

---

# Regulatory Compliance and Network Access Control (NAC)

February 20, 2007



Insight Into Management & Technology Topics

IQ knowledge

Prepared by:



© DSM Technology Consultants

## Table of Contents

EXECUTIVE SUMMARY.....	3
REGULATORY COMPLIANCE & NETWORK ACCESS CONTROL.....	4
NAC – WHAT IS IT?.....	5
A COMMON THEME FOR REGULATORY & NAC REQUIREMENTS .....	6
LAWS – REGULATIONS & TECHNOLOGIES TO CONSIDER .....	7
THE IMPULSE POINT SAFE-CONNECT™ SOLUTION .....	8
CONCLUSION.....	10
APPENDIX A.....	11
DSM: Compliance & Continuity Solutions .....	11

## Executive Summary

One of the most forceful trends shaping both private and public organizations is the need to ensure that their information systems are accurate and compliant with regulatory mandates. Ensuring compliance with laws and regulations is a pressing demand for IT departments, and now IT must also be compliant with internal governance and operational requirements, and incorporate best practices into their operations. All of these initiatives may be considered a waste if IT fails to implement a culture of security compliance that satisfies the requirements of regulatory mandates to capture, retain, and manage the corporation's information in an effective and trustworthy manner.

A compelling reason to focus your organization on compliance and make it a strategic initiative is to reduce the cost of meeting individual regulations.

A compliance strategy provides a competitive edge. If your organization can respond quickly to new regulations while others in your industry remain stuck in 'tiger-team' mode, the advantage goes to you and your organization. The ability to respond to compliance requirements, in any operating situation, will differentiate you from your competitors in the eyes of your customers, employees, shareholders, and partners.

Sarbanes-Oxley (SOX), the Health Insurance Portability and Accountability Act (HIPAA), Graham-Leach-Bliley (GLB)<sup>1</sup> and other industry-specific rule changes have ushered in a regulatory era that greatly values information technology security compliance and increases the penalties for companies and individuals whose risk-management practices are less than robust. Network Access Control represents an important component of a company's overarching security management strategy providing detailed historical audit reports for compliance auditors.

Companies that elevate network access control, or NAC, to a strategic level in their business and compliance activities do more than avoid risk. Applicable to most security activities is the old saying, "the chain is only as strong as the weakest link." In order to realize all the benefit of NAC, it needs to be fully deployed into your network -- managing all users that want access and seeing all traffic to provide both pre- and post-admission control.

In addition, technologies and procedures that address security and continuity issues have the added benefit of improving business processes and productivity, and help to mitigate costs associated with meeting compliance driven technology changes.

From the focal point of the network, DSM Technology Consultants has identified six compliance area requirements, five of which have applicability to Network Access Control:

1. **Policies** – security domain documentation that drives security policy enforcement
2. **Verification** – ensure the end-point requesting access has valid credentials
3. **Access Control** – ensure appropriate access control measures are in place to grant user access to systems, applications, data and networks
4. **Remediation** – the ability to respond to an incident, report the incidence occurrence, and quarantine and restrict the damage the incident is capable of causing
5. **Assessment and Audit** – ensure control objectives are supported by mature control activities.
6. **Training** – communication, awareness and enforcement of security policies

## Regulatory Compliance & Network Access Control

**61% of CIOs say they plan to increase IT spending to meet regulatory requirements.**

- CIO Insight, Feb 2006

The plethora of regulatory compliance rules that companies must be aware of and mitigate the risk of non-compliance is overwhelming. The regulatory landscape is full of compliance land mines for the unaware organization. From Sarbanes-Oxley, HIPAA, Basel II, and Graham-Leach-Bliley, to SEC Rules 6835 & 17-a, TREAD Act, FCC-LSOG, USA Patriot Act, CALEA, PCI Security Scans, and the California Security Breach Notice Law -- the list may as well go on ad infinitum. How do you make sense of the compliance issues, how do you monitor changes in the regulations, and how do you justify the budget to support these initiatives? Where is the integration point between regulatory compliance and network access control?

