Managing Risk for Regulatory Compliance

Challenges, Implications and Solutions for IT
Table of Contents

Introduction ............................................................................................................................................... 3
Risk Management and Regulatory Compliance.........................................................................................3
The Implications for IT .............................................................................................................................. 4
A Strategic Starting Point .......................................................................................................................... 5
Real Metrics of Business Impact .............................................................................................................. 5
A Foundation That Is Secure by Design .................................................................................................... 6
An Infrastructure That Controls the Application Delivery Network – Instead of the Variables ............ 7
A Solution That Keeps Pace with the Business .......................................................................................... 10
  • Citrix for Regulatory Compliance: Secure Data, Productive People, Cost-Efficiency ....................... 10
Introduction

At the heart of an organization’s ability to comply with the increasingly pervasive regulatory requirements of today’s business landscape is the issue of risk management with its new and broad set of challenges for the organization. At Citrix, we believe that a strategic approach to meeting regulatory requirements will yield the best results, with business benefits immediately and with flexibility for change over time.

This white paper examines trends driving requirements for regulatory compliance today, the consequent challenges for the IT team and the executives who are accountable, and the business benefits delivered by a strategic solution.

Risk Management and Regulatory Compliance

Shaped by fundamental and far-reaching changes in the massive regulatory requirements now sweeping across countries and industries, regulatory compliance today brings with it a new focus on risk management and a new and broad set of challenges for the IT team and many key executives. These challenges have direct implications for IT and the individuals who now will be held accountable, shaping the need for a new approach to regulatory compliance.

What must be done to protect corporate information?

Increased regulation worldwide, both by governments and within industries, has resulted in greater accountability for corporate officers when it comes to managing risk in their organization. The stringent audit requirements of the many and diverse regulations have increased the need for control, visibility, and accountability, directly linking information security to risk management and, in fact, driving its implementation.

In this environment, the CIO, CSO, Chief Information Security Officer, Chief Privacy Officer, and other key executives must demonstrate that they are protecting corporate information effectively – to regulatory authorities, to business partners, to their own boards of directors. This requires that measures be in place to protect internal resources, and, in turn, has created pressure to adopt a comprehensive approach to risk management.

As a result, IT has become an enabler for enterprise risk management by leveraging technology to proactively monitor and manage regulatory compliance and other business risks.1 This, of course, is not a simple matter. Industry experts believe that implementation of security today depends on establishing strong security policies and procedures, not merely turning-on auditing features or deploying encryption in a solution. End-to-end security implementation should be the goal for enterprises, according to these experts, combining database security with application-, network-, and infrastructure-level security.

1 “Securing the Network from the Inside Out”, Forrester Research, Inc., 2005
The Implications for IT

In this environment, the ability to comply with regulatory requirements becomes particularly important, as well as challenging. In fact, for most organizations, it is critical to sustaining competitive advantage and operating efficiently, requiring an understanding of the direct implications of today’s challenges.

Many laws and regulations that have been adopted in the past decade impose information security requirements on companies and agencies. Some, such as the Health Insurance Portability and Accountability Act (HIPAA), California SB 1386, and the European Union Privacy Directive, relate to consumer privacy. Others, such as the Sarbanes-Oxley Act, focus on the sanctity of data and systems for trusted record keeping and reporting. Still others have yet to go into effect, such as the requirements and standards under Basel II which are to be implemented by 2007 and the Japan version of Sarbanes-Oxley which will not be in full operation until 2008.

However, none of these regulations, according to Gartner, defines due care in security and no certification exists to ensure that a product or service will enable an organization to achieve compliance. Further, according to Forrester, although compliance requirements for many enterprises require them to take stronger measures than ever before to protect private data stored in databases, the regulations behind them typically do not offer strategies or best practices guidelines to meet the challenge.

As a result, many organizations are still struggling to understand the numerous regulations that potentially affect them and what that means from a business perspective. Because today’s organizations are increasingly information-intensive, technology is becoming a key part of strategic compliance initiatives, to ensure sustainability of compliance-related processes, mitigate risk, and manage ongoing costs.

