

BITS

FINANCIAL SERVICES
R O U N D T A B L E

BITS GUIDE TO BUSINESS-CRITICAL TELECOMMUNICATIONS SERVICES

BITS
1001 PENNSYLVANIA AVENUE, NW
SUITE 500 SOUTH
WASHINGTON, DC 20004
202-289-4322
WWW.BITSINFO.ORG

TABLE OF CONTENTS

I. Executive Summary	3
II. Risks, Requirements and Strategies	6
III. Recovery Tools and Processes.....	23
IV. Due Diligence.....	26
V. Contracts.....	30
VI. Ongoing Relationship Management: Testing, Monitoring and Auditing.....	34
VII. Concluding Recommendations	36
Appendices	
Appendix A: Glossary	37
Appendix B: Acknowledgements and References	40
Appendix C: Alternative/Emerging Technologies and Alternate Transport Mechanisms.....	43
Appendix D: Recovery Processes of Telecommunications Companies	47
Appendix E: Consolidated List of Key Questions for Risk Managers.....	50

I. EXECUTIVE SUMMARY

The *BITS Guide to Business-Critical Telecommunications Services* provides financial institutions with industry business practices for understanding and managing risks associated with essential telecommunications services. It is written primarily to guide business managers, continuity planners and other risk managers—from CEOs to procurement experts—as they analyze risks, conduct due diligence, contract for telecommunications services and integrate evolving regulatory requirements into business continuity plans.¹

This document highlights key considerations and poses questions business continuity planners and other risk managers should ask themselves and their service providers, taking into account regulatory requirements and changes in the marketplace. Each section of the document begins with a set of questions. The full list of questions is also included in Appendix C. These questions are a starting point for a rigorous examination of a financial institution's business continuity strategy for telecommunications needs and they serve as considerations in procuring adequate levels of service from telecommunications service providers. While this document provides background information and references to other resources, it does not (nor is it intended to) answer these questions. However, answering these questions will help individual financial institutions achieve the necessary levels of diversity, recoverability, redundancy and resiliency of critical telecommunications services.

Shortly after the September 11, 2001 attacks, the financial services industry, through BITS and other organizations, set out to mitigate unacceptable risks by engaging the telecommunications industry in dialogue on how best to assure sufficient levels of diversity, recoverability, redundancy and resiliency from its telecommunications service providers. This took place in the context of financial institutions reviewing their business continuity plans to reflect the heightened risks posed by terrorism and evolving regulatory requirements. The *BITS Guide to Business-Critical Telecommunications Services* is the culmination of this dialogue. This document supplements the *BITS Framework for Managing Technology Risk for IT Service Provider Relationships* (“*Framework*”).²

Telecommunications resiliency and its components—diversity, recoverability and redundancy—are critical to financial institutions, their customers and the U.S. economy. Events like 9/11 and the 2003 Northeast blackout, which affected key portions of the U.S. financial services industry, demonstrate the financial sector's dependence on the telecommunications sector.

Prior to 9/11, many in the financial services industry assumed that:

- Circuit diversity is achieved through the use of multiple carriers.
- Switched services in general, such as frame relay, inherently provide resiliency.
- More circuits mean more resilience.
- The Internet³ is inherently less reliable than telecommunications services.
- Diversity can be ordered as a contracted service.
- Internet Protocol (IP)-based services are not inherently reliable.

¹ This document is intended only to provide suggestions on business objectives, not to provide legal advice. An appropriate legal professional should be engaged to provide such advice on a case-by-case basis.

² The *BITS Framework for Managing Technology Risk for IT Service Provider Relationships* guides financial institutions in managing risk in all IT outsourcing relationships. See the BITS website for details on the *Framework*: <http://www.bitsinfo.org/bits2003framework.pdf>.

³ The term “Internet” in this paper refers to the public Internet that connects computer networks and facilities around the world.

Since 9/11, many in the financial services industry and government have learned that more realistic assumptions are:

- Circuit diversity cannot be assumed when ordered from two different carriers.
- Frame relay is shared among carriers and this raises concerns about diversity.
- Diversity remains an issue between the financial institution premises and the telecommunications point of presence (“last mile”).
- The Internet worked very well during 9/11 for messaging.
- Diversity must be engineered and means different things to different carriers and customers.
- More small circuits require more effort to monitor than a few larger ones.
- IP-based services can offer advantages.
- Means other than just diversity of redundant circuits can assure resiliency of the function they must support, such as Synchronous Optical Network (SONET) and proprietary service offerings.
- One can expect to pay more for telecommunications services that are specifically engineered (e.g., specialized versus standard contracting) to meet the resiliency needs of financial services companies.

To address risks in today’s environment and to address regulatory requirements, financial institutions seek telecommunications providers that can offer:

- No single point of failure
- Resilient infrastructure
- Engineered diversity and methods for maintaining the engineered diversity over time
- Low end-to-end latency
- Services supporting high-bandwidth needs
- Remote, out-of-band, management and testability
- Comprehensive event monitoring and reporting
- Strong network security

The following recommendations for financial institutions are essential for achieving resiliency:

- Know your mission-critical functions (and dependencies) and understand your acceptance of business risk.
- Know the extent to which your continuity of mission-critical business operations relies on the diversity, recoverability, redundancy and resiliency of your telecommunications requirements.
- Identify mission-critical services and functions that pose the highest risk to the institution if they are disrupted.
- Analyze and assess vulnerabilities and threats to mission-critical services. Threats exercise vulnerabilities and include natural disasters, malicious actions, cyber attacks and exploitation of single points of failure.
- Understand how specific diversity, recoverability, redundancy and resiliency requirements affect your institution’s ability to continue operations.
- Understand that standard contracting with multiple telecommunications service providers alone may not provide the necessary diversity, recoverability, redundancy and resiliency.
- Establish a trusted relationship with your telecommunications service provider (or system integrators/managed service providers) by conducting the necessary due diligence and oversight to detailed service engineering and established documentation of service level agreements (SLAs), to assure requirements are clearly stated. Structure contracts to address these needs on a continuing basis, and include regular metrics.
- Take advantage, where eligible, of U.S. government-sponsored programs that permit the financial services sector to use recovery and response tools such as the Telecommunications

Service Priority (TSP), Government Emergency Telecommunications Services (GETS) and Wireless Priority Services (WPS).

- Understand that emerging high diversity, recoverability, redundancy and resiliency services may cost more than standard services.
- Continue to assess emerging telecommunications and alternate transport technologies to determine whether they could provide services to further assure the necessary levels of diversity, recoverability, redundancy and resiliency are achieved.

II. RISKS, REQUIREMENTS AND STRATEGIES

KEY QUESTIONS

Note: Keep the following questions in mind as you read this section of the BITS Guide to Business-Critical Telecommunications Services. Then use the questions as part of your internal evaluation process.

Planning Elements

1. Are your financial institution's critical business requirements for diversity, recoverability, redundancy and resiliency of telecommunications detailed in your institution's business continuity plan? Are those requirements aligned with the terms of your contract for the service(s) provided by your telecommunications service provider(s)?
2. Have you conducted a risk assessment that considers the respective loss of telecommunications services to each of your critical applications?
3. Have you validated the accuracy of your assumptions for diversity, recoverability, redundancy and resiliency with your telecommunications service provider?
4. Do you have a full and complete list of your mission-critical telecommunications services and the critical systems that support them? Have recovery times for each critical telecommunications service been identified?
5. Are recovery time guarantees included in the SLA with your telecommunications service provider?
6. Are the needs for diversity, recoverability, redundancy and resiliency adequately conveyed to the service provider?
7. Have you provided your telecommunications service provider with information on your diversity, redundancy and resiliency requirements and maximum tolerable recovery times?
8. Have you identified business-critical telecommunications services in order of importance or criticality that are within your own premises? Do you know who is responsible for these critical services that are within your premises? Is the implementation of your requirements visible all the way to the point of handoff to the telecommunications provider outside your institution's facilities?
9. If you have a foreign-based telecommunications service provider, have you assessed risks? Are the risks consistent with those of your U.S.-based telecommunications provider(s)? If not, have you implemented controls to mitigate these risks?
10. Have you analyzed interoperability issues with legacy systems and use of emerging technologies (e.g., Voice over Internet Protocol, wireless, other non-wireline networks)? Are they compatible and consistent with your business continuity plans?
11. Have you established corporate policies and procedures to manage your institution's relationship with telecommunications service providers?
12. Have you identified for the service provider those mission-critical telecommunications circuits that qualify for the Telecommunications Service Priority (TSP)? Has your telecommunications

service provider verified TSP-designated circuits? Have you considered obtaining TSP protection for all eligible single-threaded circuits?

Physical Considerations

13. Do you understand your local telecommunications service provider environment and service options?

14. If your institution uses more than one telecommunications service provider, what assurances do you have that there are no physical routings or single points of failure common to both providers? What process does the provider use to guarantee these assurances? Have you asked your telecommunications service providers how they will retain redundancy and diversity requirements when provisioning or “grooming” your critical circuits?

15. Have you identified and configured communications circuits that require specific physical diversity minimums?

- Are any parts of the cabling, for example, exposed to external contractors or others beyond your control?
- Who is responsible for these areas?
- Do any third party components fall between areas of responsibility?

16. Do all of your services leave your premises in the same cable? Are they all in the same duct?

17. Do you know where in the telecommunications service provider’s core network your network services connect, how they are connected, and the physical routings they take once they leave your premises?

18. Do you know if critical services are routed via different network components so that a failure of one component will not affect all critical services? Have you specifically asked for this service?

19. Have you considered an “active-active” diverse geographic business operations and architecture, where possible, for your most critical business operations to minimize dependency on assured redundancy and diversity of telecommunications services?

20. Do you consider the technologies applied by your telecommunications service provider to be adequate? For example, do you use SONET or equivalent “self-healing” technology to connect data centers to carrier central offices to make connections as resilient as possible?

21. Have you evaluated the resiliency of SONET rings serving your circuits?

22. Have you discussed with your telecommunications service provider specific concerns regarding single-threaded circuits, SONET rings and physical versus logical SONET?

23. If you rely on single-threaded circuits, have you assessed whether this approach is consistent with your institution’s risk assessment and business continuity strategy? If not, can you work with your telecommunications service providers to implement a more robust technological alternative?

24. Have you considered concentrating multiple circuits on fewer, higher bandwidth circuits in order to simplify connectivity and better assure diversity?

25. Have you extended frame relay networks to avoid network-to-network interconnects (NNIs) and reduce complexity and single points of failure inherent with some NNI connections?

26. Have you considered the alternative technologies and services available to address potential “last mile” and inter-facility bottlenecks and single points of failure that cannot be resolved with conventional services?

27. Have you assessed the risks and implemented mitigating controls for Voice over IP systems, taking into account the need for a robust network monitoring, information security programs, and sufficient backup systems?

28. Have you examined and assessed potential single points of failure of your institution’s information security program including physical placement of routers, switches and common power sources?

Regulatory Requirements

29. Are you aware of regulatory requirements and guidance concerning business continuity planning and resiliency and diversity requirements, such as the *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System* and the FFIEC’s *Business Continuity Planning Booklet and Operations Booklet*? Do your business continuity plans meet these requirements?

30. Are your telecommunications vendor management personnel aware of regulatory requirements for critical business operations continuity and recovery goals?

Power Issues

31. Have you assessed how a power failure both at your institution’s premises and at your telecommunications service provider’s would affect mission-critical services?

32. Does your institution provide standby power on your own premises? Do you test standby power regularly?

33. When battery backup capabilities are provided, do you know how long your critical services can run under full load? Is it adequate for your needs?

34. When emergency generator capabilities are provided, how much of the full load can be handled, for how long? Is it adequate for your critical services needs?

35. Is adequate diesel fuel stored on the premises to support your emergency generator needs? Is off-site delivery of diesel fuel adequate to meet your needs?

36. Is there adequate contingency power for air conditioning and chilled water to support your critical technology services? Can the telecommunications service provider demonstrate that it maintains the batteries in outside plant equipment?

37. Does your telecommunications service provider have emergency power provisions and does it maintain and test standby power regularly?

38. Have you discussed power issues, impact on wireless networks, carriers’ fiber networks electronics equipment terminations on your premises and the need for adequate backup power, both for CPE and with the telecommunications service provider?

39. Do you provide periodic maintenance and testing of your systems at “full load” to ensure that the backup system is tested under realistic scenarios?

40. Have you included in your SLA a provision to ensure re-supply of fuel from suppliers?

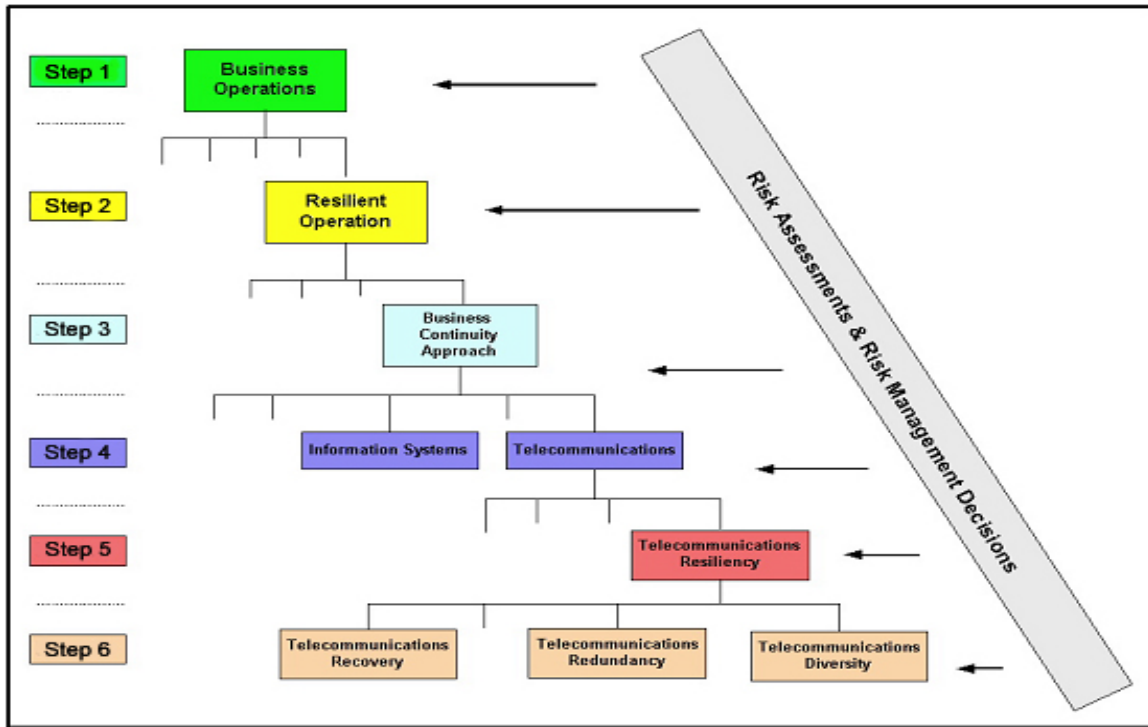
OVERVIEW

The telecommunications infrastructure was designed and engineered to support the general public’s needs. Network reliability is premised mainly on an analysis of previously experienced, unintentional, random failures, which is efficient in responding to most events that occur with regular network use. However, entities with critical operations today require strategies and support sufficient to rapidly mitigate the effects of a targeted attack on specific nodes. Because financial institutions are significantly dependent on reliable, resilient and diverse telecommunications services and must comply with regulatory and supervisory requirements, financial institutions must work diligently internally and with their telecommunications service provider(s) to achieve the necessary levels of diversity, recoverability, redundancy and resiliency.