“Today corporations are struggling to deal with a complex regulatory environment whose mandates have no budget allocations, while still managing tight IT budgets,” is an interesting quote from Rich Mogull, research director for Gartner. On top of this problem, there is a maze of other IT-related challenges. Challenges that include, automating processes that are currently manual, multiple sources for information and data, the need to understand data and information lifecycles, and process and information auditability. Corporations struggle to keep their eyes on the regulatory strategic ball while they are juggling many tactical and operational balls.

Government regulations such as HIPAA, SOX, and GLBA require changes to ensure operational capability maturity in network security policies and procedures. Network administrators need to be concerned not just about complying, but also about documenting compliance in order to ensure they understand the requirements and are capable of responding to an internal or external audit. From the network perspective, compliance with these regulations consists of the following requirements:

- **Policies:** Documented security policies to prevent intrusion and protect private information.
- **Verification:** Ensure that no one is accessing data without authorization.
- **Access Control:** Ensure appropriate access control measures are in place to grant user access to systems, applications, data and networks.
- **Remediation:** Timely ability to respond to an incident, report the incidence occurrence, and quarantine and restrict the damage the incident is capable of causing.
- **Assessment and Audit:** Documentation regarding the use of systems, applications, and data in order to ensure control objectives are supported by mature control activities.

A comprehensive NAC strategy – one that addresses both pre- and post-admission issues and covers policy, endpoint

NAC REQUIREMENTS	
POLICY	Identity Management End-Point Compliance & Isolation Policies are Rooted in the NAC
VERIFICATION	Registration Authentication Role-based Rules Location-based Rules
ACCESS CONTROL	Role-based Rules Location-based Rules
REMEDIATION	Isolation Gateway Alarms and Notification Automated Remediation Self-Remediation
ASSESSMENT & AUDIT	Documentation Compliance Assessment Port Connection Location Login/Logoff Locality Physical/Logical Address Relationship

compliance, and identity – can help organizations effectively and efficiently address regulatory compliance needs by automating these processes and providing the appropriate audit and documentation information.

## NAC – What is it?

At a high level, as defined by Forrester Research, "NAC is a mix of hardware and software technology that dynamically controls client system access to networks based on their compliance with policy." NAC is a hot buzzword; therefore, the following component-level definition of what NAC is won't map directly to all NAC products and architectures. NAC or Network Access Control is comprised of three dependent components:

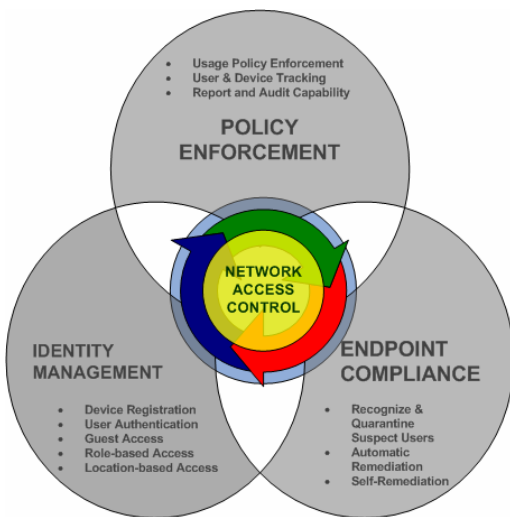
1. Policy Enforcement
2. Identity Management
3. Endpoint Compliance

*Policy Enforcement:* Policy compliance enforcement regulates endpoint security policies and ensures integrity by tracking activity and reporting, isolation, quarantine, and remediation.

*Identity Management:* Includes registration, authentication, role-based, and location management. A comprehensive approach to Identity Management ensures integration of the who, what, where, and when. That is to say, who is connecting to my network, what device are they using, what is their location, and what time of day are they accessing the network? This information is used to determine what endpoint security policies are applicable, what degree of access the user is permitted, and make real-time decisions on any actions that must be taken to ensure network integrity, i.e. permit access or isolate and quarantine.