In general, regulatory mandates seek to focus the enterprise on accountability and control, primarily through process discipline and corporate governance, and often are implemented in IT. Compliance requirements typically include:

- use of authentication to assure the identity and authorization of users
- limitations on access to information
- privacy of personal information
- segregation of responsibilities between users and groups to limit abuses
- auditing, which is usually required to demonstrate compliance and brings with it the associated requirement for an appropriate level of reporting.

The difficulties – and cost – of implementing compliance are exacerbated by the fact that many organizations have a highly distributed information infrastructure, with systems, devices, and data found throughout the enterprise.

These are not trivial considerations. Despite the fact that compliance timelines might be uncertain, some aspects of initiatives are already quite clear, such as the substantial penalties for non-compliance which often include personal liability for business executives. As well, incidents associated with loss of information security can lead to loss of customer confidence, brand damage, lost revenue, stock price impact, and class action lawsuits.

---

2 “Eight Steps Needed to Define Reasonable Security”, Gartner, Inc., 2005
5 “Eight Steps Needed to Define Reasonable Security”, Gartner, Inc., 2005
A Strategic Starting Point

Together, the new and broad challenges of today’s business landscape and the consequent implications for IT teams and the executives who are accountable for regulatory compliance suggest that a strategic approach will yield the best results, both immediately and in the flexibility to meet new challenges over time. This requires:

- **a foundation** that is secure by design, not by chance, to help eliminate the traditional compromise between security on the one hand and productivity and profitability on the other.

- **an application delivery infrastructure**, that eliminates the related costs, inefficiencies, and inability to support business goals that are inherent in a fragmented approach to IT operations.

- **a solution** that keeps pace with the business, to help IT execute rapidly and efficiently, reducing the need for custom integration of individual products, accommodating legacy and future technologies, and providing an architectural approach that designs for change to meet the business’s needs on demand.

Real Metrics of Business Impact

As the global leader and most trusted name in application delivery infrastructure, Citrix since 1989 has been helping organizations to deliver any application to users anywhere with the best performance, highest security, and lowest cost.

In fact, Citrix was the first company to understand how organizations use applications to run their business, and to develop an application delivery infrastructure with solutions based on the customer’s perspective. Instead of limiting IT solely to modernizing systems and optimizing business processes for better operating efficiencies, Citrix solutions make IT relevant to the business, giving IT the flexibility to change on demand and over time across technical, physical, and organizational dimensions. Without changing the overall environment, IT gains an agile infrastructure that connects application delivery to the business value of the application, enabling IT to keep pace with the business, to handle multiple challenges concurrently, and to drive productivity and profitability initiatives across the company and across business units.

With annual revenue of $1.1 billion in 2006, Citrix today is relied upon by IT teams and their strategic executives at more than 200,000 organizations throughout the world, including 100% of the Fortune 100 companies and 98% of the Fortune Global 500. These organizations are using Citrix solutions to capture new business opportunities and competitive advantages. For example:

- Prudential Fox & Roach REALTORS, the sixth-largest provider of real estate services in the U.S., uses Citrix to protect corporate data accessed by 3,700 geographically dispersed and mobile independent agents, while also cutting IT support costs by 20%.

- A leading business process outsourcing (BPO) company in India, part of LASON, Inc., USA, is using Citrix to ensure 100% security of customer data, while also increasing by 300% the productivity of online BPO jobs.

- Saint Anthony’s Health Center, a health care facility in the U.S. that offers state-of-the-art medicine administered with skill and care, is using Citrix to comply with requirements of the Health Insurance Portability and Accountability Act, while also saving $700,000 on hardware replacement costs over

Although THLP does not currently have regulatory compliance issues, the firm expects that it will have to deal with regulations at some future date. “Right now, we feel secure with our Citrix implementation, which enables us to provide role-based access to information without opening up the network to vulnerability. When compliance issues arise, we are in a solid position to address them with this Citrix solution.”

Hoby Cook, Vice President of IT, Thomas H. Lee Partners, L.P.
• Mutual Service Corporation, a leading financial planning broker/dealer and investment firm and wholly owned subsidiary of Pacific Life, is using Citrix to meet the requirements of all government regulations for its industry, while also seizing an opportunity to dramatically change the way they do business.

• Thomas H. Lee Partners, L.P., one of the oldest and most successful private equity firms in the U.S., brought Citrix into the organization for the highest level of information security over the network – considered pivotal to its competitive position – and got bulletproof security and IP telephony access as well.