A comprehensive risk management strategy includes:

- Risk assessment and risk mitigation;
- Due diligence;
- Contracting;
- Testing; and
- Monitoring.

The chart below outlines major steps financial institutions employ to determine their telecommunications diversity, recoverability, redundancy and resiliency needs.



Decision Process: Business Continuity Strategy

Figure 1: A high-level analysis and decision process for determining a business continuity strategy

KEY TERMS

Risk managers must work with their telecommunications service providers to establish mutually acceptable definitions for diversity, recoverability, redundancy and resiliency as some of these terms are based on “tariffs” that may not adequately address the specific needs of the financial services customer. For example, the Federal Reserve Board states that “resilience of the U.S. financial system in the event of a ‘wide scale disruption’ rests on the rapid ‘resumption’ and ‘recovery’ of the ‘clearing and settlement activities’ that support ‘critical financial markets.’”⁴ Moreover, terms differ by country. In the United Kingdom, financial institutions and telecommunications companies often refer to the diversity issue as “separacy,” which means end-to-end separation.

Key terms are defined as follows:⁵

Diversity

Financial institutions view diversity from a functional perspective: primary and backup telecommunications capabilities should not share common points of failure. More important, financial institutions believe that diversity is a proactive component of resiliency and is required to

⁴ The Federal Reserve Board, the Office of the Comptroller of the Currency, and the Securities and Exchange Commission, *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System*, September 5, 2002, p. 6.

⁵ Adapted from the President’s National Security Telecommunications Advisory Committee, *Financial Services Task Force Report*, April 2004.

ensure predictable recovery of financial services functions if primary telecommunications services are disrupted. At a technical level, however, the telecommunications industry recognizes that a single engineering definition of network diversity does not exist. Service providers define diversity solutions in contracts with each customer according to the customer's unique requirements. Diversity solutions can range from simple, relatively inexpensive measures, like dual dial tone sources, to comparatively costly network architecture solutions. Diversity management can ensure that redundant assets do not share common points of potential failure, thus protecting a network from catastrophic failure. Financial institutions should monitor their telecommunications service providers to ensure that diversity is established and maintained.

Diversity encompasses a multitude of factors, including technology, geography, facilities and business continuity planning. Moreover, diversity can be achieved through a number of means:

- **Media diversity**, which provides alternative communications transport mechanisms (e.g., wireless, satellite);
- **Entry diversity**, which offers more than one cable entrance into a building;
- **Pair and cable diversity**, which provides a local loop connection through multiple, non-adjacent pairs in more than one cable;
- **Path or route diversity**, which provides end-to-end, physically or logically separate routes for a circuit;
- **Central office diversity**, which provides local loops that terminate in more than one central office;
- **Site diversity**, which provides alternative or backup locations;
- **Service provider diversity**, which involves services obtained from more than one telecommunications service provider; and
- **Supplier diversity**, which provides more than one vendor for the infrastructure's underlying hardware and software.

Service providers typically negotiate contract-specific diversity services to meet customers' national security/emergency preparedness (NS/EP) telecommunications requirements.⁶

Recovery and redundancy together cannot provide a sufficient level of resiliency if these measures can be disrupted by a single event; therefore, diversity is crucial.

A related term commonly used in the United Kingdom is "separacy." Separacy ensures that specified circuits are physically separated throughout the network so that there are no common exchanges, interconnection points or cable routes. Separacy provides physical and logical separation of a circuit or system from source to destination.

Diversity Assurance

"Diversity assurance" is a related term. Diversity assurance is defined as a preventive measure in which communications service providers verify at regular intervals that diversity (no single point of failure) for a commonly agreed-to baseline of critical facilities within a network is maintained. If a loss of diversity occurs, service providers must restore facilities to the baseline diversity status. Without a real-time solution to guarantee that a circuit's path or route is static and stable, a financial institution cannot be assured at all times that its diversity plan is being met. Currently, no standard offerings provide diversity assurance. The closest solution is an after-the-fact monitoring of circuit

⁶ "National security and emergency preparedness telecommunications services" are the telecommunications services used to maintain a state of readiness or to respond to and manage any event or crisis (local, national or international) that does or could cause injury or harm to the population; cause damage or loss of property; or degrade or threaten the NS/EP posture of the United States. NCS, *Telecommunications Service Priority System for NS/EP Service User Manual* (NCS Manual 3-1-1), March 1998.

diversity. The Federal Aviation Administration (FAA) Leased Interfacility National Air Space Communications System (LINCS) network requires a certification on route diversity once a month. However, this is a manual process that is labor intensive, time consuming and not scalable. The telecommunications industry, through the Alliance for Telecommunications Industry Solutions (ATIS), is examining new processes and procedures to provide diversity assurance certification of routing in a more real-time manner that would support a multiple telecommunications provider environment.

Recoverability

Recoverability is the reactive component of resiliency. Recoverability must be considered from the perspective of the critical financial services business function and the underlying telecommunications infrastructure. The procedures for recovery of critical functions are typically documented in business continuity plans, which must be exercised regularly.⁷ Recovery capabilities ensure that methods are in place to quickly restore critical business operations if a partial or full interruption or failure occurs. Response time and recovery activities depend on many factors including:

- The scale and scope of an incident;
- Access control to damaged service provider/customer assets and premises;
- Prevailing weather conditions;
- Status of the electric power infrastructure;
- Service provider/customer backup capability;
- Security and safety considerations; and
- Regulatory demands.

From the perspective of the telecommunications service provider, recoverability of network services may include automatic and manual measures to recover (or restore) interrupted services. These measures could include network management controls, SONEt technology, other automatic service recovery technologies, and manual provisioning transfer to alternate facility routes.

Redundancy

Redundancy provides alternative methods of telecommunications capabilities to sustain business operations and eliminate any single point of failure that could disrupt primary services. For telecommunications supporting critical financial services functions, redundancy includes, but is not limited to:

- Dual sites where the function is performed;
- Dual telecommunications offices serving each site; and
- Dual routes between each customer site and the serving central offices.

Other redundancy measures include, but are not limited to:

- On- and off-site backup equipment and data storage;
- Multiple telecommunications circuits; and
- Alternative communications technologies.

Resiliency

Resiliency can be enhanced by implementing telecommunications services capabilities that can better withstand shocks or hazards with minimal interruption or failure. A resilient financial services operation and its critical telecommunications services must be able to mitigate hazards of nature,

⁷*Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System*, pp. 8-17.

such as earthquakes, tornados, floods and other natural disasters, as well as human-made hazards, such as bombings, cyber crimes, malicious destruction, and terrorist attacks. Financial institutions and others that make up the nation's critical infrastructure face additional challenges in the current threat environment. They must similarly be able to mitigate the effects of random events and potentially hazardous and sophisticated scenarios, which are often specifically designed to inflict long-term extended damage on critical infrastructures and economic stability. A financial institution's level of resiliency is determined, in part, by how well each of the terms defined above is accomplished.

RISKS

The major risks facing financial institutions with regard to diversity, redundancy, resiliency and recoverability of telecommunications services are:

Inadequate Diversity, Lack of Physical Redundancy, and Existence of Critical Points of Failure

Financial institutions' diversification plans and strategies are often hampered by static assurances that contracted telecommunications services will meet diversity and redundancy requirements. Many financial institutions that contract with two different providers mistakenly assume that this approach provides an acceptable level of diversity. However, it has been found that service providers often use the same physical path or pass through the same central office.

Concentrations of circuits traversing specific geographic locations could pose excessive risks to financial institutions and telecommunications service providers, unless the critical assets are adequately supported by fully redundant secondary sites. Dialogue among the appropriate financial institutions and telecommunications service providers may be necessary to determine whether additional actions to further engineer continuity of critical financial functions supported by the circuits are warranted.

State and local policies and building owners often determine routes—and therefore whether diversification is possible—by dictating where telecommunications companies can install telecommunications lines.⁸ Consequently, financial institutions and telecommunications service providers should review physical diversity at the building level (e.g., multiple cable/fiber entry points per building, separate risers within each building, backup sites).

Limited Information Sharing

Limited information is provided to financial institutions and other telecommunications customers concerning the specific physical communications paths used to carry critical transaction information due to concerns of post-9/11 critical network infrastructure protection, confidentiality and competition. Moreover, telecommunications service providers may take actions that are at odds with the diversity assurance needs of financial institution customers. For example, telecommunications companies may limit (via trace tools) access to information that identifies the routes by which data are transmitted. While the company may do this to address competing security concerns, it creates challenges for risk managers who need to know this information.⁹ The Federal Communications

⁸ For example, fiber builds are based on population growth and route diversity is often dictated by the characteristics of the current infrastructure such as the placement of sewer, highway and railroad lines. Building codes at state and local (including municipal) levels can also impede reforms that would improve the redundancy and resiliency of telecommunications networks.

⁹ The New York State Public Service Commission, in an "Order Concerning Network Reliability Enhancements" (July 28, 2004), addressed and balanced the competing security need for customer-specific

Commission Network Reliability and Interoperability VI Homeland Security Physical Security Best Practices stress the need to protect critical facilities information.¹⁰

In addition, antitrust laws that bind telecommunications service providers and regulatory requirements that force telecommunications service providers to protect Customer Proprietary Network Information complicate telecommunications service providers' ability to share confidential mutual client information with one another. Competitive forces also contribute to the lack of information sharing among telecommunications providers and their financial institution customers. As a result, general contractual arrangements with multiple telecommunications providers are not sufficient to assure financial institutions that they have achieved requisite telecommunications diversity or redundancy.

Uncertain Impact on Emerging Technologies and Integration with Existing Technologies

Emerging technologies, such as wireless and broadband, will affect how the financial services industry processes transactions and conducts business. These new technologies may play an important role in solving redundancy problems, but emerging technologies may not be designed with essential security and resiliency features and new risks associated with them may not be understood. Reliability and resiliency must not be assumed for mission-critical processing or recovery capabilities. They must instead be based on detailed analysis.

Internet Reliability

The Internet before 9/11 was beset with many problems, including lack of strong SLAs, slow performance, un-guaranteed delivery, highly variable response times, and vulnerability to various forms of attacks.¹¹ In the wake of 9/11, however, the Internet clearly demonstrated its flexibility and resilience. This was in large measure due to its diffuse micro nodal architecture.¹² During those first few days when firms found that their private line network was destroyed and would not be restored for some time, they discovered that their Internet connection was still working. In an effort to meet their clearance and settlement requirements as well as participate in some markets the following Monday, they needed to use the only surviving communication infrastructure they had. The Internet demonstrated to them and the balance of the financial community that it could in fact be relied on to meet their basic business communications needs.

While the Internet is not a turnkey replacement for all dedicated private networks, it can act as a resilient replacement for some networks or an effective minimal secondary or tertiary backup to the primary private network. Some experts believe the Internet today cannot yet meet the demands of high volume, real-time market data dissemination and sub-second trade execution instructions. However, today's Internet can meet the requirements of many other support services within the

information on the physical path of carriers' for customers with Telecommunications Service Priority (TSP) circuits so that customers with enhanced reliability needs can be assured of diversity in serving arrangements and be informed of any changes that may occur over time to those arrangements. The Commission is requiring those carriers serving its jurisdiction to tariff for TSP customers a new "Critical Facilities Administration" service, or alternatively, to show cause why they should not. View the report at <http://www.dps.state.ny.us/DPS-NetworkReliabilityRpt.pdf>.

¹⁰ See www.nric.org.

¹¹ The term "Internet" in this paper refers to the public Internet that connects computer networks and facilities around the world. The current Internet is a best effort basis with no quality of services guarantees.

¹² "Diffuse micro nodal architecture" differs from the hierarchical nodal infrastructure carriers use today, in which increasing numbers of circuits are concentrated in fewer nodes as one moves up the hierarchy. With a hierarchical nodal infrastructure, loss of one of the nodes near the top of this pyramid results in the widespread loss of communications circuits along with their backups.

financial community. And, unlike many dedicated private networking technologies, the Internet continues to evolve and grow.¹³

Other Concerns

Some military government agencies have warned about the risk of electromagnetic pulses (EMPs). EMPs result from a high-energy explosion such as a nuclear bomb. EMPs can disrupt or destroy nearly every form of electrical system. These problems can include interference of radio frequency links, irreparable damage to microcircuits and even disabling satellites.

Electrical equipment can be “hardened” to protect itself from an EMP. These protections also serve to enhance the quality of communications. Metallic shielding can route EMP fields away from vital electrical components. If the equipment is also connected to a cable, transient protection like surge protectors, wire termination procedures, screened isolated transformers, protective enclosures, spark gaps and filters can protect at the point of entry. Other methods, such as increasing immediate backup units and avoidance (e.g., keeping equipment out of range of EMP bursts) can indirectly protect against EMP.¹⁴

Other areas of concern include a coronal mass ejection, which has affected satellites.¹⁵

REQUIREMENTS

Regulators require financial institutions to manage risks associated with third-party service providers. Ensuring uninterrupted telecommunications service is a critical component of financial institutions’ business continuity plans. In recent years, financial regulators and self regulatory organizations have focused greater attention on business continuity, outsourcing and information security. The following is a brief overview of some of the requirements governing telecommunications diversity, recoverability, redundancy and resiliency:

Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System¹⁶

The Federal Reserve Board, Office of the Comptroller of the Currency and the Securities and Exchange Commission issued requirements in April 2003 for “core clearing and settlement organizations” and “financial institutions that play significant roles in critical markets.” The paper acknowledges the effect telecommunications dependencies can have on recovery times.