*Endpoint Compliance:* Access to enterprise networks today happens either remotely, wirelessly, or by wired end-users. Security threats must be identified and remediated in real-time to ensure network security and safeguard business operations and assets. Endpoint compliance must assess both pre- and post-admission vulnerability, as well as provide validations and ensure policy compliance has been enforced.

It should be noted as of the completion of this paper, there are no defacto NAC standards, although the Trusted Computing Group ("TCG") is writing NAC standards to promote multivendor interoperability. The TCG Trusted Network Connect Sub Group ("TNC") has defined and released an open architecture and a growing set of standards for endpoint integrity. The TNC architecture enables network operators to enforce policies regarding endpoint integrity at or after network connection. The standards ensure multi-vendor interoperability across a wide variety of endpoints, network technologies, and policies.



Pure-play NAC vendors are best positioned to tie the three NAC components together most effectively!

## A Common Theme for Regulatory & NAC Requirements

Security is every company's dilemma. The single most important theme running through all regulations is to ensure the security and trustworthiness of the company's intellectual property. Whether you are publicly traded, work in the financial services sector, or are in the business of healthcare, almost all large enterprises must demonstrate their compliance with network security best practices.

So, with all this valuable stored intellectual property, it is assumed that the data will comply with the definition of being trustworthy. To be trustworthy data must meet five key qualities:

1. *Integrity* – the ability to demonstrate information has not been changed
2. *Accuracy* – information remains consistent over its entire lifespan
3. *Authenticity* – the source of the content and who had control over it can be demonstrated
4. *Accessibility* – the record can be accessed based on rules-based policies
5. *Confidentiality* – the ability to demonstrate the content is only accessible by those who need to view and manage it

All five qualities point to the need for corporations to ensure their security house is in order and capable of ensuring data integrity, accuracy, authenticity, and accessibility under any circumstance. NAC makes networks inherently resistant to access attempts by unauthorized users and devices along with systems that fail to meet a baseline security standard. Access control is the first step in a wider plan for networking security with the second step being a broad and co-coordinated threat management approach.

NAC adoption is especially intense in particular vertical markets, such as education and healthcare. These segments usually lag in the adoption of new technology, but that's not the case with endpoint security. Universities, for example, are early NAC adopters because they have less control over the devices accessing networks than corporate entities. Tech-savvy students equipped with laptops, desktops, PDAs, and game consoles featuring applications that operate beyond the control of university IT managers are a security concern. Healthcare sector interest stems from two factors, first is the need to secure medical and biomedical devices that run embedded operating systems and are difficult to patch. Second, hospitals offering wireless access in patient rooms find themselves bringing unmanaged devices into the organization, along with a significant unmanaged extended enterprise network—which are HIPAA compliance vulnerabilities.

*While Sarbanes-Oxley is financial legislation, at its heart it is about ensuring that internal controls or rules are in place to govern the creation and documentation of information in financial settlements. Since its systems are used to generate, change, house and transport that data, CIOs have to build the controls that ensure the information stands up to audit scrutiny.*

