are the current focus of regulators, there is a clear trend towards enterprise-wide assessments of business risk, which:

> *"…represent a significant opportunity for financial institutions to gain material benefits and economies from their risk assessment methodologies.[4]"*

Guidance on this approach remains formative, but key steps include:

1. Identifying enterprise risks that may affect the institution (typically performed by senior management or the Board of Directors who own the risk).

2. Defining business processes that drive enterprise risks.

3. Assessing business process risks.

4. Linking technology to the business processes (e.g., identifying threats, vulnerabilities, impacts, and controls) and focusing efforts on higher risks that support the business process, and

5. Developing plans and strategies to further manage business risks and mitigate risks that are outside approved tolerances.

For anyone who has completed the Business Impact Analysis, the Risk Assessment and the Risk Management phases of their DR program, the first four steps should look very familiar. There is an almost step-by-step correlation between the risk management process defined by the DR/BCP

[1] FFIEC IT Examination Handbook, Audit Booklet – August 2003, page 5
[2] FFIEC IT Examination Handbook, Business Continuity Planning Booklet - March 2008, pp 9-10
[3] Ibid, page 2
[4] FDIC, Supervisory Insights Winter 2009, page 29

guidance, and the new enterprise-wide business risk assessment. Aligning your overall strategic business plan with an enterprise-wide risk assessment and a risk-based business continuity program will assure that all areas are properly addressed, and can keep you ahead of changes in regulatory guidance.

COST EFFICIENCY:

From initial policy development, to prioritization of process recovery, to resource allocation, aligning your strategic plan with your BCP can result in real world cost efficiencies. First, it stands to reason that coordination between policies will result in fewer man-hour resources expended on policy development. The strategic plan identifies overall goals and priorities, the priorities are carried forward to the BCP as critical processes and their interdependencies, and recovery procedures assure recovery and resumption of the process. Alignment means more carryover from policy to procedure to practice, because you're not starting from scratch every time.

But the real cost savings are found in the implementation of your recovery procedures. For example, most institutions address the need for redundancy in their critical IT infrastructure by stocking spare hardware. Duplicate servers, workstations, routers and firewalls are purchased and kept on standby to be quickly configured and deployed in the event of a disaster. But hardware obsolescence, particularly in servers and workstations, may make quick deployment questionable, or even doubtful. According to the FFIEC,

> *"…recovery time objectives (RTO's) are now much shorter than they were a few years ago, and for some institution, RTO's are based on hours and even minutes.[5]"*

Rebuilding a server from a cold spare to full functionality can easily take 24 – 36 hours, possibly exceeding your RTO for the business process for which the server is a critical component. What is the cost, not just financial, but reputation and strategic cost, if your critical business processes don't come back online in time? At that point there are only two options; enhance your recovery capability, or increase your recovery time objectives. The former option requires an additional resource commitment, and the latter requires you to re-visit your strategic plan and your business impact analysis, and that requires board and senior management approval. Cost savings can be realized in "hard" dollars, by not stocking hardware that in the end might not meet your recovery objectives, and/or in "soft" dollars by expending fewer scarce personnel resources.

RISK REDUCTION:

For institutions serviced by a core provider, operational risk (also referred to as transactional risk) is the biggest concern because it manifests itself in virtually every process involved in the delivery of institution's products or services. Operational risk not only includes operations and transaction processing, but also areas such as customer service, systems development and support, internal control processes, and capacity planning. Operational risk also may affect other risks such as credit, interest rate, compliance, liquidity, price, strategic or reputation. In an

[5] FFIEC IT Examination Handbook, Business Continuity Planning Booklet - March 2008, page 2

evaluation of the interdependencies of your critical business processes, chances are critical service providers are at or near the top for risk remediation. According to the FFIEC:

> *"Examiners also should explain how the (service provider's) deficiencies increase the risk to the serviced institutions. For example, inadequate business resumption plans at the TSP may increase the transaction and reputation risks at serviced institutions.*[6]*"*

Although the operational details of a third party provider may be outside your direct control, it is not outside your responsibility to address them and to apply mitigating controls as far down the process delivery chain as you can. Residual risk acceptance is the final step in the risk management process, not the first. Incorporating specific recovery procedures for your critical core providers in your BCP will provide assurance that management recognizes their strategic importance to the institution, and has properly identified and addressed the risks.

CONCLUSION:

Financial institution management should incorporate business continuity considerations into the overall design of its business model from the top down in order to mitigate the risk of service disruptions, and support their strategic plan. Allocating sufficient resources to this task is the responsibility of the Board and senior management. Designing redundancy into your critical business processes is one way to greatly enhance your recovery ability, while at the same time supporting the objectives of your strategic plan.

Safe Systems has a full complement of products and services to address all of your business continuity challenges. From DR plan development and testing, to hosted services, facilities, and core communications, we can enhance your ability to meet the expectations of the Board, your customers, and the regulators.

ABOUT THE AUTHOR

Tom Hinkel, Director of Compliance, is responsible for ensuring that Safe Systems' services incorporate and abide by appropriate financial industry regulations and best practices. In this position, Hinkel works closely with R&D, Product Management, and Operations Managers to ensure that new and existing services comply with FFIEC standards. Most importantly, by staying current on regulatory issues facing financial institutions, Hinkel serves as a regulatory compliance resource for Safe Systems' customers. With over fifteen years experience, initially on the engineering side installing and supporting bank networks and later in IT regulatory compliance, Hinkel's areas of expertise spans the entire spectrum of information technology. He has served on the inside as Manager of Information Systems, as well as Information Security Officer, and as an independent consultant for banks of all sizes from denovo to $1B+. Hinkel has been with Safe Systems, Inc. since 2005, most recently as an Account Manager. Hinkel holds a Bachelor of Arts degree from Illinois Wesleyan University, an Associate of Arts degree in

[6] FFIEC IT Examination Handbook, Supervision of Technology Service Providers – March 2003, page 5

computer programming, the GSEC security certification from the SANS Institute, and is currently studying towards the Certified Information Systems Auditor designation.

ABOUT SAFE SYSTEMS, INC.

Founded in 1993, Safe Systems is the national leader in providing compliance-centric IT solutions exclusively to financial institutions. As a technology partner, and recent winner of the MSP Best in Class Award by CompTIA and MSP Partners, Safe Systems has worked with over 500 financial institutions and manages over 16,000 network devices nationwide. Safe Systems' scalable and cost effective solutions include IT managed services, compliance solutions, business continuity and disaster recovery, network design and installation, security services, and IT and compliance training. Safe Systems helps financial institutions to significantly decrease costs, increase revenues, and improve performance. For additional information about Safe Systems, Inc., please visit www.safesystems.com or call 877.752.0550.