¹³ Today’s Internet is forming the basis of the IP Next Generation Network (NGN), which will emerge during the next decade. The National Security Telecommunications Advisory Committee (NSTAC) will develop recommendations in 2005 to ensure the NGN will be able to fulfill the national security and emergency preparedness needs of the financial services community and the nation. Corporate communication networks should take into account the effectiveness of the Internet and plan to integrate it into their BCP communications strategies.

¹⁴ The Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack discussed its report with the House Armed Services Committee on July 22, 2004. Chairman Duncan Hunter noted that “The proliferation of nuclear weapons and the rise of new nuclear powers with small nuclear arsenals have forced us to think about EMP as an asymmetric threat in its own right. At the same time, our economy is increasingly dependent on the electronic systems vulnerable to electromagnetic pulse.” See http://armedservices.house.gov/press_releases/2004/04-07-22Hunter.pdf.

¹⁵ These issues are discussed in the FCC’s NRIC VI Focus Group 1A final report, Issue 3, December 2003. See www.nric.org under “areas of attention.”

¹⁶ See <http://www.occ.treas.gov/ftp/bulletin/2003-14a.pdf>.

FFIEC Booklets¹⁷

The *FFIEC Business Continuity Planning Booklet* and the *FFIEC Operations Booklet* highlight critical aspects of effective business continuity planning and specifically address reliance on telecommunications networks and telecommunications providers. The booklets recommend financial institutions identify and document single points of failure in their internal and external communications systems and establish appropriate SLAs with telecommunications service providers.

SEC, CFTC and SRO Rules

The Securities and Exchange Commission, National Association of Securities Dealers (NASD) and the New York Stock Exchange (NYSE) require NASD and NYSE members to create and maintain a written business continuity plan identifying procedures relating to an emergency or significant business disruption. Under the rules, every NASD and NYSE member must develop a plan that addresses ten specific elements for business continuity, including data backup and recovery, all mission critical systems, critical business constituent impact, and alternate communications between the firm and its employees, regulators and customers. In addition, the continuity plan must address how the member will ensure that customers have prompt access to their funds and securities if the firm is unable to continue in business. The SEC and the Commodities Futures Trading Commission have developed policies and procedures for applying NS/EP telecommunications programs to key market utilities and market participants.

FCC Requirements

The Federal Communications Commission requires some telecommunications companies to report information electronically to the FCC about significant disruptions to their communications systems.

STRATEGIES TO ACHIEVE DIVERSITY, RECOVERABILITY, REDUNDANCY AND RESILIENCY REQUIREMENTS

The Basic Approach

Industry business practices for diversity include:

- Separation of multiple circuit paths;
- Decentralization of office facility connections; and
- Alternative transmission technologies.¹⁸

These three telecommunications resiliency measures are complementary and may coexist to provide a predictable level of business continuity for critical NS/EP services. The financial services sector relies on the telecommunications sector to ensure that these measures are applied end-to-end on critical connections when specified by the customer to the service provider. Redundancy and diversity must be carefully configured as part of the network design. Once put into place, routine monitoring of the network is required by the service provider and customer to insure that single points of failure are not introduced, either by the customer or the vendor. Even if it is possible to verify through testing that some recovery and redundancy measures are in place, financial services

¹⁷ See http://www.ffiec.gov/ffiecinfbase/html_pages/bcp_book_frame.htm.

¹⁸ Network Reliability and Interoperability Council VI, *Homeland Security-Physical Security Prevention and Restoration Report*, March 14, 2003. (See http://www.nric.org/fg/charter_vi/fg1/RECOM_FG_1A_Homeland_Security_Physical_Security_Mar14.doc.) Network Reliability and Interoperability Council VI, *Homeland Defense-Cyber Security Best Practices*, March 14, 2003. (See http://www.nric.org/fg/charter_vi/fg1/FG1B_front_matter_and_proposals_FINAL_3-13-03.doc.)

firms need to rely on other methods of due diligence to verify the engineering and recoverability of telecommunications services.

When performing resiliency assessments, it is important to consider:

- Essential business functions;
- Time sensitivity of each essential function;
- Threats to the continuity of the functions and the services upon which they depend;
- Threat mitigation options;
- Cost/benefit analysis;
- Mitigation strategy;
- Implementation;
- Testing; and
- Information sharing on all of the above.

Procuring Diversity Services

Risk managers can apply many different strategies to achieve diversity, recoverability, redundancy and resiliency. However, there are three primary strategies for procuring diversity services:

- Purchase services from one service provider;
- Purchase services from two or more telecommunications service providers; and
- Use more than one type of transmission medium.

Purchase Services from One Service Provider

In most areas of the U.S., the local exchange carrier (LEC) is the only service provider that has the variety of facilities in place to provide the necessary multiple paths. Most of the larger LECs offer facility diversity services primarily through their SONET rings. With SONET ring services, a customer has two paths to the PSTN. If the ring is cut in one place, the customer's service remains connected to the PSTN via its second path. While SONET ring services are likely to be more reliable than the standard offerings (and more expensive), these services are not without problems. For example, there are documented instances in which a portion of a SONET ring has collapsed or folded on itself. This resulted in a single point of failure for the customer's PSTN paths. Another negative aspect of purchasing facility diversity services exclusively from one service provider is that it can lead to substantial segments of single points of failure over time if the service provider "grooms" (i.e., modernizes and consolidates) its facilities.

The purchase of services from a single service provider can lead to other single points of failure. For example, if a carrier provides diverse circuits using parallel cables that terminate in the same central office, the circuits may have the same source of power. If that same power source fails, both circuits will fail. Also, diverse circuits may use the same timing source. Failure of that timing source will also render both diverse circuits inoperable.

Purchase Services from Two or More Service Providers

The premise for this option is that a customer would achieve facility diversity by purchasing telecommunications services from two or more service providers. Presumably, since the two service providers would be expected to have distinct facilities, the facility diversity problem would be solved. On its surface this would appear to be a reliable way to achieve facility diversity. However, telecommunications service providers often lease some facilities from other providers to provide the complete set of services requested. This can lead to the services traveling unintentionally over the same facility. In addition, even when both service providers have enough facilities to maintain two

distinct parallel paths, their facilities may be located in the same or adjacent underground conduit runs or manholes. Ensuring facility diversity is made more complex by the lack of computerized detailed routing records available to the customers by the carriers. The coordination needed to ensure the required diversity, especially if both carriers groom these circuits, could be complex and difficult to achieve. If three or more service providers were used, the problems would be even more complex. This option can only be effective if the financial institution takes on the responsibility (or hires a third party) for continually monitoring the diversity characteristics of all services purchased because the telecommunications service providers do not share such information with each other.

Use Alternative Transmission Media

The options discussed thus far have one common problem: It is very difficult to maintain wireline facility diversity in the long run, as telecommunications service providers make changes to their equipment and transmission facilities. This is true because:

1. Services provided over diverse wired facilities tend, over time, to be consolidated into more efficient, higher capacity, but less diverse facilities unless specifically exempted from “grooming”; and
2. Major carriers do not have real-time computerized cable facility record system solutions that ensure that facility diversity services, once established, will continue as long as the customer requires such services.

One way to resolve this problem is to use backup facilities that can never be in the same cable sheaths, in the same trenches, in the same conduit runs, or on the same pole lines as the primary telecommunications facilities. Using a wireless backup system has been shown to be an effective way to accomplish this.

While wireless backup systems can help ensure diversity and reliability of telecommunications transmission facilities, the effectiveness of these systems depends on how well they are designed and how they are connected to the public network. For example, wireless backup systems should have sufficient emergency power to operate effectively during lengthy commercial power outages. Also, if possible, a wireless backup system should be terminated at an alternative central office, so that if the primary central office fails, the backup system will still operate. Care should also be taken to ensure that wireless backup systems have batteries and a generator if they are served by the same power plant and timing systems as the primary systems.

A number of mature wireless products can be used to provide highly reliable backup communications systems. Emerging technologies will soon be worth considering as well. Microwave and satellite systems are available and can provide highly reliable and functional voice and data services. It appears that microwave systems have the edge over satellite systems on the quality of voice transmissions and installation times. In addition, free-space optics and spread-spectrum technologies hold considerable promise. However, financial institutions should assess whether applications can deal with delays inherent with satellite links as well as the effects of inclement weather and other line-of-sight issues with microwave technology. For example, during 9/11, some microwave systems did not work because of the heavy dust in New York City. Moreover, satellites are adversely affected by heavy rains and storms.

Risk Mitigation Remedies

The chart below provides an overview of numerous risk mitigation remedies that financial institutions can pursue. The “Issue” column quantifies a potential concern associated with the loss of telecommunications for data and voice. Each associated column describes risk mitigants that can provide greater resiliency and minimize single points of failure. The customer is responsible for working with its carriers to ensure that the design of the solution is redundant. The customer must

also develop a process to monitor and ensure that the carriers do not modify or change any design that could compromise diversity and fault tolerance.

Bear in mind that this chart oversimplifies the issues financial institutions may encounter and the subsequent risk mitigants that organizations might employ. It is intended as an overview to encourage organizations to conduct further investigation and analysis. For example, reliance on Internet virtual private networks (VPNs) has its limitations in the likely event that a failure that causes a SONET ring failure may also affect Internet service provider (ISP) links.

Table 1: Telecommunications Issues and Mitigants

Issue	Mitigant (1)	Mitigant (2)	Mitigant (3)
	Preferred		▶ Last Resort
Circuit Issues			
Primary circuit down	TSP designated and alternate diverse circuit implemented	ISDN backup installed	Alternate route engineered and included in an SLA
Circuit disconnection	Engineer and implement circuit redundancy over diverse route	Validate records/SLAs	Internet VPN ¹⁹
Software glitch: primary network	Implement backup IP network	Utilize ISDN backup	Utilize Internet VPN
SONET ring collapse	Implement alternate "traditional" network/lines		
Fiber Issues			
Fiber cut	Implement fiber diversity via multiple paths	Create fall back to fiber loss with "traditional" non-fiber circuit redundancy (diverse)	Internet VPN
Hardware/Software Failures			
Voice switch	Implement redundant, geographically diverse Public Branch Exchange (PBX)	Use vended Centrex-type call plan re-routing	Implement VoIP
Data switch	Implement redundant switches at multiple sites		
Router	Implement redundant routers at geographically diverse sites		
Multiplex	Implement redundant hardware at geographically diverse sites		
Digital cross connect system	Implement alternate fail-over network at geographically diverse location		
Fiber terminal			
Customer hardware failure	Have critical spare hardware on hand or establish SLA with vendor	Implement hardware redundancy at geographically diverse location	Utilize the Internet with VPN
Carrier hardware failure	Have critical spare hardware on hand or establish SLA with vendor	Implement circuit redundancy (diverse) with vendor	Utilize Internet with VPN
Software glitch with primary vendor	Implement backup network	ISDN backup	Utilize Internet with VPN
VoIP virus	Implement antivirus software mechanism and ensure	Use alternate traditional network	

¹⁹ The term "Internet" in this paper refers to the public Internet that connects computer networks and facilities around the world. The current Internet is a best effort basis with no quality of services guarantees.

Table 1: Telecommunications Issues and Mitigants

Issue	Mitgant (1)	Mitigant (2)	Mitigant (3)
	Preferred		→ Last Resort
	currency update		
VoIP Clipping	Avoid double duty devices (e.g., PC/phone)	Use alternate traditional network	
VoIP DDOS	Implement alternate fail over to traditional network	Create and test strategy for addressing DDOS attacks	
Facility Issues			
Carrier facility destruction	Create circuit redundancy by engineering separate diverse routes that are contractually guaranteed	Utilize Internet with VPN	Hold vendors to SLA
User facility destruction	Ensure geographically diverse backup site and circuit duplicity exist and are contractually guaranteed	Utilize Internet with VPN	
Central office (C.O.) failure	Ensure circuit redundancy from diverse C.O. for mission critical circuits (include Internet circuits)		Hold vendors to SLA
Environmental Issues			
Customer environmental	Implement UPS/generators for mission critical circuits and related equipment	Implement capability to provide for backup heating, cooling, air-conditioning (HVAC)	Utilize Internet with VPN
Carrier environmental	Implement UPS/generators for mission critical circuits and related equipment	Implement capability to provide for backup HVAC	Utilize Internet with VPN
Power outage	Implement UPS/generators for mission critical circuits and related equipment	Install analog, non-electrically powered telephones	Implement cellular/satellite telephone switches and circuits
Voice			
Administrative problems with call managers	Implement GETS and WPS		
Miscellaneous			
Internet service provider (ISP) loss	Use diverse paths and separate ISP providers	Hold vendors to SLA	

Circuit Issues

Financial institutions should determine whether single-threaded circuits are consistent with their risk assessment. If not, the institution should work with its telecommunications service provider to implement more robust technological alternatives. Financial institutions should obtain TSP protection on all single-threaded circuits that meet the program criteria due to the vulnerability to disruption of single-threaded circuits versus SONET.

Some financial institutions provide multiple services/business processes over single circuits through load-balancing techniques. However, certain critical functions cannot be aggregated and are instead supported by separate virtual networks and bound by hardware and legacy applications. In these cases, risks should be assessed to mitigate any related exposures.

Circuits supporting a lower volume of financial transactions but high dollar amounts might be as critical to an institution as those supporting a high volume of lower dollar amount financial transactions. Accordingly, each institution should determine its own risk assessment and the appropriate level of protection for each type of circuit.

Power Issues

Financial institutions should consider alternative sources of backup power, depending on circuit layout, when the loss of power at one institution could impact services provided through other institutions because of interdependencies among these institutions and their critical financial services. With their telecommunications service providers, financial institutions should identify those facilities that merit backup power for specific technologies (e.g., SONET, ATM) and network hardware and network points of presence (e.g., uninterruptible power supplies and standalone electrical generators). To the extent that telecommunications service provider equipment is located on your institution's premises and it is not connected to your institution's backup power supply, it is important to check whether the telecommunications service provider service includes batteries. This may be a challenge in multi-tenant buildings in which telecommunications service provider equipment is not in the institution's space.