- CIO Magazine

## Laws – Regulations & Technologies to Consider

Laws & Regulations	Who Should Be Concerned	Key Provisions	NAC Capability Requirements
<b>Sarbanes-Oxley (SOX)</b> <b>Statement on Auditing Stds (SAS 70)</b>	Public companies filing in the USA	<ul style="list-style-type: none"> <li>■ Security policies must be documented and enforced</li> <li>■ Access to sensitive data must be closely managed</li> <li>■ Threats against network assets must be mitigated</li> </ul>	<ul style="list-style-type: none"> <li>■ User Authentication</li> <li>■ Role-based Access</li> <li>■ Role-based Authentication</li> <li>■ Endpoint Compliance</li> <li>■ Alarms and Alerts</li> <li>■ Audit Logs</li> <li>■ Location-based Rules</li> </ul>
<b>Health Insurance Portability &amp; Accountability Act (HIPAA)</b>	Healthcare providers, Healthcare insurers, All organizations handling healthcare information or Insurance	<ul style="list-style-type: none"> <li>■ Control access to electronic health information</li> <li>■ Remote user access policy enforcement</li> <li>■ Access to personal data must be closely managed</li> <li>■ Threats against network assets must be mitigated</li> </ul>	<ul style="list-style-type: none"> <li>■ User Authentication</li> <li>■ Role-based Access</li> <li>■ Role-based Authentication</li> <li>■ Endpoint Compliance</li> <li>■ Alarms and Alerts</li> <li>■ Location-based Rules</li> </ul>
<b>GLBA (Graham Leach Bliley), PCI (PCI Security Scans)</b>	Regulated financial services companies	<ul style="list-style-type: none"> <li>■ Security policies must be documented, monitored, and enforced</li> <li>■ Access to sensitive data must be closely managed</li> <li>■ Threats against network assets must be mitigated</li> </ul>	<ul style="list-style-type: none"> <li>■ User Authentication</li> <li>■ Role-based Access</li> <li>■ Role-based Authentication</li> <li>■ Endpoint Compliance</li> <li>■ Alarms and Alerts</li> <li>■ Audit Logs</li> </ul>
<b>CALEA (Communications Assistance for Law Enforcement Act)</b>	Providers of commercial voice services, Facilities-based Internet service providers	<ul style="list-style-type: none"> <li>■ Security policies must be documented, monitored, and enforced</li> <li>■ Access to sensitive data must be closely managed</li> <li>■ Threats against network assets must be mitigated</li> </ul>	<ul style="list-style-type: none"> <li>■ User Authentication</li> <li>■ Role-based Access</li> <li>■ Role-based Authentication</li> <li>■ Endpoint Compliance</li> <li>■ Alarms and Alerts</li> <li>■ Location-based Rules</li> </ul>
<b>FISMA (Federal Information Security Management Act)</b>	Government	<ul style="list-style-type: none"> <li>■ Security policies must be documented, monitored, and enforced</li> <li>■ Access to sensitive data must be closely managed</li> <li>■ Threats against network assets must be mitigated</li> </ul>	<ul style="list-style-type: none"> <li>■ User Authentication</li> <li>■ Role-based Access</li> <li>■ Role-based Authentication</li> <li>■ Audit Logs</li> </ul>

## The Role of Compliance in Your Technology and Security Programs

<b>Technologies Involved in Compliance</b>								
Source: IDC, 2006	SOX	HIPAA	GLB	SEC 17A-4	21 CFR Part 2	Basel II	USA Patriot Act	Calif. SB 1386
Security	✓	✓	✓	✓	✓	✓	✓	✓
Financial Compliance	✓					✓		
Business Intelligence & Data Warehousing	✓					✓		
Content / Document Management & Search	✓	✓	✓	✓	✓	✓	✓	✓
Data / Application Integration	✓				✓	✓		
Business Process Automation	✓	✓			✓	✓		
Records Management & Archiving	✓	✓		✓		✓	✓	
Storage	✓	✓		✓	✓	✓	✓	
ERP	✓					✓		

## Safe•Connect

### Simpler...

- Vendor-independent solution integrates into existing network architecture and doesn't require manipulation of switches or forklift upgrades
- No redundant appliances necessary to maintain 100% network availability
- Fewer moving parts and less hardware translates into lower maintenance costs and reduced manpower

### Smarter...

- Out-of-line architecture is 5 times more scalable
- Non-intrusive network switch independent isolation/Layer2 quarantine technology (I-LAN)
- Continuous "real-time" pre- and post-admission policy assessment and enforcement without network degradation
- Provides consistent function across wired, wireless, and VPN networks

### Faster...

- Easy to deploy and maintain, installs in hours versus days
- Only Managed Service NAC solution available (monitoring, support, and maintenance)
- Low Total Cost of Ownership (TCO) – 1/3 the cost of legacy NAC solutions

## The Impulse Point Safe•Connect™ Solution

The Impulse Safe•Connect™ system provides an open network access control solution that easily integrates into vendor-diverse network environments. Very few organizations can commit to a single vendor network strategy. Acquisitions, mergers, and budget allocations all contribute to a network's total infrastructure and growing companies often marry networks that appear to work in opposition of each other. The Safe•Connect NAC solution's out-of-line network design integrates into your system today and will continue to work with your infrastructure as it grows and matures.

