



ActivCard®

**The Role of IT Security and  
Compliance Regulations**

White Paper

[www.activcard.com](http://www.activcard.com)

# Table of Contents

---

**Executive Summary ..... 3**

**Compliance through Technology ..... 3**

**Compliance Regulations: An Overview..... 3**

**High Expectations for IT Security ..... 5**

**Good IT Security Equals Good Business..... 6**

**ActivCard Solutions ..... 7**

**About ActivCard ..... 8**

## Executive Summary

---

New government regulations and mandates originally aimed at corporate accountability include many provisions that impact a company's IT security and environment. From protecting consumer privacy to ensuring electronic records and signatures, the myriad of new compliance regulations demand more secure IT administration and operation. Companies need to evaluate their security vulnerabilities, shoring up weaknesses and demonstrating auditable security systems.

## Compliance through Technology

---

A series of new compliance regulations concentrate on three key areas: security, privacy and corporate governance. They require increased security and reporting capabilities covering everything from logical and physical security to database administration and disaster recovery. Companies must prove to the federal government, as well as to many state governments, that their IT security, administration and operations are in line with new regulations and mandates.

**Security.** Companies must have applications in place, which can access and monitor external and internal threats and tools and policies to counter threats.

**Privacy.** Companies must ensure the privacy and confidentiality of customers' information, including medical records, credit card information, bank accounts and other personal or financial data.

**Corporate Governance.** Public companies will be required to ensure the accuracy of financial reporting, including the ability to demonstrate the integrity of the systems and applications used to generate financial reports.

According to a paper released by the META Group in September 2004, the regulations, particularly Sarbanes-Oxley, require increased levels of IT security, including but not limited to:

- **User life cycle management.** Organizations should have a process for provisioning an identity, managing its privileges over its lifetime and its removal when no longer necessary.
- **Authorization.** The control of privileges a user has must be clear, defined and able to be documented.
- **Remote user authentication and use.** Authorized personnel accessing financial systems from outside a controlled perimeter should be required to authenticate using two-factor authentication.
- **Strong authentication.** Strong authentication means at least two-factor authentication for all accesses to financial systems.

## Compliance Regulations: An Overview

---

Compliance regulations are often seen as a product of the corporate malfeasance scandals of Enron, WorldCom and others in 2001 and 2002. Scandals, however, are only part of the story. As online commerce and enterprise boomed over the past decade, many branches of government grew increasingly concerned about security and privacy.

Some compliance regulations – particularly those found in the U.S. Public Company Accounting Reform and Investor Protection Act of 2002 (commonly known as Sarbanes-Oxley) – were the direct result of accounting and financial scandals at large, publicly held corporations, but others – particularly Gramm-Leach-Bliley Financial Services Modernization of 1999 – were more the result of security lapses that made the public vulnerable to identity theft and fraud.

Whatever the reasons for the new mandates, many compliance regulations directly impact how companies secure their IT systems, oversee their administration and manage their operations. The point is that enhanced IT security will play a major role in satisfying compliance regulations.

### **Sarbanes-Oxley Act**

Passed in 2002, Sarbanes-Oxley makes senior management, advisors and members of the board of directors individually accountable for the accuracy of its financial reports. The legislation currently affects only publicly held companies; private companies are not impacted.

IT security is impacted in several ways by Sarbanes-Oxley. The regulation requires companies have in place “appropriate controls” that will demonstrate the integrity of the systems and applications used to generate financial reports. Companies must be able to show the presence of user, system and application resource-access controls, and also demonstrate processes that monitor and correct lapses in the controls.

### **Gramm-Leach-Bliley Act**

This legislation is primarily known for its regulations regarding consumer privacy and protections, including the requirement that financial institutions notify consumers about the institution’s privacy policy, including how they share customer information.

The legislation also contains requirements that affect IT security systems and applications. It requires that financial institutions ensure the security and confidentiality of customer’s personal information against what is termed “reasonably foreseeable” internal or external threats. For institutions that provide online commerce, a process must be in place that assesses and monitors the IT threat environment and have in place tools and policies to counter threats.