Alternatives and Emerging Technologies

Financial institutions are using numerous emerging technologies and alternate transport mechanisms to enhance the resiliency of telecommunications. Although these technologies hold promise, they cannot be applied universally as a solution for telecommunications diversity in the financial services sector. Bandwidth, data transmission latency, reliability and security issues may limit the practical application of these technologies as near-term solutions. For example, it is important for business continuity planners to know or have access to information on the routes/paths through which data passes. This information is essential to recover from a service disruption.

Appendix A provides an overview of alternatives and emerging technologies such as satellite, laser, microwave, spread spectrum technology, wireless and Voice over IP. The appendix also includes examples of alternate transport mechanisms developed by the Securities Industry Association and the Depository Trust and Clearing Corporation. Financial institutions should consult with their telecommunications providers to evaluate the appropriateness of specific alternative technologies.

III. RECOVERY TOOLS AND PROCESSES

KEY QUESTIONS

Note: Keep the following questions in mind as you read this section of the BITS Guide to Business-Critical Telecommunications Services. Then use the questions as part of your internal evaluation process.

41. Have you discussed with your telecommunications service provider the scenarios used in the provider's contingency plans?
42. Are the provider's recovery time objectives consistent with your institution's requirements?
43. Does the telecommunications service provider have any partnerships or SLAs with other service providers to continue providing service to your institution?
44. Do you know the telecommunications service provider's priorities for restoring service? Where do your institution's requirements rank?
45. Do you have information about or are you assured of rapid access to information on the routes or paths through which your information passes when recovering from a disruption in service?

OVERVIEW

The federal government requires telecommunications companies to offer special tools to organizations that are eligible for priority restoration of telecommunications service. In December 2002, the federal financial regulators revised their policies and procedures for NS/EP telecommunications programs. These policies and procedures now include those functions supporting the Federal Reserve's NS/EP mission to maintain national liquidity.²⁰

Federally Available Tools

Government Emergency Telecommunications Service

Government Emergency Telecommunications Service (GETS) provides emergency access and priority processing in the local and long distance segments of the public switched wireline network. Companies use GETS in emergency or crisis situations, when the probability of completing a call over normal or other alternate telecommunication is significantly decreased. Individuals who perform one or more of the following NS/EP functions are eligible for GETS access:²¹

- National security leadership
- National security posture and U.S. population attack warning
- Public health, safety and maintenance of law and order

²⁰ The Federal Reserve Board expanded the scope of services that would seriously affect continued financial operations if a telecommunications disruption lasting "a few minutes to one day" occurred. Because they are considered critical to the operation and liquidity of banks and the stability of financial markets, these functions require same-day recovery: large-value interbank funds transfer, securities transfer, or payment-related services, such as Clearing House Interbank Payments System (CHIPS), Society for Worldwide Interbank Financial Telecommunications (SWIFT), and Fedwire; Automated Clearinghouse (ACH) operators; key clearing and settlement utilities; U.S. Department of Treasury automated auction and processing system; and large-dollar participants in these systems and utilities.

²¹ For GETS eligibility criteria, see <http://gets.ncs.gov>.

- Public welfare and maintenance of national economic posture
- Disaster recovery

Telecommunications Service Priority

The Telecommunications Service Priority (TSP) Program allows NS/EP users priority access to telecommunications services vital to coordinating and responding to crises.²² It is extremely important that financial institutions acquire TSP assignments for qualifying critical circuits.²³ The Federal Reserve Board estimates that approximately 6,000 NS/EP-level circuits qualify for TSP within the financial services sector. By contrast, the nation's telecommunications networks currently support more than 183 million wireline circuits alone.²⁴

Hurricanes, floods, earthquakes and other natural or human-made disasters can overwhelm telecommunications service vendors with requests for new telecommunications services and restoration of existing telecommunications services. The TSP Program prioritizes service requests by identifying those services critical to NS/EP. A telecommunications service with a TSP assignment receives full attention by the service vendor before a non-TSP service.

Financial institutions should regularly exercise their business continuity plans and involve their telecommunications providers when critical (TSP-eligible) circuits are connected to backup sites.

Due to the vulnerability to interruption of single-threaded circuits versus SONET and other protection processes, financial institutions should evaluate whether to obtain TSP protection on single-threaded circuits.

Wireless Priority Service

Wireless Priority Service (WPS) provides customers with priority cellular network access.²⁵ The WPS was approved by the FCC for NS/EP requirements on a call-by-call priority basis. The NCS executes the program on behalf of the Executive Office of the President. Only individuals in NS/EP key leadership positions are authorized to use WPS.

The financial services industry and the telecommunications industry have separate processes for responding to and recovering from a major disaster.²⁶ Financial institutions should consult with their telecommunications service providers to learn more about telecommunications industry plans and to ensure that these plans are consistent with the institution's business continuity plans. Moreover, telecommunications service providers should be included in regular testing of business continuity plans, when critical circuits are connected to backup sites.

Financial Industry Recovery Processes

Financial institutions and telecommunications companies follow the processes below in responding to NS/EP events. Crisis management coordination for the entire financial services sector is executed

²² TSP eligibility criteria are available at <http://tsp.ncs.gov>.

²³ The TSP program provides service vendors with a Federal Communications Commission mandate for prioritizing service requests by identifying those services critical to NS/EP. A telecommunications service with a TSP assignment is assured of receiving full attention by the service vendor before a non-TSP service. For additional information, see <http://tsp.ncs.gov>.

²⁴ Federal Communications Commission, Industry Analysis and Technology Division, Wireline Competition Bureau, *Local Telephone Competition: Status as of June 2003*, December 22, 2003. See http://www.fcc.gov/Bureaus/Common_Carrier/Reports/FCC-State_Link/IAD/lcom1203.pdf.

²⁵ See <http://wps.ncs.gov/>.

²⁶ See Appendix B for a brief overview of each of these processes.

via the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC). The FSSCC works closely with the U.S. Department of the Treasury and federal financial regulatory agencies through the Federal Banking Information Infrastructure Committee (FBIIC). In a crisis, incidents are reported to the FSSCC, the Financial Services Information Sharing and Analysis Center (FS/ISAC), and/or associations such as BITS and the Securities Industry Association (SIA). Each organization launches its own “crisis management coordination” process; however, most processes feed in to and coordinate with others.²⁷

Telecommunications Industry Recovery Processes

Telecommunications companies work together through the National Coordinating Center (NCC) of the National Communications System to respond to major disasters.²⁸ Additionally, all carriers have incident management plans that guide their responses. Responses are escalated based on the scope of the service impact, the duration of the service disruption, and whether the incident is a NS/EP-qualifying event. The telecommunications industry uses a multi-tiered response plan: low impact, medium impact and high impact. See Appendix B for a more detailed overview of the NCC’s crisis management processes.

²⁷ For additional information, see www.fsscc.org and www.fbiic.gov.

²⁸ The National Coordinating Center for Telecommunications is a joint industry/government organization. Its mission is to assist in the initiation, coordination, restoration and reconstitution of NS/EP telecommunications services or facilities under all conditions, crises or emergencies.

IV. DUE DILIGENCE

KEY QUESTIONS

Note: Keep the following questions in mind as you read this section of the BITS Guide to Business-Critical Telecommunications Services. Then use the questions as part of your internal evaluation process.

Planning Elements

46. What personnel resources is the telecommunications service provider prepared to commit to the relationship? How many employees will have detailed technical knowledge?
47. Have you assessed the financial stability of the telecommunications service provider?
48. What assurances can the telecommunications service provider give you to demonstrate it can meet your business needs and business continuity requirements?
49. How does the telecommunications service provider determine its liability limits associated with availability guarantees?
50. With what process does the telecommunications service provider assess its services to your institution? How does it correlate those services with new requirements to make sure that duplication and single points of failure are avoided?
51. Does the telecommunications service provider have an integrated process to ensure the circuits remain diverse?
52. Do you know who “owns” a major telecommunications facility (e.g., central office), especially those used by multiple carriers? Do you know what your telecommunications service provider’s business continuity plan is for responding to the destruction of a major facility?
53. What assurances can the telecommunications service provider give that reciprocal lease agreements are in place with other vendors and that these leased facilities do not introduce single points of failure?
54. How (and how quickly) will the telecommunications service provider inform clients of a service interruption?

Physical Considerations

55. Is the telecommunications service provider prepared to help you understand the complexities of its network and to work with you to provide suitable solutions for resiliency?
56. How does the telecommunications service provider assess the physical threats against its network assets? How does it mitigate the risk of these physical threats relative to your regulatory requirement for business continuity plans?
57. Can the telecommunications service provider demonstrate that there is no single point of failure in the infrastructure solution that has been engineered to meet your requirements? Can the provider explain the process it uses to assure your solution is maintained while changes are occurring in the provider’s or others’ systems?

58. How does the telecommunications service provider's engineering process guarantee diversity is maintained in relation to all the key elements (risers, building entry points, last mile ducts and manholes, local exchange, network routes, international links and other key points)? How are potential single points of failure identified?
59. How is spare capacity engineered (for example, by percent utilization threshold or number of last mile customer circuits)? Does capacity engineering take into consideration redirected call volumes when customers activate their business continuity plans to avoid choke points and loss of critical services?
60. Can the telecommunications service provider provide information on the routes/paths through which information passes?
61. Questions for mobile/wireless telecommunications service providers:
- a. Are there known "dead zones"?
 - b. What recovery/fail over capabilities and capacity are built in to the network?
 - c. How is resiliency built in to the infrastructure?
 - d. Does capacity engineering consider redirected call volumes when customers activate their business continuity plans to avoid choke points?
 - e. How can signal capacity and strength be increased during or after an event?
 - f. For side band audio: What radio frequencies are used? Are there distance limitations?
 - g. Are there any potential conflicts with other service providers or emergency communication services?
 - h. How are cell towers, switching stations and central offices set up for resiliency?
 - i. What are the backup power arrangements at cell towers and other facilities?
62. Can your telecommunications service provider uniquely identify your mission-critical circuits throughout its system in an end-to-end fashion and maintain that identification through changes, such as re-engineering?
63. How can the financial institution verify the accuracy of the routing information provided?
64. Do carriers customarily divert a company's traffic from a stated route to an unknown route without the customer's knowledge?

Monitoring, Testing and Reporting Results

65. Can the telecommunications service provider assure you that its diversity services will continually meet your requirements? What assurance can the telecommunications service provider give you that it has monitoring in place to meet your requirements? Can you validate and receive regular reports of the results of this monitoring?
66. Can the telecommunications service provider give you reliable recovery time estimates for defined contingency situations, such as the loss of a central office? Can the telecommunications service provider produce results of tests, especially when multiple telecommunications service providers are involved in supplying contracted services?
67. What are the telecommunications service provider's power backup, restoration and contingency plans? Are they tested? If yes, what are the results? Have you received results relevant to your service?
68. Does the telecommunications service provider have appropriate contingency plans in place to meet your institution's needs? How often does the provider test these plans?
69. Can the telecommunications service provider provide availability figures? If so, how does the telecommunications service provider account for major disruptive events in its calculation?
70. How does the telecommunications service provider monitor the network and performance of each facility?
71. What are the telecommunications service provider's change management practices as they relate to network monitoring, maintenance, equipment and software releases?
72. How are switching stations/central offices set up for resiliency? How often is this resiliency tested?
73. Does your telecommunications service provider have a tested business continuity plan? If so, does the plan meet your institution's business continuity requirements?
74. Does the telecommunications service provider test its business continuity plan? Are customers permitted to participate in tests?

OVERVIEW

Financial institutions should perform business impact analyses to determine telecommunication thresholds for their core functions and processes. Financial institutions should examine impacts within the overall payments, clearance and settlement infrastructure that, if not met or exceeded, could impact national security.

In choosing a telecommunications service provider, first determine whether the service provider has the financial resources to make the necessary investments to meet your institution's diversity assurance needs.

Financial institution risk managers should:

- Insist on viewing full routing information from the telecommunications carriers.

- Establish diverse routing and redundant facilities for critical circuits.
- Utilize alternate providers that traverse independent infrastructures.
- Introduce procedures and processes to enable the institution to effectively identify carrier diversity risks.
- Implement solutions that provide clearly defined diversity attributes and ensure their compliance with our requirements.
- Consider telecommunication diversity when planning data centers.
- Ensure circuits are not routed through interdependent (i.e., “tandem”) central offices in violation of intent and instructions.
- Redesign the circuit order process.
- Focus on diversity and engineering considerations.
- Improve carrier awareness of institutions’ diversity requirements.
- Mitigate geographical risk.
- Continue development of new diversity initiatives.

V. CONTRACTS

KEY QUESTIONS

Note: Keep the following questions in mind as you read this section of the BITS Guide to Business-Critical Telecommunications Services. Then use the questions as part of your internal evaluation process.

75. Are your institution's definitions of diversity, recoverability, redundancy and resiliency consistent with the definitions used by your telecommunications service provider? Are they specified in your contract or service agreement?

76. When you order new services, do you discuss your existing services to ensure that no dangerous assumptions are made about diversity, recoverability, redundancy and resiliency? Do you review existing requirements to prevent duplication or introduction of situations that compromise other critical requirements?

77. Have you included provisions in the contract and SLA requiring the telecommunications service provider to provide information on routing to ensure that diversity is maintained? Will these provisions provide you with enough information to meet your diversity, recoverability, redundancy and resiliency requirements?

78. Have you included provisions in the SLA requiring the telecommunications service provider to give updates on network issues, proposed engineering downtime and other changes in normal operations?

79. Has your service provider shared engineering drawings with you that show your circuit construction and routing? Have references to these drawings been incorporated into your contract?

80. Have you narrowed the *force majeure* clause to require that all diverse paths be directly disrupted before the service provider is excused under the *force majeure* clause? Have you established service restoration schedules that your service provider must meet in the event that the *force majeure* clause goes into effect?

81. Have you prevented the incorporation by reference of tariffs or other external documents into your contract? If you have not, have you carefully examined all such documents to prevent inconsistent and/or unacceptable contract terms?