A Foundation That Is Secure by Design

As a company and through its many products and services, Citrix’s foundational approach to security provides the right degree of protection for delivering applications and extending access to users anywhere, anytime – without compromising security. We call it secure by design, because it enables organizations of any size to treat security as an integral part of their architecture, not as an afterthought.

• **Application delivery.** Citrix is the only company that offers a service-oriented architectural approach for delivering all classes of applications with the fastest performance, highest security, and lowest cost: application virtualization and application streaming for Windows applications and application optimization for Web applications. Enabling secure use of public networks, this combination offers unique opportunities for control of the endpoint environment, application execution, and information containment.

• **Application security and control.** To deliver application security and control across IT and business initiatives, Citrix combines the power of two key security capabilities – SSL VPN and Single Sign On.

• **Policy-based controls.** Administrators can set end-to-end policies that dictate what can be accessed from each specific access scenario. Policies can take into account users, groups, device types, network locations, and end-point security.

• **Advanced authentication.** In cooperation with partners, Citrix offers authentication with strong measures such as two-factor authentication, using tokens, smart cards and biometrics. Citrix is committed to ensuring that customers have the widest range of authentication options available, from leading authentication providers.

• **Industry partnerships.** Citrix works closely with industry security leaders, to create certified tight integration with our products and services. Customers can be confident that Citrix has established the partnerships needed to tightly integrate secure-by-design capability with the security eco-system, in areas such as authentication, identity management, and encryption.

• **Industry certification.** Citrix is continually evaluating industry and government certification programs, and ensuring that products are submitted and certified where appropriate. These programs include FIPS 140-2, Common Criteria, and Section 508 accessibility.

• **Industry standards.** Citrix is committed to both using and developing open, robust, secure standards for infrastructure security. We make use of established industry standards, such as Secure Sockets Layer (SSL) encryption, and are involved in the development of emerging standards, such as
the Security Assertion Markup Language (SAML).

- **End-point security.** In partnership with industry leaders, Citrix leverages new and innovative end-point compliance-enforcement solutions, centralizing the assurance that end-points are secure and compliant before access is delivered.

- **Comprehensive reporting and auditing.** A compliance audit could require reporting that encompasses the entire information lifecycle, including interaction with end-points as well as with the datacenter. Citrix’s solutions encompass both environments, able to provide comprehensive, auditable reporting that includes the user environment as well as the datacenter.

### An Infrastructure That Controls the Application Delivery Network – Instead of the Variables

Behind Citrix’s position as the global leader in application delivery infrastructure is the company’s strategic and systematic approach to developing solutions for application delivery: enabling applications to be delivered, supported, and shared on-demand with the best performance, security, and total cost of ownership.
The Application and the Business

Businesses today are running more than ever on applications, arguably positioning the application as the main intersection point between IT and the business. Given that customer, financial, operational, and market information are the lifeblood of any enterprise, effective delivery of applications is becoming one of the most important competencies that winning businesses will need. This creates the opportunity for IT to connect application delivery to the business value of the application, making IT relevant to the business.

However, at the same time, users are being pulled further and further from applications by technical, physical and organizational distance, introducing countless variables that endlessly and rapidly change. For example:

- **technical distance** – consider the proliferation of computing endpoints; Web-based changes in application design; software as a service and managed services being adopted more readily; and a systematic decoupling of computing components with Web services known as service-oriented architecture. IT must support all of these application and user scenarios, both new and old.

- **physical distance** – IT is consolidating the complexity of distributed computing into datacenters; datacenters are being aggregated to less vulnerable places; users are more mobile, getting work done from home, office hotels, and wireless hotspots; users and governments are demanding flex working and more virtual work styles; and work is being shifted offshore to places where it’s more efficient and effective. At the same time, companies must extend applications to external users, suppliers, and partners who can be anywhere in the world.

- **organizational distance** – boundaries between organizations are falling as business processes are decoupled and outsourced; virtual organizations are becoming more prevalent, allowing business to focus on core competency; and organizational re-structuring, driven by mergers and acquisitions, is accelerating.