The inherent scalability advantages of Safe•Connect's distributed software architecture and managed support approach enables organizations to address their NAC enterprise requirements in a cost-effective manner. 10,000 users across multiple locations can be supported by a single appliance using the Safe•Connect solution without expensive forklift upgrades or switch manipulation. Other NAC vendors usually support fewer than 2,000 users and often require a duplicate appliance for redundancy purposes.

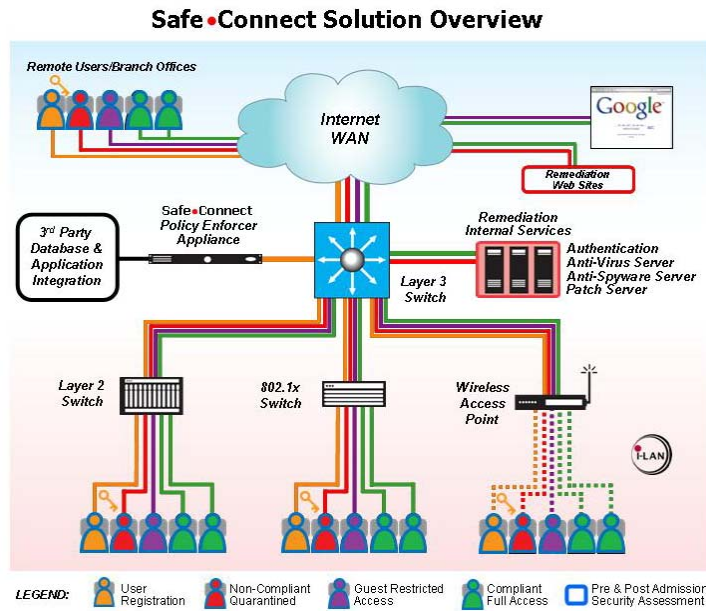
By focusing on endpoint policy management, Safe•Connect provides the following capabilities:

- Prevents unauthorized user access to wired, wireless, and VPN networks. Role-based policy management integrates with enterprise AD, LDAP, IAS, or RADIUS directory services.
- Automates the registration of end user computing devices and audits agreement to acceptable use policies.
- Ensures users maintain compliance with anti-virus, anti-spyware, Microsoft security patches, P2P file sharing software, and custom endpoint security policies.
- Automates the isolation of non-compliant devices at Layer2 using I-LAN quarantine technology and provides individualized remediation guidance.
- Flexible role-based policy management for employees, consultants, and guests.
- Enables organization to build custom policies and messaging to address their unique endpoint security standards and enforcement rules.
- Manages adherence to rogue access point devices that utilize NAT.

### HOW DOES IT WORK?

1. The Safe•Connect Policy Enforcer Appliance is installed on the organization's premises and is connected to an existing router.
2. The organization configures their desired policies and enforcement rules using the Safe•Connect Policy Management Console by network segment or directory services group.
3. Endpoint devices connecting to the company network will be intercepted, authenticated, presented with the organization's acceptable use policies, and issued a Safe•Connect Policy Key.
4. The Safe•Connect Policy Key certifies that the endpoint device adheres to endpoint security policies on a continuous/real-time basis. It reports non-compliance to the Safe•Connect Policy Enforcer and delivers individualized remediation guidance. The endpoint device remains completely isolated using I-LAN quarantine technology until the policy breach is resolved.

Safe•Connect offers consistent endpoint device support for wired, wireless, and VPN Networks.



The Safe•Connect Policy Manager includes real-time and historical compliance reporting that provides audit specific policy status information that addresses regulatory requirements. Continual pre- and post-admission security validation and reporting also means that you are aware of a policy breach when it occurs, not the next time a user attempts to gain network access.

The screenshot shows the 'Safe•Connect Real Time Reporting' web interface. It features a search bar, a 'Log Out' button, and a 'Policy Status Summary' section. The main content is a table with columns for IP, MAC, User Name, Device, and Status. The table lists various users and their compliance status, with some users marked as 'Music Dorm 1' or 'Art room'.