82. Are your definitions of diversity, recoverability, redundancy and resiliency consistent with the definitions used by your telecommunications service provider? Do contracts and SLAs reflect these agreed-upon definitions?

OVERVIEW

Financial institutions cannot assume general contractual arrangements with their telecommunications providers will provide requisite telecommunications diversity or redundancy. Instead, specific diversity/redundancy capabilities must be contracted for, engineered, and periodically monitored. Recovery and redundancy together cannot provide sufficient resiliency if they can be disrupted by a single event such as the loss of a telecommunications provider central office. Therefore, diversity is crucial.

Industry best practices for diversity include separation of multiple circuit paths, decentralization of office facility connections, and alternative transmission technologies. A resilient financial services operation and its critical telecommunications services must be able to endure hazards of nature like earthquakes, tornados, floods and other natural disasters, as well as human-made hazards, such as bombings, cyber crimes, malicious destruction and terrorist attacks.

It is important to understand how service providers define diversity and how contracts interrelate with tariffs. Often, telecommunications companies define diversity in their tariff, but no standard definitions exist across tariffs.

General contract terms often interfere with maintaining continuous service of NS/EP critical circuits during a significant event or crisis. Specifically, *force majeure* clauses can nullify a party's obligations under a contract.²⁹ Financial institutions should understand *force majeure* clauses in contracts related to NS/EP circuits or critical functions. As a general matter, financial institutions should strive to minimize *force majeure* provisions as much as possible. Care should be taken to ensure that critical functions will not be left unsupported if the "unforeseeable" becomes reality. In the post-9/11, environment, resiliency should be contemplated and understood in terms of potential interruption from events considered outside the control of either party.

With a highly resilient communications network, the contract terms are as important as the design. A rigorous contract is necessary not only to protect your firm's interest but to also convey a sense of importance to the provider of the service and to ensure a mutual understanding of the service and all the associated terms and conditions. One cannot acquire highly available bandwidth when the purchasing department views bandwidth as a commodity service. Great care and effort must be undertaken to ensure that the service will meet and continue to meet the business continuity needs of your organization and its customers.

²⁹ *Force majeure* is defined as a clause "to protect the parties in the event that a part of the contract cannot be performed due to causes which are outside the control of the parties and could not be avoided by the exercise of due care." *Black's Law Dictionary*, 6th ed., 1990.

KEY CONSIDERATIONS FOR CONTRACTS

Financial institution business continuity needs go well beyond the standard SLA. Below are key points to consider in a contract. Bear in mind that financial institutions may not be able to successfully negotiate all of these provisions. Therefore, the provisions should be regarded as goals.

Service Level Agreements

Financial institutions must understand and agree to the terms and conditions of the SLA under which a third party vendor will deliver its telecommunications network services. It is important to note that a contractual SLA is only a commercial agreement and by no means a guarantee that the service will be delivered according to the SLA. The SLA should address your organization's key business requirements.

SLAs should cover (but are not limited to):

- The scope of monitoring and the exercise of control over the network;
- The up-time performance of the system;
- Escalation and response time procedures for problem identification and resolution;
- The prioritization and level of effort for restoring performance due to system degradations and/or outages;
- Effective change management practices with respect to handling maintenance, grooming, etc. in ways that would minimize or eliminate the potential for affecting the performance of your network during peak production hours; and
- Scheduled maintenance, planned maintenance, unplanned maintenance and their notification periods. (This is important given that the availability numbers often do not include the scheduled or planned maintenance.)

Tariff Clauses

Contracts frequently include a phrase making the contract subject to "all applicable tariffs." The phrase can bring in many volumes of rules, regulations and laws that may serve to override or limit the language negotiated for in other parts of the contract. To the extent possible, financial institutions should attempt to exclude all tariffs, except those explicitly enumerated in the contract. The listed tariffs should then be examined to ensure they are not inconsistent with the contract language and your business objectives.

Definitions

A definitions section is helpful in describing the meaning of certain industry terms or terms of art. For example, the word "diversity" has a very different meaning from provider to provider and from state to state. Words such as "diversity," "resiliency" and "availability" should also be defined in the contract so both parties clearly understand what is being bought/sold as part of the solution provided.

As Built Engineering Drawings

Financial institutions may wish to have an understanding of "as built" engineering drawings included in the contract. These drawings illustrate how the circuit was built and routed and help ensure that once the circuit is placed in service and accepted, diversity will be maintained. The contract should include a clause stating that full payment will not be made until all the drawings are viewed and accepted by your firm's engineering department.

Assignment Clause

Often in a contract, the vendor will reserve the right to subcontract any or all of the service to other providers. You should reserve the right to approve all of a vendor's subcontractors before the work

or service is given to them. Also, all terms to which the vendor has agreed must be included in the contract with the subcontractor. If the vendor undergoes a material change in ownership, you should have the right to terminate the contract on short notice without any early termination penalty. Any indefeasible right to use (IRU) created under the contract must be effective at the signing of the contract and constructed so as to survive assignment to a new owner and not be voided by bankruptcy. IRU is a legal construct used to create a synthetic title to a non-physical asset such as one wavelength of service in a fiber network.

Force Majeure Clause

This clause is usually very broad. It often includes language that excludes many events, some of which are the very events one is ordering the circuit to protect against. At times, the clause is written so broadly that even a minor event can be used as an excuse for failure to perform. Some examples of reasons not to perform include fire, flood, war, terrorism, power loss, lack of spares and labor disputes. Fire, flood, war and terrorism must be so extensive in scope as to cause direct disruption to both the primary path and the backup path concurrently. The key here is to ensure that your provider will try to restore your service on a priority basis as soon as possible.

One might also argue that power loss in its broadest sense should not be considered a *force majeure* event. The carrier should have batteries that last hours, generators that have local fuel for days and a fuel re-supply system that lasts weeks. Ideally, the only power failure that should be excluded is one that is regional in scope and lasts many days, combined with governmental action barring the delivery of fuel for a week or more. Similarly, lack of available spare parts should not be excused out of hand. To lack spares is fundamentally inconsistent with the service availability for which you are contracting. Labor disputes might arise, but they should not be used as an excuse when the labor dispute is under the providers' control.

In short, the goal of contract negotiations is to ensure that the financial institution and the service provider understand and agree to the terms under which the services will be rendered for the duration of the relationship.

VI. ONGOING RELATIONSHIP MANAGEMENT: TESTING, MONITORING AND AUDITING

KEY QUESTIONS

Note: Keep the following questions in mind as you read this section of the BITS Guide to Business-Critical Telecommunications Services. Then use the questions as part of your internal evaluation process.

83. Do you have a specific department or staff person(s) assigned to manage the relationship with your telecommunications services provider?
84. Have you established policies and procedures to facilitate telecommunications administration?
85. Does designated staff have the authority to oversee telecommunications service providers? For example, does designated staff have the authority to establish network objectives, principles and standards? Is a designated employee responsible for ordering and monitoring mission-critical circuits?
86. Do you know how your telecommunications provider will coordinate with other telecommunications providers in an emergency or national security event? Do you know whom to contact at your telecommunications service provider in times of emergency? Who will serve as your institution's "advocate"?
87. Have you established diversity criteria with your telecommunications service provider? Have you developed audit programs to ensure compliance with the criteria?
88. Have you educated your telecommunications service provider on the business processes supported by critical circuits and interdependencies with other financial institutions?
89. Have you discussed ways to involve multiple telecommunications providers to assess risks, geographic concentrations and single points of failure in primary and backup sites?
90. Have you established an ongoing relationship with your counterpart at the service provider? (He or she can provide a different perspective on issues that affect both companies and better prepare you for business interruptions. These relationships can mean the difference between getting access to good information during a disaster and getting only the information that is available to the general public.)
91. Does your provider perform business continuity/disaster recovery testing? Can your organization participate? Have you participated in business continuity/disaster recovery tests conducted by your telecommunications service provider? (These tests can be an opportunity to illustrate for your management the importance of information sharing and the value of the business continuity planning process. They can also illustrate the depth of your company's dependence on external resources.)
92. Do you understand the service provider's operating strategy and position within the larger regional or national infrastructure? (When your building is down, this information can help you explain the situation to your senior management and provide realistic expectations for service restoration.)
93. Has the telecommunications service provider tested its backup facilities to ensure their availability?

94. Do you regularly review your company's resilience requirements with your telecommunications service provider?

95. Does your service provider notify you of network updates, proposed engineering downtime or other changes in normal operations?

96. Do you have primary and alternate methods of contacting your provider (e.g., telephone numbers, pagers, email addresses) for use during times of crisis?

97. Does your telecommunications service provider have alternative contact information for your response team members?

OVERVIEW

The final step in the vendor management process is ongoing oversight, monitoring and relationship management. This includes establishing a rapport with and setting expectations for your telecommunications service provider.

Financial institutions should start by expanding their expectations of the telecommunications service provider and ensuring the provider buys in to your strategy. The service provider should know your institution's architecture and strategic plan. To this end, you might consider establishing a department with clear objectives and well defined roles and responsibilities.

Give the service provider time and attention to demonstrate its commitment. Define the architecture and establish network goals so you will know when you reach your objectives and others at your company can see the impact your strategic plans have made. Update the service provider on strategy changes, business plan changes and other business climate issues and request a dedicated contact point with the service provider for consistency and continuity. Explain how you expect the service provider to behave and grade it accordingly. True business partnerships are possible when you are clear about expectations and discuss the provider's "report card" periodically.

Financial institutions should establish budgeting and auditing processes to support their policies. Examples of telecommunications budgeting and auditing processes include:

- Invoice processing tied to projects;
- Invoice processing tied to expenses related to service calls or other technical field work;
- Billing analysis of vendor bills related to telecommunications;
- Budget planning assistance for management; and
- Project expense tracking.

VII. CONCLUDING RECOMMENDATIONS

The following recommendations to financial institutions are essential for achieving resiliency:

- Know your mission-critical functions (and dependencies) and understand your acceptance of business risk.
- Know the extent to which your continuity of mission-critical business operations relies on the diversity, recoverability, redundancy and resiliency of your telecommunications requirements.
- Identify mission-critical services and functions that pose the highest risk to the institution if they are disrupted.
- Analyze and assess the vulnerabilities and threats to mission-critical services. Threats exercise vulnerabilities and include natural disasters, malicious actions, cyber attacks and exploitation of single points of failure.
- Understand how specific diversity, recoverability, redundancy and resiliency requirements affect your institution's ability to continue operations.
- Understand that standard contracting with multiple telecommunications service providers alone may not provide the necessary diversity, recoverability, redundancy and resiliency.
- Establish a trusted relationship with your telecommunications service provider (or system integrators/managed service providers) by conducting the necessary due diligence and oversight to detailed service engineering and established documentation of SLAs to assure requirements are clearly stated. Structure contracts to address these needs on a continuing basis and include regular metrics.
- Take advantage of U.S. government sponsored programs that permit the financial services sector to use recovery and response tools such as the TSP, GETS and WPS.
- Understand that engineering high diversity, recoverability, redundancy and resiliency services may cost more than standard services.
- Continue to assess emerging telecommunications and alternate transport technologies to determine whether they could provide the services to further assure the necessary levels of diversity, recoverability, redundancy and resiliency are achieved.

APPENDIX A

GLOSSARY

Alternative routing	<p>The use of another path to transmit information, in some cases with a different medium. For example, using different networks when the normal network is rendered unavailable.</p>
Asynchronous transfer mode (ATM)	<p>A high-speed switching method using fixed-length cells of 53 bytes to support multiple types of traffic.</p> <p>Like frame relay, ATM is a packet-switched data network protocol using permanent virtual circuits (PVC) to route data. However, because ATM uses fixed-sized cells to transfer the traffic, and because it doesn't use data store-and-forward, it can better handle time-sensitive traffic like real-time voice and video.</p> <p>ATM can carry high-speed, constant bit-rate traffic in a predictable way, which is important for mission-critical applications like real-time financial transactions.</p> <p>ATM networks are highly resilient to infrastructure failures. They are designed with many nodes and routes between the nodes, allowing many options for traffic to bypass network problems. End-to-end network availability is typically between 99.7% and 99.9%, depending to a large extent on the performance of local tails to the customer office.</p>
Best practice	<p>Measures proven effective in certain situations to promote resiliency or mitigate risks or vulnerabilities.</p>
Frame relay service	<p>Frame relay is designed to handle variable volumes of traffic of different types, making it the ideal solution for reliable LAN-to-LAN interconnection. It is most commonly used for applications requiring between 64 kbs and 2 mbs.</p> <p>Many of the applications carried over LANs are bandwidth-hungry. Often they need the LAN for short periods of time, resulting in "bursty" traffic patterns (periods of high volume alternating with periods of low volume). Frame relay is designed precisely for this type of traffic flow to ensure bandwidth is used efficiently. It offers high efficiency, minimal network delay, high availability, prioritized service levels and protocol-transparent transmission, enabling many diverse traffic types to be transported over a common, resilient and integrated network.</p> <p>A typical frame relay network is highly resilient against network failures. It is designed with many nodes and routes between the nodes, allowing many options for traffic to bypass network problems. Network availability is typically between 99.7% and 99.9%, depending to a large extent on the performance of local tails to the customer office.</p>
National security/emergency preparedness (NS/EP)	<p>The telecommunications services used to maintain a state of readiness or to respond to and manage any event or crisis (local, national or international) that does or could cause injury or harm to the population; cause damage or loss of property; or degrade or threaten the NS/EP posture of the U.S. (NCS, Telecommunications Service Priority System for NS/EP Service User Manual</p>

	(NCS Manual 3-1-1), March 1998.)
Point of presence (POP)	The local telecommunications exchange that services a customer's premises.
Public switched telephone network (PSTN)	The public local and long-distance telephone systems that are used for switched and non-switched services.
Separacy	Commonly used in the United Kingdom to mean end-to-end separation. Separacy ensures that specified circuits are physically separated throughout the network so that there are no common exchanges, interconnection points or cable routes. Provides physical and logical separation of a circuit or system from source to destination.
Service level agreement (SLA)	A formal agreement between a service provider and its customer that covers the nature, quality, availability, scope and response of the service provider. The SLA should cover day-to-day situations and disaster situations, as service needs may vary in a disaster. It should also cover service level guarantees.
Single point of failure	The single source of a service, activity and/or process (i.e., no alternative exists), whose failure would lead to the total failure of an activity and/or dependency.
Standard services	Implies no customer priorities or no special customer considerations.
Synchronous Optical Network (SONET)	An interface standard for telecommunications transmission over fiber-optic cables.
Synchronous digital hierarchy (SDH)	<p>A fiber-centric technology commonly configured in resilient ring architecture, so that if any network failure occurs, service is automatically re-routed along an alternative path. The network terminating equipment at a customer's premises would normally be connected back to independent network nodes by completely separate fiber paths, routed along different ducts, and fed into the customer's premises at separate entry points. This ring architecture provides a high level of availability.</p> <p>SDH is also used as a point-to-point service in many applications. Customers wishing to take advantage of the resilience of a ring architecture should qualify this with the provider.</p>
Telecommunications Service Priority (TSP)	The TSP Program provides NS/EP users priority authorization of telecommunications services that are vital to coordinating and responding to crises. The TSP Program defines these telecommunications services as the transmission, emission or reception of intelligence of any nature, by wire, cable, satellite, fiber optics, laser, radio visual or other electronic, electric, electromagnetic or acoustically coupled means, or any combination thereof. As a result of hurricanes, floods, earthquakes and other natural or man-made disasters, telecommunications service vendors may become overwhelmed with requests for new telecommunications services and requirements to restore existing telecommunications services. The TSP program provides service vendors with a Federal Communications Commission (FCC) mandate for prioritizing service requests by identifying those services critical to NS/EP. A telecommunications service with a TSP assignment is assured of receiving full attention from the service vendor before a non-TSP service. The procedure for applying for this designation and frequently asked questions about the TSP

	Program can be found at the TSP website, http://tsp.ncs.gov/ .
Threat	Anything with the potential to damage or compromise the communications infrastructure or some portion of it. ³⁰
Transparency	The extent to which the customer has visibility of the services provided and the seamless interaction of those services.
Vulnerability	A characteristic of any aspect of the communications infrastructure that renders it, or some portion of it, susceptible to damage or compromise. ³¹

³⁰ See *FCC Network Reliability and Interoperability Council VI Homeland Security Physical Security Focus Group (1A) Final Report*, Issue 3, December 2003, p. 39, at www.nric.org.