This introduces many challenges for IT because the degree of difficulty of application delivery is directly proportional to distance. Absent the right approach to application delivery, application distance will force businesses to live with unacceptable application performance, to compromise information security in the interest of productivity and profitability, and to endure higher operating costs when delivering applications over the network.

Flexibility for Fast Response to Business Change

Recognizing the inefficiency of focusing on controlling variables that will change endlessly, Citrix focuses on controlling the application delivery network instead. Leveraging the new architectural approach of service-oriented computing for application delivery, Citrix provides the loose coupling between the application point-of-origin and the user point-of-access to support an infinite number of scenarios between these two points. This approach gives business the ability to change on demand in order to seize opportunities and gain competitiveness, and is at the heart of making IT relevant to the business.
Optimal Application Delivery and Complete Line-of-sight Control for Any Application

Citrix is the only technology company with a complete solution to deliver, secure, optimize, and monitor application services from point-of-origin of the application to point-of-access by the end user. Citrix application delivery infrastructure provides optimal delivery and complete line-of-sight control for each class of application, solving the application delivery challenges at the six key strategic points-of-presence:

- **Directly in front of Web applications**, where most new application development is happening today
- **Directly in front of Windows applications**, where most existing line-of-business applications are deployed today
- **Directly in front of desktops and desktop applications**, deployed in the datacenter for delivery over the network
- **At the gateway**, where users gain secure access to all of their applications
- **At the front door of the branch office**, where more than half of all enterprise employees access their applications
- **Directly on the end point**, with full visibility into the end-user experience
A Solution That Keeps Pace with the Business

Citrix combines benefits that deliver a very high degree of control which can be leveraged throughout an organization, from the data center to the endpoint, wherever the endpoint might be and wherever it might be found. This level of control corresponds to significant compliance requirements for internal IT controls and business processes. As a result, organizations can balance information security with business productivity and cost-efficiency, optimizing controls with extremely high granularity but also great flexibility. This includes an exceptional capability to limit critically sensitive information solely to the right people, in the right context, at the right time, facilitating compliance with the mandates of regulations throughout the world and its industries.

Citrix for Regulatory Compliance: Secure Data, Productive People, Cost-Efficiency

Application control, reporting, logging, and monitoring to reduce compliance costs

Citrix assists organizations to meet internal standards and comply with government and industry regulations by making it easy and cost-effective to centralize and consolidate applications, delivering the power to observe, monitor, and measure resources with robust business reporting, delegated administration, a common management infrastructure, and integration with third-party network- and systems-management tools. For example, much of regulatory compliance involves reporting,
logging, monitoring, and alerting. Citrix Presentation Server™ provides this functionality with a unified management console and reporting center. Visibility into the health and status of a Citrix Presentation Server farm is provided to third-party network-management tools so that administrators can monitor the wider computing environment from their preferred tool.

Information containment

One of the distinctive innovations in the Citrix Access Gateway™ and its Advanced Access Control option is the power to intelligently automate security and compliance measures based on the access context, providing a high degree of control over sensitive information. Citrix SmartAccess™ technology senses the context of the endpoint and delivers policy-compliant access accordingly. SmartAccess determines who is requesting access, where they are, when access is requested, and how it is requested. If compliant, then and only then will SmartAccess enable access to resources according to policy.

Granular security zones

Compliance might require the segregation of resources among specific users and groups. At the level of application delivery, Presentation Server and the Access Gateway both enable applications to be isolated in their execution environment between specific users, roles, and user groups. This centralizes isolation of controls on application management and ownership, even when the same application is available to different user or ownership groups on the same server environment. Finely grained Citrix access management also includes features that support content redirection, to ensure that proper and secured centralized applications are used rather than those local to the endpoint. This restricts access to specific resources as administratively defined.

More comprehensive audits

The best security tools are useless without a clear view of how the information system is used: who uses it, how, under what conditions. But this view is often just a dream for IT and security teams because a multitude of security solutions, all keeping their own logs, prevent their having a session-oriented view of the information system – unless they go searching for the information left by each user in the firewall log, in the authentication system log, and in the logs of each application used. That is, of course, if all of these applications support such a functionality. And yet, this kind of information is not only very useful when investigating a security incident, it can also be essential for ensuring regulatory compliance when an organization is required to keep detailed logs on the use of its information system.