IP	MAC	User Name	Device	Status
10.0.10	32-13-U2-Q4-06-24	iroberts	PC	Music Dorm 1
10.0.11	33-13-V2-Q4-08-24	twoods	PC	Music Dorm 1
10.0.12	18-12-V2-25-58-24	borialy	PC	Music Dorm 1
10.0.13	SR-MM-V3-Q9-53-14	qantark	PC	Music Dorm 1
10.0.14	SR-MM-35-77-53-65	dholly	PC	Music Dorm 1
10.0.15		unknown	PC	Music Dorm 1
10.0.20	11-A4-D2-44-76-R4	sdishma	PC	Art room
10.0.21	31-A7-S2-42-26-R4	moreland	PC	Art room
10.0.22	31-57-X2-D2-86-U4	ebasil	PC	Art room
10.0.23	41-52-R5-K2-87-S2	atrevor	PC	Art room
10.0.24	C5-52-R5-66-Q2-ZA	avaster	PC	Art room
10.0.25	C5-52-R8-66-Q6-ZA	bbalor	PC	Art room
10.0.26	88-52-D7-66-Q6-ZA	tomteehall	PC	Art room
10.0.27	89-52-H7-S7-Q6-ZQ	jenkins	PC	Art room
10.0.28	89-59-H7-24-Q6-KL	maxxygar	PC	Art room
10.0.29	25-8V-H2-C4-Q4-PO	nhairy	PC	Art room

More information on the Safe•Connect Network Access Control solution can be seen at [www.impulse.com](http://www.impulse.com).

## Conclusion

The challenges facing corporate IT infrastructure today are many. Key among these are combating ever more frequent security incidents and striving to maintain regulatory compliance. Given the deluge of vulnerabilities and attacks, and the need to ensure devices accessing networks are legitimate, no one can say the job of the network security administrator is easy. A common thread among these challenges is the need to ensure protection and control of the endpoint. Controlling who can access what, when it can be accessed, and from where, goes a long way toward meeting regulatory challenges.

Each regulation includes detailed compliance standards that must be met. However, the “common sense” network security policies delivered by a comprehensive NAC strategy address most of these requirements. Organizations that must comply with regulations that protect sensitive data would do well to implement a NAC solution that automates key network security processes such as:

- Authentication and access policies that ensure authorized access to files containing regulated data
- Location-based rules that authenticate and protect against unauthorized access to data no matter where the user is located
- Role-based admission policies that ensure data integrity
- Rapid network-based reaction to detecting and responding to security breaches that might compromise regulated data
- Safeguard from viruses, Trojans, Spyware, worms, and other malicious code
- Real-time audit of network activity that tracks who is accessing data and applications, and when and how it is accessed

Organizations require network access control solutions that ensure systems are in compliance with IT security policies before those devices are allowed to access the network. Security and compliance governance policies are useful only if they are enforced *all* the time. Determining security compliance after granting any network access is too late. The ability to respond to compliance requirements in any operational situation will differentiate your organization from your competitors in the eyes of your customers, employees, shareholders, and partners.