³¹ See *FCC Network Reliability and Interoperability Council (NRIC) VI Homeland Security Physical Security Focus Group (1A) Final Report*, Issue 3, December 2003, p. 39, posted at www.nric.org.

APPENDIX B

ACKNOWLEDGEMENTS AND REFERENCES

The *BITS Guide to Business-Critical Telecommunications Services* was developed by a small, dedicated team of professionals from BITS member organizations, one non-member organization, and BITS staff. It is based on meetings and calls of the BITS Telecommunications Working Group and BITS Crisis Management Coordination Working Group, and draws on the following sources:

- BITS white paper, “Telecommunications for Critical Infrastructure: Risks and Recommendations” (December 2002)³²
- BITS Forums on Telecommunications Resiliency (June 2002 and June 2004)
- The National Security Telecommunications Advisory Committee Financial Services Task Force Report (April 2004) (See [http://www.ncs.gov/nstac/reports/2004/Financial%20Service%20Task%20Force%20Report%20\(April%202004\).pdf](http://www.ncs.gov/nstac/reports/2004/Financial%20Service%20Task%20Force%20Report%20(April%202004).pdf))
- The Alliance for Telecommunications Industry Solutions’ Diversity Assurance Pilots
- BITS’ and the National Communications System’s Joint Telecommunications/Financial Services Sector’s Pilot Recoverability Assessment Information Exchange³³
- The United Kingdom’s National Infrastructure Security Co-Ordination Centre and “Good Practices Guide on Telecommunications Resilience” (May 2004) (See www.niscc.gov.uk.)
- The Lower Manhattan Telecommunications Users Working Group’s “Building a 21st Century Telecom Infrastructure: Findings and Recommendations”
- The Federal Communications Commission’s Network Reliability and Interoperability Council (NRIC) best practices (See www.nric.org.)
- BITS Lessons Learned: Northeast Blackout of 2003 (October 2003)
- Securities Industry Association Business Continuity Committee Critical Infrastructure Guidelines (May 2004 draft)
- SAIC/ISAC “Securing the Wireless Environment,” March 2004
- “Securing an Open Society: Canada’s National Security Policy” (April 2004) (See http://www.pco-bcp.gc.ca/docs/Publications/NatSecurnat/natsecurnat_e.pdf.)
- “Liquidity Effects of September 11, 2001” by James McAndrews and Simon M. Potter, *Economic Policy Review*, November 2002

³² “Telecommunications for Critical Infrastructure: Risks and Recommendations” was prepared for and distributed to the CEOs of BITS/FSR member companies. The paper outlines key risks and provides more than two dozen recommendations for the financial services, telecommunications and government sectors. The paper outlines a number of major areas of risk: network vulnerabilities such as inadequate telecommunication line diversity; lack of physical redundancy; existence of critical points of failure; limited information-sharing ability; lack of business and political processes necessary to overcome legal and privacy issues; and the uncertain impact of emerging technologies and integration with existing technologies.

³³ The Joint Telecommunications/Financial Services Sectors Pilot Recoverability Assessment Information Exchange was sponsored by the National Communications System (NCS), an entity of the Department of Homeland Security; the National Coordinating Center for Telecommunications (NCC), a joint government-industry operational entity with focus on coordination of telecommunications support during National Security and Emergency Preparedness events; and BITS. The objectives of the Assessment were to: a) examine a specific geographic area with a high concentration of critical financial functions, which, if not available, could have implications for national security and emergency preparedness; b) determine what telecommunications assets and services support these financial functions; c) highlight systemic infrastructure issues and potential mitigation strategies; and d) recommend more efficient ways to conduct similar assessments in other geographic areas. The Assessment was governed by legal and business rules to ensure protection of proprietary and confidential data and to ensure compliance with antitrust laws.

- “Payments Risk Committee Best Practices to Assure Telecommunications Continuity for Financial Institutions and the Payments and Settlement Utilities,” September 2004 (See <http://www.newyorkfed.org/prc/telecom.pdf>.)
- National Communications System’s “Critical Facilities Report” (May 2004)

The following individuals made significant contributions to this document:

Andrew F. Bach, Securities Industry Automation Corporation
 Roger Callahan, Bank of America Corporation
 John Fowler, Northern Trust Corporation
 Melvyn Musson, Edward Jones Investments
 Susan Vismor, Mellon Financial Corporation
 Catherine Allen, BITS
 John Carlson, BITS
 Cheryl Charles, BITS
 Teresa Lindsey, BITS
 Susanna Space, BITS
 Heather Wyson, BITS

BITS would also like to acknowledge the important role that John L. Burke played in guiding and supporting the efforts of the BITS Telecommunications Working Group. John served as BITS’ legal counsel for many years and was a partner at Foley Hoag, LLP. John passed away in June 2004.

In addition, the following individuals reviewed or provided helpful comments and edits on drafts of this document:

Ken Buckley, Federal Reserve Board of Governors
 John Compitello
 Cristin Flynn Goodwin, BellSouth Corporation
 Ernie Gormsen, Verizon
 John Ingold, BITS
 Doug Langley, BellSouth Corporation
 Chuck Madine, Federal Reserve Board
 Donald Monks, The Bank of New York Company, Inc.
 Michael Obiedzinski, Depository Trust and Clearing Corporation
 Bruce Parker, Foley Hoag, LLP
 George Perretti, Depository Trust and Clearing Corporation
 Jane Polk, National Communications System
 Karl Rauscher, Bell Labs Network Reliability & Security Office of Lucent Technologies
 Eric Robbins, Federal Reserve Bank of Kansas City
 Carl Rosenberger, The Bank of New York Company, Inc.
 Howard Spro, Securities Industry Association
 Harry Underhill, AT&T
 Didier Verstichel, SWIFT
 Ciro Vitiello, The Bank of New York Company, Inc.
 Colin Whittaker, Association for Payment Clearing Services (APACS)
 Dan Wing, Cisco Systems
 Al Wood, The Clearing House

BITS Crisis Management Coordination Chairman: Allan Woods, Mellon Financial Corporation

BITS Telecommunications Working Group Chairman: John DiNuzzo, Bank of America Corp.

BITS Telecommunications Working Group Participants

AT&T	MCI
Bank of America Corporation	Mellon Financial Corporation
The Bank of New York Company, Inc.	National Communications System
BellSouth Corp.	Northern Trust Corporation
Booz Allen Hamilton	Office of the Comptroller of the Currency
Citigroup Inc.	The Options Clearing Corporation
The Clearing House	The PNC Financial Services Group, Inc.
Compass Bancshares, Inc.	Qwest
Compitello Associates	Raytheon Company
Credit Suisse First Boston	SBC Communications Inc.
Edward Jones	Securities Industry
Federal Communications Commission	Automation Corporation (SIAC)
Federal Reserve Board	Securities Industry Association (SIA)
Federal Reserve System	SouthTrust Bank
Foley Hoag, LLP	Sprint
General Services Administration	Synovus
Harris Bankcorp, Inc.	U.S. Department of Homeland Security
Hibernia Corporation	U.S. Department of Treasury
JPMorgan Chase & Co.	Verizon
LaSalle Bank Corporation	Zeichner Risk Analytics, LLC
Lucent Technologies Bell Labs	

About BITS

BITS was created in 1996 to foster the growth and development of electronic financial services and e-commerce for the benefit of financial institutions and their customers. A nonprofit industry consortium that shares membership with The Financial Services Roundtable, BITS seeks to sustain consumer confidence and trust by ensuring the security, privacy and integrity of financial transactions. BITS works as a strategic brain trust to provide intellectual capital and address emerging issues where financial services, technology and commerce intersect, acting quickly to address problems and galvanize the industry. BITS' activities are driven by the CEOs and their appointees—CIOs, CTOs, Vice Chairmen and Executive Vice Presidents—who make up the BITS Executive Committee and BITS Advisory Council. For more information, go to www.bitsinfo.org.

BITS
1001 PENNSYLVANIA AVENUE, NW
SUITE 500 SOUTH
WASHINGTON, DC 20004
202-289-4322
WWW.BITSINFO.ORG

APPENDIX C

ALTERNATIVE/EMERGING TECHNOLOGIES AND ALTERNATE TRANSPORT MECHANISMS

Alternative technologies such as satellite, laser, microwave and spread spectrum wireless can offer alternate routings for the most critical communications if reliance on more than terrestrial transport is considered necessary.³⁴ Using these wireless technologies can often overcome hurdles imposed by local regulators reluctant to permit pavement to be torn up for new or alternative fiber conduits in and out of a municipality. These technologies are offered as options (not requirements) for financial institutions to consider when developing business continuity plans and assessing appropriate levels of resiliency for a given function. Financial institutions may consider the following sample alternative technologies:

Satellite Technology

The Department of Defense (DOD) has relied on satellite communications as part of its defense communications structure for several decades. Satellite communications links efficiently extend the reach of terrestrial communications systems to distant areas and provide an independent infrastructure for alternative routing of traffic in an emergency. Most important, because their principal assets are in space, satellite communication systems with diverse ground sites can continue to function during disasters (e.g., natural disasters or terrorist attacks) that might render other communication methods inoperable.

Aside from the obvious benefits, which include large coverage areas and high-speed and high-quality transmission, satellites offer much-needed operational flexibility. Satellite communication networks offer users the ability to change network size and traffic flows in addition to monitoring and controlling equipment in a timely manner. Presently, agencies across the U.S. government lease broadband circuits on a variety of commercial satellites in geostationary orbit (an altitude of 30,000km) for both operational and emergency communications. In addition, the U.S. government owns a number of military-unique communications satellites in the same orbit that offer circuits with added protection, making them largely immune to jamming and other kinds of attack.

Although satellite communications offer many benefits, they do have a few drawbacks. Severely inclement weather (hurricanes, for example) can temporarily interrupt satellite transmission in the affected area, and other transmission delays in satellite circuits may affect certain types of applications.

Laser Technology

Private sector companies use laser-based technologies to transfer data in metropolitan areas. These optical-based applications use a series of connectors to “beam” information between nodes. Laser transmissions are difficult to detect; however, the technology is not a viable option for rural areas because the maximum distance between transmission links is only 500 meters. In addition, natural disasters and weather phenomena hamper laser communications capabilities.

Microwave Technology

Narrowband microwave technology is similar to broadcasting from a radio station. Unlike laser technology, which requires a direct line of sight, microwave technology uses the portion of the electromagnetic spectrum that exists below infrared frequencies but above normal radio frequencies to transmit voice and data communications (18.82 to 19.205 GHz).

³⁴ See NSTAC FSTF Report, April 2004.

Microwave radio links are used to integrate a broad range of networks from fixed and mobile communication networks. At present, many of the data communications services offered by mobile cellular networks are supported by microwave technology. Microwave technology takes less time to install than wire alternatives and can provide greater flexibility. Although the cost of microwave technology may be higher than other options, microwave technology is highly resistant to outside interference. Possible drawbacks are that the broadcast range of microwave technology is roughly 5,000 square meters, and the transmissions cannot travel through steel or load-bearing walls.

Spread Spectrum Technology

Spread spectrum technology uses wideband, noise-like signals to spread a given radio signal over a wide spectrum of radio frequencies. In standard narrowband communications, each channel operates over a tiny segment of the radio spectrum and the FCC regulates the spectrum by assigning or licensing segments. Spread spectrum technology allows multiple radio signals to operate in an open, unlicensed band with little or no interference. Spread spectrum and narrowband signals can share the same band simultaneously. The variance in spread spectrum signals makes the transmission difficult to detect, intercept or demodulate.

Wireless

Financial institutions need to assess the security threats associated with Wireless Local Area Networks (WLANs) and their security needs with respect to the confidentiality, integrity and availability of their information assets. WLANs are vulnerable to denial of service attacks such as network jamming. As such, they should not be used as the only means to access the organization's networks and systems. Load balancing across multiple access points should be implemented to mitigate the risk of an access point being inaccessible due to flooding of network packets at a particular access point.