• Automated reporting – As part of Citrix Presentation Server, the Resource Manager provides the administrator with the tools for monitoring and analyzing the use of the information system. From a single console, an administrator can find out who connected from where and what applications were used for how long. This logging applies to all clients, no matter where they come from and regardless of their authentication method, without the need for the organization to deploy a third-party logging tool. The administrator can also find out how much server memory and CPU resources are used individually.

“...
Centralized authentication for Windows applications

Inadequate password management is known to be the cause behind the majority of security incidents. Three high-risk practices are particularly common: passwords themselves are too weak, such as too short or chosen from a dictionary; passwords are stored in a non-secure place, such as written on piece of paper by the keyboard, which is a classic; and, finally, passwords are not changed frequently enough. These bad practices combined with an ever increasing number of passwords for each user to remember – often 10 or more per user – lead to a single conclusion: organizations can no longer afford to ignore password management. Unfortunately, implementing an adequate solution is not as simple as it might seem, mainly due to the lack of authentication standardization. Indeed, too many applications still use their own authentication database without offering the possibility of integrating it into a directory, or even a public key management infrastructure.

- **Application security** – The Single Sign On functionality of Presentation Server, powered by Citrix Password Manager™, enhances application security for Windows applications, while reducing support costs. With automated application logons, password policy control, and self-service password reset, IT can enhance the security of all password-protected Windows applications delivered by Presentation Server.

- **Technology working for IT** – By entering passwords on behalf of the user, password management is simplified and security is reinforced at critical points. Passwords are entered only once – at first launch – and then submitted automatically on the users’ behalf each time an application requires them. Those encrypted log-ins are stored both locally and remotely, in the company directory where they are just simple objects attached to the profile of each user, or on a network share. Because users no longer have to deal with passwords, these can be as long and complex as is necessary for security. The administrator can define their length, the minimum amount of figures, letters or special characters, and so forth. And, of course, they can be changed as often as desired, completely transparently from a user perspective.

- **Simplified Integration** – This capability easily integrates with the Windows and Novell OS because it does not require the GINA authentication library to be replaced. Instead, it makes the most of the Microsoft chaining capabilities, which allow its own library to be used after the main authentication has taken place.

Integrating strong authentication to the legacy

IT and Security teams are only too familiar with the problem of strong authentication: the organization obviously can’t do without it, but even when the solution is deployed, everything remains to be done. For example, it must be ensured that every new module added to the information system can integrate into it, which is not always as easy as it seems. As another example, an application imposed today by the operational teams might not recognize the two-factor authentication solution chosen by security architects the year before. In such a situation, a software relay needs to be installed in order to translate authentication requests – until the next such incident occurs.

- **It all starts from the legacy** – With Citrix, there is no ripping and replacing of the existing infrastructure. The authentication procedures implemented use the standard Microsoft and Novell GINA libraries, as well as UNIX authentication procedures. Furthermore, the Citrix architecture does not have its own user base. Instead it uses the existing one, such as the company directory, for instance. Therefore, log-in procedures do not need to be modified.
• **Smart cards and secure tokens** – What is more, existing authentication procedures by smart cards or tokens, such as RSA SecureID, Secure Computing SafeWord or Vasco, can easily integrate with the Citrix architecture. As a result, these methods can be used to authorize Citrix sessions for remote access to business applications, data, and so forth.

• **Smart card authentication on Windows 9x** – Although the Windows 9x operating systems do not natively support smart card authentication, Windows 9x-based clients can recognize smart cards when opening a session on a Citrix server. The process is completely transparent and is made possible only by Presentation Server’s native smart card support; however, the card cannot be used to control local log-ins. This allows strong authentication to be provided on existing software, thereby extending its lifecycle. As well, through Password Manager, the Citrix solution can integrate with most two-factor authentication solutions that are currently available, including token, biometric, and proximity security systems.

Keep sensitive data confidential when delivering Web applications to millions of customers online

Web applications provide direct access to some of the most sensitive and valuable data in any enterprise – including financial records, credit card numbers, and customer identity information. But delivering these applications securely is particularly challenging because Web vulnerabilities are generally easy to exploit, and attacks cannot be detected by traditional security products. Web applications require defenses against a wide range of application-layer threats, such as denial of service (DoS) and worm attacks. Citrix® NetScaler® application delivery systems, which include built-in SSL encryption, have been architected to forward valid client requests to servers and to block illegitimate requests. Plus, since Citrix NetScaler’s single, unified device takes the place of a number of point solutions, overall network infrastructures are dramatically simplified, and overall operational costs are dramatically reduced.