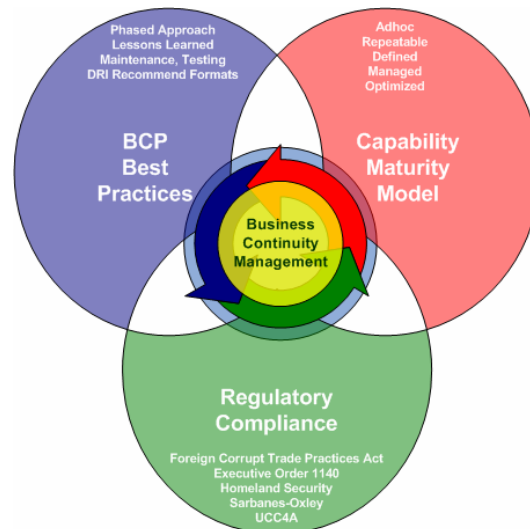
## Appendix A

### DSM: Compliance & Continuity Solutions

Are you still struggling with how to address regulatory compliance mandates? DSM's Compliance & Business Continuity solutions may be your answer. With compliance deadlines and sporadic regulatory audits becoming the norm, establishing the proper safeguards to protect your proprietary information is more challenging than ever. Adding to the challenge is the lack of a common language among regulators, standards organizations, consumers, and developers. Plus, there is a lack of a common structure for expressing requirements and assurance, and there is the need for credible organizations to evaluate requirements and validate compliance. You may need assistance translating the interpretation of regulations to identifying the proper technology and control measures to support your compliance program. We have the experienced personnel to support you in developing, deploying, and monitoring all your compliance initiatives.

DSM removes the challenges of compliance and business continuity with our Business Continuity Management Framework. Using DSM's seven-phase approach to compliance and four-phase approach to business continuity we ensure effective practices are used to springboard your compliance and continuity initiatives to a successful conclusion.

DSM's experience and certified consultants, tools, and intellectual property allows us to quickly assess, develop, implement, and test compliance and continuity initiatives for your organization.



**DSM's Seven Phase Best Practices Framework for Achieving Regulatory Compliance:**

1. Assessment
2. Goal Definition
3. Gap Analysis
4. Architecture Design
5. Implementation Plan Development
6. Plan Implementation
7. Ongoing Administration & Validation

**DSM Compliance Service Offerings:**

- ▶ Regulatory Exposure Assessment
- ▶ Compliance Organization & Governance
- ▶ Compliance Policy Gap Analysis
- ▶ Regulatory Risk Assessment
- ▶ Third Party Risk Management
- ▶ Compliance Implementation Strategic Planning

**DSM's Four Phase Best Practices Framework for Achieving Operational Resilience with Business Continuity:**

1. Discovery & Analysis
2. Plan Development
3. Plan Implementation
4. Ongoing Administration & Validation

**DSM Business Continuity Service Offerings:**

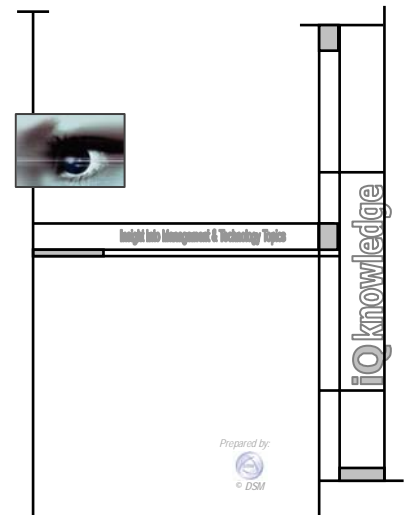
- ▶ Risk Assessment & Business Impact Analysis
- ▶ Recovery & Restoration Strategies
- ▶ Plan Development & Implementation
- ▶ Testing & Administration
- ▶ Plan Audit Services & Capability Assessment

**DSM Corporation Differentiators:**

- ▶ Highly-trained, certified, and experienced solutions consultants
- ▶ Customized Solutions with a methodical framework approach
- ▶ Extensive Industry Experience
- ▶ Access to experts in multiple IT disciplines
- ▶ Vendor Independence

DSM collects and distills industry best practices in business continuity, security and other Information Technology areas. DSM can deliver timely and effective enterprise security tailored to meet your organization's specific needs.

DSM Technology Consultants is pleased to present iQknowledge®, a series of whitepapers to assist organization's in making good management and technology decisions to support their business needs.



DSM Technology Consultants  
7800 Preston Road, Suite 136  
Plano, TX 75024  
Tel: 214-701-8814  
www.dsm.net

This document may be reproduced and distributed in whole only when it includes the cover page and this notice. Any reproduction, use, appropriation, or disclosure of this information, in part, without the specific prior written authorization of InQuest Corporation is strictly prohibited.

Copyright ©2007 DSM Technology Consultants. All rights reserved. Unpublished rights reserved under U.S. copyright laws. DSM iQKnowledge, and DSM logo are trademarks of DSM Technology Consultants. All other trademarks are property of their respective owners.