Wireless technologies demand careful attention and planning given the risks:

- There is no *quality* of service component to wireless technology. Significant packet loss should limit the implementation of WIFI to mission-appropriate infrastructure.
- WIFI is composed of complex technology with complicated paths for data management and a wide array of technology utilization.
- Unauthorized connectivity (e.g., rogue access points) presents data interception and other serious threats.
- WIFI is vulnerable to viruses, denial of service attacks, unauthorized access, traffic analysis, eavesdropping, man-in-the-middle attacks and session hijacking.
- The frequencies in which these technologies operate are currently unregulated and shared with many other devices that emit radio signals. This presents potential interference problems (e.g., decreased range) which must be managed.

Concerns:

- Expect outages if you use wireless exclusively.
- Don't rely exclusively on physical security, build logical security in deeply.
- Consider all types of wireless (including cellular) in planning.
- Familiarize yourself with current and emergent technology. (Stay ahead of the curve.)
- Don't always adopt immediately. (Wireless technology changes rapidly.)

Financial institutions should consider alternative sources of backup power, depending on circuit layout, when the loss of power at one institution could impact services provided through other institutions because of interdependencies between these institutions and their critical financial services. In coordination with their telecommunications service providers, financial institutions should identify those facilities that merit backup power for specific technologies (e.g., SONET,

ATM) and network hardware and network points of presence (e.g., uninterruptible power supplies and standalone electrical generators).

IP and Voice Over Internet Protocol

Shortcomings in hardware and legacy applications can be overcome by utilizing IP networks. A shift toward IP networks might raise latency issues depending on access to broadband technology. Traditionally robust architectures such as public switch telecommunications network (PSTN) and X.25 links are moving toward an IP base. This could be seen as a single point of failure situation. However, though the typical IP network (the public Internet for example) is a best-effort system with few guarantees of service quality, the IP networks offered by service providers are often closed systems with high-quality service guarantees.

Voice over IP (VoIP) is quickly emerging as an alternative to more traditional methods of voice communication. VoIP appears to provide more resiliency for customers, but it is too early to be considered robust enough for heavy-duty commercial use. Security, bandwidth, latency and interoperability issues are major concerns for financial institutions. Risk managers must continue to assess changes such as the migration to VoIP to determine whether these next generation solutions provide the necessary levels of resiliency, redundancy and diversity.

While the trend toward voice and data convergence may reduce costs and enhance functionality to financial institutions, they also expose vital telecommunications networks to traditional forms of Internet attack, such as worms and viruses. For example, a large-scale distributed denial of service (DDoS) attack could degrade call performance by slowing voice packet arrival at a given destination and effectively cut off voice communication.³⁵ VoIP networks have an inherent weakness when it comes to delays in the transmission of packets carrying the voice traffic.³⁶

Alternate Transport Mechanisms for Financial Institutions

The financial services sector has several key private telecommunications networks provisioned and/or managed by sector infrastructure organizations. Many of these networks are increasingly migrating away from older or more proprietary technologies to IP-based telecommunications. Some of these alternatives rely on different routes than those used by telecommunications service providers, which can provide greater geographic diversity. These alternatives may provide alternative means of communication should an institution lose connectivity through traditional means.

Secure Financial Transaction Infrastructure. Secure Financial Transaction Infrastructure (SFTISM) is a financial industry network solution that combines recovery, redundancy and diversity solutions to provide continuous telecommunications resiliency. SFTISM is the result of a telecommunications strategy employed to achieve assurance of redundancy and diversity for a critical financial industry function provided by the Securities Industry Automation Corporation (SIAC).

SIAC designed SFTISM to be a robust, resilient infrastructure with no single point of failure, and very low end-to-end latency and skew. It consists of a dynamic configuration with remote management and testability capabilities, and an effective event monitoring and reporting structure that relies on several key elements: migration to IP and elimination of legacy protocols, consolidation of traffic

³⁵ Telecommunications and network providers argue that there are effective ways to configure networks so that malicious activity does not interfere with voice traffic. They also assert that certain technologies can mitigate denial-of-service and distributed-denial-of-service attacks within an enterprise.

³⁶ This delay is also called "jitter." Unlike the Internet, the Public Switched Telecommunications Network does not have this problem because it is tightly clocked (at greater expense and with restrictions on how equipment might be deployed) and the PSTN has effectively no buffering.

onto fewer, larger pipes by replacing multiple special purpose circuits, and location of SIAC “□ emarks” away from data centers. Primary SFTISM customers include the New York Stock Exchange, the American Stock Exchange, other U.S. market centers, market data providers, and clearance and settlement institutions.

SFTISM follows stringent data communications architecture requirements. It provides bandwidth guarantees per internal network and guaranteed bandwidth per application. SFTISM also ensures customers’ presence at a minimum of two access centers and protects one customer from another through route and filter management. Its access centers rely on several service providers’ services and extranets to support multiple applications and offer easy capacity reallocation and expansion. Network operations centers provide customers two remote, out-of-band management teams that can take over all operations if one of them is destroyed., ensuring continuous operation. These two centers have been engineered and equipped to be fully self sufficient and to sustain operations for several consecutive days in the event of a natural or manmade disaster. In addition, SIAC audits its circuit routing on a set schedule to ensure the regular grooming that telecommunications service providers perform does not compromise diversity. Recently, the Securities Industry Association (SIA) and Securities and Exchange Commission (SEC) recognized SFTISM as an industry-wide solution.³⁷

Securely Managed and Reliable Technology. Securely Managed and Reliable Technology (SMART) is a centralized, end-to-end managed communications infrastructure provided by DTCC. SMART connects a nationwide complex of networks, processing centers and control facilities. Each is highly secured; engineered with multiple, independent levels of redundancy; and capable of processing DTCC’s entire clearance and settlement workload. DTCC ensures the availability and reliability of the settlement infrastructure by extending SMART onto members’ operating premises.

SMART is unique in that DTCC owns and manages all elements of the network from its processing complex all the way through to the customer premises, including the hardware and software and even the relationships with multiple telecommunications carriers, to diversify connections and to ensure continuity of service. Because of this, DTCC guarantees consistent service levels, ensuring that customers have needed capacity, reliability and consistency from end to end. This end-to-end management of the entire complex makes it possible for DTCC to routinely exercise contingency capabilities without coordinating special industry-wide tests. For example, on a day-to-day basis, DTCC routinely reroutes a member’s settlement instructions through different parts of the networks, into different processing sites. Due to the routing capabilities built into SMART, this rerouting occurs without any involvement of member firms. Rather than maintaining business continuity capabilities in standby, all sites, networks and management centers are treated as a unified complex that is always operational. Since DTCC owns all elements of the network, SMART is registered with the Department of Homeland Security for priority restoration in the event of an outage. This end-to-end managed complex is unique to SMART among financial services infrastructures in the U.S.

Another advantage for customers connected to SMART is that access is streamlined into all of DTCC’s services. This means DTCC customers can simplify their networks and consolidate location- and application-specific circuits into fewer, larger, general-use connections.³⁸

³⁷ For additional information on SFTISM, see <https://sfti.siac.com/sfti/index.jsp>.

³⁸ For additional information on SMART, contact Michael Obiedzinski at 212-855-1818 or email mobiedzinski@dtcc.com.

APPENDIX D

RECOVERY PROCESSES OF TELECOMMUNICATIONS COMPANIES

The National Coordinating Center (NCC), which serves as the information sharing and analysis center for the U.S. telecommunications sector, is managed by the National Communications System (NCS). Representatives of the major telecommunications service providers work together to respond to major NS/EP events. The following is an overview of the process that the NCC follows in responding to incidents and events.

The NCC responds to events based on the potential impact of the event, ranging from limited impact to more serious events. Established thresholds (scope and time) determine when response activities are automatically elevated to another management level. In addition, customer SLAs define required responses to these events. Recovery efforts also include mutual aid agreements, in which carriers and service providers elect to enter agreements for collaborating to supply materials and equipment to those in need to restore service in the wake of an emergency.

Network operations centers have established incident management plans and communication protocols in response to event triggers:

- **Low Impact:** Coordination of low-impact events affecting multiple carriers requires communication between and among the operations control and customer care centers of each organization, but does not necessarily require coordination of emergency operations centers, network operations centers or executives of the affected organizations.
- **Medium Impact (e.g., severe storm, flood or minor earthquake):** Involves communication among all levels including emergency operations centers and network operations centers. However, senior executives of the affected organizations are not involved at this time. Account teams are looped into the process for constant communication with customers. NCC representatives may be involved.
- **High Impact (e.g., catastrophic events, 9/11):** Involves coordination and communication among all parties at all involved carriers, from the customer care center to the executives, NCC representatives and government agencies. Senior executives are involved due to the severity of the event and can provide additional resources as necessary. NCC representatives are involved in these events.

Customer communications occur through dedicated account teams available 24X7, and the teams serve as customer advocates for a financial institution in the event of a service malfunction. Account teams play an important role in addressing end-to-end service problems involving more than one carrier. If the problem goes beyond the initial carrier's network, the original carrier generally coordinates with the other involved carriers and retains control and responsibility from the customer's perspective.

During a Low-Impact event, such as a rural cable cut of short duration:

- Carriers monitor their networks 24X7.
- Operations Control Centers (OCCs) may include:
 - Switching (toll and local centers, etc.)
 - Facilities (fiber, cable, distributed electronics, etc.)
 - Technologies (ATM, SONET, etc.)
 - Regional
- As necessary, the OCC coordinates with customer care center (CCC) and field forces.
- CCC and field forces interface with customers.
- Inter-carrier coordination depends on the nature of the event.

During a Medium-Impact event, such as a switch outage (of short duration) or cable cut in a metropolitan area:

- Some events may immediately require a Medium-Impact event response.
- Some Low-Impact events may evolve to a higher level as a result of recovery time or cumulative impact.
- OCC coordination is supplemented by the emergency operations center (EOC) and the network operations center (NOC).
- Account teams join the event coordination.
- NCC industry representatives engage with the NOC.
- Multiple telephone bridges are now in operation:
 - NOC, EOC, OCC, CCC bridges (NCC representatives are on these bridges.)
 - Technical bridges
 - Operational bridges
 - Account team bridges
- Inter-carrier coordination is highly probable.

During a High-Impact event (e.g., Northridge and Loma Prieta earthquakes, Hurricane Andrew, the 9/11 attacks):

- Corporate executives enter the event, interacting with NOC, NCC representatives and account teams.
- NCC representatives alert the appropriate government agencies.
- Account teams are now engaged with all elements of the coordination effort and in contact with affected customers.
- Multiple inter-carrier coordination is underway.
- Unless superseded by a higher priority (e.g., TSP), coordination decisions and priorities are made at the NOC and executive levels and are based on input from all elements of the restoration effort.

NCC companies also engage in post-event evaluations that may include:

- “After-action” studies conducted by NCC and NSTAC:
 - Over sixty issues from the 9/11 response were developed by NSTAC, with perimeter control being the primary concern.
 - Previous studies have identified the need for coordination between telecommunications and electric power infrastructures.
- Response to Hurricane Andrew led to the development of a voluntary mutual aid agreement for use by any two parties:
 - Has been used several times between U.S. and Canada.
 - Agreement was reviewed and revitalized in NRIC VI.
- The FCC’s NRIC has developed library of industry best practices:
 - Provides a menu of options.
 - Not all practices are applicable to every organization.

Telecommunications service providers typically restore their own control services and order wires prior to any customer services. Telecommunications service providers then adhere to the TSP rules to restore and provision the NS/EP priority services of their customers by:

- Restoring TSP services assigned restoration priority 1
- Provisioning emergency TSP services assigned provisioning priority E
- Restoring TSP services assigned restoration priority 2, 3, 4 and 5
- Provisioning TSP services assigned provisioning priority 1, 2, 3, 4 and 5

TSP restoration priority may affect automatic as well as manual restoration processes.

Restoration time also depends on several factors, most notably geographic location. If disruption occurs in a metropolitan area (as opposed to a rural area), restoration can take much longer due to:

- The presence of multiple cables, technologies and carriers;
- Difficult and dangerous access;
- Perimeter access control (especially after an intentional attack);
- Overlapping jurisdictions; and
- Governmental restrictions.

Response and recovery activities are incident-dependent. Other factors affecting recovery time include:

- Scale of the disaster site (how big);
- Scope of the disaster impact (how bad);
- Access control to damaged assets and customer premise;
- Prevailing weather conditions;
- Status of electric power infrastructure;
- Security and safety considerations; and
- Regulatory demands (e.g., TSP).

Other factors to consider about recovery:

- A component failure *may* have no impact on the function supporting the mission.
- Component recovery (repair) is not the only way to recover the function.
- There may be no functional impact on the mission *if* contingencies are in place and perform as planned.

The telecommunications industry believes it has developed a redundant and diverse system. The system is called Signaling System 7 (SS7) or the 5 “9s” network. According to NCC companies, the system can be engineered to maintain continuity for 99.999% of the time based on the following characteristics:

- SSPs, STPs and SCPs have dual processors.
- STPs and SCPs are deployed in geographically dispersed mated pairs.
- Signaling links are engineered for route diversity and physical separation.
- SS7 links are specially marked in databases for special handling.
- SS7 links have priority over services with TSP.

APPENDIX E

CONSOLIDATED LIST OF KEY QUESTIONS FOR RISK MANAGERS

The questions below are the starting point for a rigorous examination of a financial institution's telecommunications environment. The answers will help financial institutions achieve the necessary levels of diversity, recoverability, redundancy and resiliency.

Each question appears in the body of the paper; see the corresponding question number in the appropriate section. In some cases, the same or similar questions appear in more than one section to ensure they are addressed in each applicable area.