Strengthen security for Web application delivery with award-winning firewalls

The Citrix Application Firewall option delivers the industry’s highest performing Web application security, capable of protecting Web servers without degrading throughput or application response times. The Application Firewall delivers best-fit performance for any enterprise or data center installation, with security technology that implements a positive security model based on HTTP industry standards and best coding practices for HTML. Web application behavior that deviates from the positive security model is treated as potentially malicious and is blocked. Because it understands good application behavior, the positive security model does not require attack signatures or pattern matching techniques to detect and block attacks. It is the only proven approach delivering zero day protection against unpublished exploits.

Reduce data security risks when delivering Windows desktops

Through desktop virtualization, Citrix Desktop Server™ centralizes end-user desktops and data in the datacenter, thereby retaining control of the IP and reducing the security risk of data loss at the endpoint. Desktop Server revolutionizes the way Windows desktops are delivered and managed by enabling the dynamic delivery of virtual desktops – desktops that combine full PC functionality with the cost-savings, manageability, and security of thin clients. Desktop Server provides a virtual desktop

“The Citrix solution supports our key Health Insurance Portability and Accountability Act goal – giving people access to only the information they need. Recently a HIPAA security risk assessment was conducted and the consulting firm found no security holes or problems with our Citrix system. That was great news.”

— Tim Kruse, Supervisor of IT Development, Saint Anthony’s Health Center
delivery system that delivers the best Windows desktop experience for any office worker and reduces 
the costs and provisioning challenges of desktop refreshes and new desktops for office workers. For 
example: desktop refreshes for migration to a new operation system can be accomplished more 
cost-effectively by extending the life of the endpoint and IT can deliver virtual desktops that provide the 
right desktop to the right users at the right cost profile. Centralized delivery of software updates and 
patches reduces the cost and effort involved in managing desktops, regardless of end-user location.

Deliver desktop applications without worrying about application and system 
conflicts and without lowering security standards

IT can deliver Windows applications to desktops without lowering security standards, both delivering 
and updating applications without giving users administrative rights. When it comes to desktop 
application installation, IT typically has faced the challenge of dealing with application conflicts and 
operating system instability. Presentation Server provides the application delivery option of application 
streaming to enable IT to centrally manage and deliver Windows applications to any user, even 
when the user is not connected to a network. Applications are streamed to a protected isolation 
environment, rather than installed on the user’s device, thereby eliminating application conflicts and the 
need for extensive regression testing.

Accelerate all applications over any WAN, anywhere – from any datacenter, 
anywhere.

When information and applications must travel long distances over wide area networks, the process 
can significantly degrade performance, impact the user experience, and force expensive bandwidth 
upgrades. In today’s business environment, IT is under pressure to increase security by moving 
application and server infrastructure out of the branch office and other physically distant locations 
and into centralized datacenters, which has the effect of reducing application performance. Citrix 
WANScaler™ optimizes the broadband connection between the branch office and the enterprise 
datacenter, reducing user wait times, improving productivity, and accelerating response time for all 
applications – all over the world and without modification of any network components or the need to 
tunnel traffic.

Know what’s happening at the users’ end of any application

With its focus on end users and achieving business goals, Citrix EdgeSight™ moves IT emphasis away 
from the “plumbing” – the networks, servers, and infrastructure that support business – to the business 
itself and the conductors of that business. By measuring performance and availability from the users’ 
perspective, EdgeSight cuts across organizational and geographic boundaries and monitors the actual 
end-user experience. This extensive view into the end-user experience lets IT identify, address, and 
resolve issues before they jeopardize security or disrupt business. EdgeSight also provides increased 
visibility into software license utilization, enabling IT to identify new applications that have entered the 
environment, such as spyware, which can pose security risk and violate internal policies. The result: IT 
organizations have the insight, data, and tools they need to ensure that all IT resources are operating at 
peak efficiency – so that the business can do the same.