Table 2: Consolidated List of Key Questions for Risk Managers

Indicate here if not applicable	Q no.	Question	Comments
II. Risks, Requirements and Strategies			
	1	Are your financial institution's critical business requirements for diversity, recoverability, redundancy and resiliency of telecommunications detailed in your institution's business continuity plan? Are those requirements aligned with the terms of your contract for the service(s) provided by your telecommunications service provider(s)?	
	2	Have you conducted a risk assessment that considers the respective loss of telecommunications services to each of your critical applications?	
	3	Have you validated the accuracy of your assumptions for diversity, recoverability, redundancy and resiliency with your telecommunications service provider?	
	4	Do you have a full and complete list of your mission-critical telecommunications services and the critical systems that support them? Have recovery times for each critical telecommunications service been identified?	
	5	Are recovery time guarantees included in SLAs with your telecommunications service provider?	
	6	Are the needs for diversity, recoverability, redundancy and resiliency adequately conveyed to the service provider?	
	7	Have you provided your telecommunications service provider with information on your diversity, redundancy and	

Indicate here if not applicable	Q no.	Question	Comments
		resiliency requirements and maximum tolerable recovery times?	
	8	Have you identified business-critical telecommunications services in order of importance or criticality that are within your own premises? Do you know who is responsible for these critical services that are within your premises? Is the implementation of your requirements visible all the way to the point of handoff to the telecommunications provider outside your institution's facilities?	
	9	If you have a foreign-based telecommunications service provider, have you assessed risks? Are the risks consistent with those of your US-based telecommunications provider(s)? If not, have you implemented controls to mitigate these risks?	
	10	Have you analyzed interoperability issues with legacy systems and use of emerging technologies (e.g., Voice over Internet Protocol, wireless, other non-wireline networks)? Are they compatible and consistent with your business continuity plans?	
	11	Have you established corporate policies and procedures to manage your institution's relationship with telecommunications service providers?	
	12	Have you identified for the service provider those mission-critical telecommunications circuits that qualify for the Telecommunications Service Priority (TSP)? Has your telecommunications service provider verified TSP-designated circuits? Have you considered obtaining TSP protection for all eligible single-threaded circuits?	
	13	Do you understand your local telecommunications service provider environment and service options?	
	14	If your institution uses more than one telecommunications service provider, what assurances do you have that there are no physical routings or single points of failure common to both providers? What process does the provider use to guarantee these assurances? Have you asked your telecommunications service providers how they will retain redundancy and diversity requirements when provisioning or "grooming" your critical circuits?	
	15	<p>Have you identified and configured communications circuits that require specific physical diversity minimums?</p> <ul style="list-style-type: none"> • Are any parts of the cabling, for example, exposed to external contractors or others beyond your control? • Who is responsible for these areas? • Do any third party components fall between areas of responsibility? 	
	16	Do all of your services leave your premises in the same cable? Are they all in the same duct?	

Indicate here if not applicable	Q no.	Question	Comments
	17	Do you know where in the telecommunications service provider's core network your network services connect, how they are connected, and the physical routings they take once they leave your premises?	
	18	Do you know if critical services are routed via different network components so that a failure of one component will not affect all critical services? Have you specifically asked for this service?	
	19	Have you considered an "active-active" diverse geographic business operations and architecture, where possible, for your most critical business operations to minimize dependency on assured redundancy and diversity of telecommunications services?	
	20	Do you consider the technologies applied by your telecommunications service provider to be adequate? For example, do you use Synchronous Optical Network (SONET) or equivalent "self-healing" technology to connect data centers to carrier central offices to make connections as resilient as possible?	
	21	Have you evaluated the resiliency of SONET rings serving your circuits?	
	22	Have you discussed with your telecommunications service provider specific concerns regarding single-threaded circuits, SONET rings, and physical versus logical SONET?	
	23	If you rely on single-threaded circuits, have you assessed whether this approach is consistent with your institution's risk assessment and business continuity strategy? If not, can you work with your telecommunications service providers to implement a more robust technological alternative?	
	24	Have you considered concentrating multiple circuits on fewer, higher bandwidth circuits in order to simplify connectivity and better assure diversity?	
	25	Have you extended frame relay networks to avoid network-to-network interconnects (NNIs) and reduce complexity and single points of failure inherent with some NNI connections?	
	26	Have you considered the alternative technologies and services available to address potential "last mile" and inter-facility bottlenecks and single points of failure that cannot be resolved with conventional services?	
	27	Have you assessed the risks and implemented mitigating controls for Voice over IP systems taking into account the need for a robust network monitoring, information security program, and sufficient backup systems?	
	28	Have you examined and assessed potential single points of failure of your institution's information security program	

Indicate here if not applicable	Q no.	Question	Comments
		including physical placement of routers, switches and common power sources?	
	29	Are you aware of regulatory requirements and guidance concerning business continuity planning and resiliency and diversity requirements, such as the <i>Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System</i> , the <i>FFIEC Business Continuity Planning Booklet</i> , and the <i>FFIEC Operations Booklet</i> ? Do your business continuity plans meet these requirements?	
	30	Are your telecommunications vendor management personnel aware of regulatory requirements for critical business operations continuity and recovery goals?	
	31	Have you assessed how a power failure both at your institution's premises and your telecommunications service provider's would affect mission-critical services?	
	32	Does your institution provide standby power on your own premises? Do you test standby power regularly?	
	33	When battery backup capabilities are provided, do you know how long your critical services can run under a full load? Is it adequate for your needs?	
	34	When emergency generator capabilities are provided, how much of the full load can be handled, for how long? Is it adequate for your critical services needs?	
	35	Is adequate diesel fuel stored on the premises to support your emergency generator needs? Is off-site delivery of diesel fuel adequate to meet your needs?	
	36	Is there adequate contingency power for air conditioning and chilled water to support your critical technology services? Can the telecommunications service provider demonstrate that it maintains the batteries in outside plant equipment?	
	37	Does your telecommunications service provider have emergency power provisions and does it maintain and test standby power regularly?	
	38	Have you discussed power issues, impact on wireless networks, carriers' fiber networks electronics equipment terminations on your premises and the need for adequate backup power both for CPE and with the telecommunications service provider?	
	39	Do you provide periodic maintenance and testing of your systems at "full load" to ensure that the backup system is	

Indicate here if not applicable	Q no.	Question	Comments
		tested under realistic scenarios?	
	40	Have you included in your SLA a provision to ensure re-supply of fuel from suppliers?	
III. Recovery Tools and Processes			
	41	Have you discussed with your telecommunications service provider the scenarios used in the provider's contingency plans?	
	42	Are the provider's recovery time objectives consistent with your institution's requirements?	
	43	Does the telecommunications service provider have any partnerships or SLAs with other service providers to continue providing service to your institution?	
	44	Do you know the telecommunications service provider's priorities for restoring service? Where does your institution's requirements rank?	
	45	Do you have information about or are you assured rapid access to information on the routes or paths through which your information passes when recovering from a disruption in service?	
IV. Due Diligence			
	46	What personnel resources is the telecommunications service provider prepared to commit to the relationship? How many employees will have detailed technical knowledge?	
	47	Have you assessed the financial stability of the telecommunications service provider?	
	48	What assurances can the telecommunications service provider give you to demonstrate it can meet your business needs and business continuity requirements?	
	49	How does the telecommunications service provider determine its liability limits associated with availability guarantees?	
	50	With what process does the telecommunications service provider assess its services to your institution? How does it correlate those services with new requirements to make sure that duplication and single points of failure are avoided?	
	51	Does the telecommunications service provider have an integrated process to ensure the circuits remain diverse?	

Indicate here if not applicable	Q no.	Question	Comments
	52	Do you know who “owns” a major telecommunications facility (e.g., central office), especially those used by multiple carriers? Do you know what your telecommunications service provider’s business continuity plan is for responding to the destruction of a major facility?	
	53	What assurances can the telecommunications service provider give that reciprocal lease agreements are in place with other vendors and that these leased facilities do not introduce single points of failure?	
	54	How (and how quickly) will the telecommunications service provider inform clients of a service interruption?	
	55	Is the telecommunications service provider prepared to help you understand the complexities of its network and to work with you to provide suitable solutions for resiliency? If so, who will do this?	
	56	How does the telecommunications service provider assess the physical threats against its network assets? How does it mitigate the risk of these physical threats relative to your regulatory requirement for business continuity plans?	
	57	Can the telecommunications service provider demonstrate that there is no single point of failure in the infrastructure solution that has been engineered to meet your requirements? Can the provider explain the process it uses to assure your solution is maintained while changes are occurring in the provider’s or others’ systems?	
	58	How does the telecommunications service provider’s engineering process guarantee diversity is maintained in relation to all the key elements (risers, building entry points, last mile ducts and manholes, local exchange, network routes, international links, and other key points)? How are potential single points of failure identified?	
	59	How is spare capacity engineered (for example, percent utilization threshold or by number of last mile customer circuits)? Does capacity engineering take into consideration redirected call volumes when customers activate their business continuity plans to avoid choke points and loss of critical services?	
	60	Can the telecommunications service provider provide information on the routes/paths through which information passes?	
	61	<p>Questions for mobile/wireless telecommunications service providers:</p> <ul style="list-style-type: none"> a. Are there known “dead zones”? b. What recovery/fail over capabilities and capacity are built in to the network? c. How is resiliency built in to the infrastructure? 	

Indicate here if not applicable	Q no.	Question	Comments
		d. Does capacity engineering consider redirected call volumes when customers activate their business continuity plans to avoid choke points? e. How can signal capacity and strength be increased during or after an event? f. For side band audio: What radio frequencies are used? Are there distance limitations? g. Are there any potential conflicts with other service providers or emergency communication services? h. How are cell towers, switching stations and central offices set up for resiliency? i. What are the backup power arrangements at cell towers and other facilities?	
	62	Can your telecommunications service provider uniquely identify your mission-critical circuits throughout its system in an end-to-end fashion and maintain that identification through changes, such as re-engineering?	
	63	How can the financial institution verify the accuracy of the routing information provided?	
	64	Do carriers customarily divert a company's traffic from a stated route to an unknown route without the customer's knowledge?	
	65	Can the telecommunications service provider assure you that its diversity services will continually meet your requirements? What assurance can the telecommunications service provider give you that it has monitoring in place to meet your requirements? Can you validate and receive regular reports of the results of this monitoring?	
	66	Can the telecommunications service provider give you reliable recovery-time estimates for defined contingency situations, such as the loss of a central office? Can the telecommunications service provider produce results of tests, especially when multiple telecommunications service providers are involved in supplying contracted services?	
	67	What are the telecommunications service provider's power backup, restoration and contingency plans? Are they tested? If yes, what are the results? Have you received results relevant to your service?	
	68	Does the telecommunications service provider have appropriate contingency plans in place to meet your institution's needs? How often does the provider test these plans?	
	69	Can the telecommunications service provider provide availability figures? If so, how does the telecommunications service provider account for major disruptive events in its calculation?	
	70	How does the telecommunications service provider monitor the network and performance of each facility?	

Indicate here if not applicable	Q no.	Question	Comments
	71	What are the telecommunications service provider's change management practices as they relate to network monitoring, maintenance, equipment and software releases?	
	72	How are switching stations/central offices set up for resiliency? How often is this resiliency tested?	
	73	Does your telecommunications service provider have a tested business continuity plan? If so, does the plan meet your institution's business continuity requirements?	
	74	Does the telecommunications service provider test its business continuity plan? Are customers permitted to participate in tests?	
V. Contracts			
	75	Are your institution's definitions of diversity, recoverability, redundancy and resiliency consistent with the definitions used by your telecommunications service provider? Are they specified in your contract or service agreement?	
	76	When you order new services, do you discuss your existing services to ensure that no dangerous assumptions are made about diversity, recoverability, redundancy and resiliency? Do you review existing requirements to prevent duplication or introduction of situations that compromise other critical requirements?	
	77	Have you included provisions in the contract and SLA requiring the telecommunications service provider to provide information on routing to ensure that diversity is maintained? Will these provisions provide you with enough information to meet your diversity, recoverability, redundancy and resiliency requirements?	
	78	Have you included provisions in the SLA requiring the telecommunications service provider to give updates on network issues, proposed engineering downtime and other changes in normal operations?	
	79	Has your service provider shared engineering drawings with you that show your circuit construction and routing? Have references to these drawings been incorporated into your contract?	
	80	Have you narrowed the <i>force majeure</i> clause to require that all diverse paths be directly disrupted before the service provider is excused under the <i>force majeure</i> clause? Have you established service restoration schedules that your service provider must meet in the event that the <i>force majeure</i> clause goes into effect?	
	81	Have you prevented the incorporation by reference of tariffs or other external documents into your contract? If you	

Indicate here if not applicable	Q no.	Question	Comments
		have not, have you carefully examined all such documents to prevent inconsistent and/or unacceptable contract terms?	
	82	Are your definitions of diversity, recoverability, redundancy and resiliency consistent with the definitions used by your telecommunications service provider? Do contracts and SLAs reflect these agreed-upon definitions?	
	83	Do you have a specific department or staff person(s) assigned to manage the relationship with your telecommunications services provider?	
VI. Ongoing Relationship Management: Testing, Monitoring and Auditing			
	84	Have you established policies and procedures to facilitate telecommunications administration?	
	85	Does designated staff have the authority to oversee telecommunications service providers? For example, does designated staff have the authority to establish network objectives, principles and standards? Is a designated employee responsible for ordering and monitoring mission-critical circuits?	
	86	Do you know how your telecommunications provider will coordinate with other telecommunications providers in an emergency or national security event? Do you know who to contact at your telecommunications service provider in times of emergency? Who will serve as your institution's "advocate"?	
	87	Have you established diversity criteria with your telecommunications service provider? Have you developed audit programs to ensure compliance with the criteria?	
	88	Have you educated your telecommunications service provider on the business processes supported by critical circuits and interdependencies with other financial institutions?	
	89	Have you discussed ways to involve multiple telecommunications providers to assess risks, geographic concentrations and single points of failure in primary and backup sites?	
	90	Have you established an ongoing relationship with your counterpart at the service provider? (He or she can provide a different perspective on issues that affect both companies and better prepare you for business interruptions. These relationships can mean the difference between getting access to good information during a disaster and getting only the information that is available to the general public.)	
	91	Does your provider perform business continuity/disaster recovery testing? Can your organization participate? Have you participated in business continuity/disaster recovery tests conducted by your telecommunications service	

Indicate here if not applicable	Q no.	Question	Comments
		provider? (These tests can be an opportunity to illustrate for your management the importance of information sharing and the value of the business continuity planning process. They can also illustrate the depth of your company's dependence on external resources.)	
	92	Do you understand the service provider's operating strategy and position within the larger regional or national infrastructure? (When your building is down, this information can help you explain the situation to your senior management and provide realistic expectations for service restoration.)	
	93	Has the telecommunications service provider tested its backup facilities to ensure their availability?	
	94	Do you regularly review your company's resilience requirements with your telecommunications service provider?	
	95	Does your service provider notify you of network updates, proposed engineering downtime or other changes in normal operations?	
	96	Do you have primary and alternate methods of contacting your provider (e.g., telephone numbers, pagers, email addresses) for use during times of crisis?	
	97	Does your telecommunications service provider have alternative contact information for your response team members?	