### **Federal Information Security Management Act (FISMA)**

Expansive in scope, FISMA was enacted by the Bush Administration in 2002 in response to concerns about cyber-security. The act requires federal agencies to develop, document and implement agency-wide programs to secure data and information systems that support agency operations and assets, including those managed by other agencies or contractors. Agencies will be subject to annual tests, including evaluations of their IT security systems. With some 1.4 million cyber-security incidents documented by the government in 2003, many analysts believe the government will put additional pressure on federal agencies to secure their IT infrastructure quickly.

### **Basel II**

Already a part of international banking law, the Basel II Accord is essentially a risk management mandate requiring proven IT security and administration. Capital reserves, supervision and market discipline are Basel II's three risk management pillars. Expected to be finalized by 2006, banking institutions are required to reserve capital that can be used to cover operational risks, including those that arise from inadequate internal processes or external events.

### **U.S. Healthcare Information Portability and Accountability Act (HIPAA)**

HIPAA was originally passed in 1996 to help expand insurance coverage to the unemployed, but over the past several years, it has been expanded to include privacy clauses and security requirements. With the vast amount of medical and patient information online and in databases, the Bush Administration, in 2002, set forth new HIPAA regulations requiring healthcare and insurance organizations have procedures in place to prevent, detect, contain and correct security violations.

They must also have procedures and processes to regularly review records of information system activity.

### European Union Data Protection Directive

As more companies operate in the global economy, European and other international directives must be a part of their business processes. This directive specifies that “personal data” must have “appropriate security.” While that may seem vague, the directive points to IT security systems and infrastructure.

## High Expectations for IT Security

---

Requirements for compliance will be wide-ranging and individual to each company, institution or organization, but several key elements to enhance IT security can be defined. A recent editorial in the Compliance Policy Newsletter segmented the needs as follows:

- Assessment of IT security
- Gap analysis
- Policy definition
- Implementing controls and monitoring those controls
- Auditing and reporting the results



Jay Cohen, chief compliance officer of Dun & Bradstreet, stressed the role technology plays in fulfilling government regulations at a recent conference on compliance regulations. He noted, "technology is an expectation" of the regulators. He added that if a technology is available to identify a problem but a company isn't using it, regulators will want to know why.

Gartner Group, a leading technology research firm, defines a base set of IT security administration and operations capabilities that can satisfy some aspects of the compliance regulations, including:

- Identity and access management policies define access controls for IT resources and applications
- Configuration policies define how IT resources must be configured to make them secure
- IT security infrastructure protects the organization from external intrusion and attacks
- Vulnerability management processes discover and mitigate vulnerabilities and lapses in security policies
- Strong monitoring tools and procedures detect internal and external threats

In the end, Gartner advises that companies implement vulnerability management and IT security management processes and technologies to make the IT infrastructure more secure and resilient. "This," Gartner says, "will improve your ability to demonstrate compliance with a variety of regulations."

Across the board and in all industries, analysts are making it clear that IT technology will play a major role in compliance. A Tower Group report looked at the role of technology in the Basel II Accord explaining, "Capital reserves, supervision and market discipline are Basel II's three risk management pillars. A cohesive technology platform building on these pillars will prove instrumental in integrating the risk and compliance needs across the enterprise."

Caution is always advised as companies look to comply with the increasingly complex legislation. As business invests in its IT security and infrastructure, three guidelines are critical:

- Develop systems that are flexible enough to handle changes in legislation
- Pay close attention to the storing and safeguarding of data
- Create a culture of corporate transparency

## **Good IT Security Equals Good Business**

---

While at first blush, the compliance regulations may feel like legislative over-reach, many analysts believe the regulations are an opportunity for companies and institutions to implement best practices for their IT infrastructure.

With consumer confidence waning in the security of online commerce, the well-publicized phishing attacks and the increasing number of identity thefts and fraud, business will be well served by enforcing much stronger IT security.

IT systems are the engine that drives the modern business process and protecting its infrastructure is good business – whether or not compliance regulations demand it. The compliance regulations give organizations the opportunity to address all the vulnerabilities in their IT security system, infrastructure and environment.

Security breaches are serious, costing millions, while doing untold damage to a company's credibility. Some 75 percent of companies that reported logical security breaches also suffered financial losses, according to a 2003 Computer Security Institute-FBI survey.

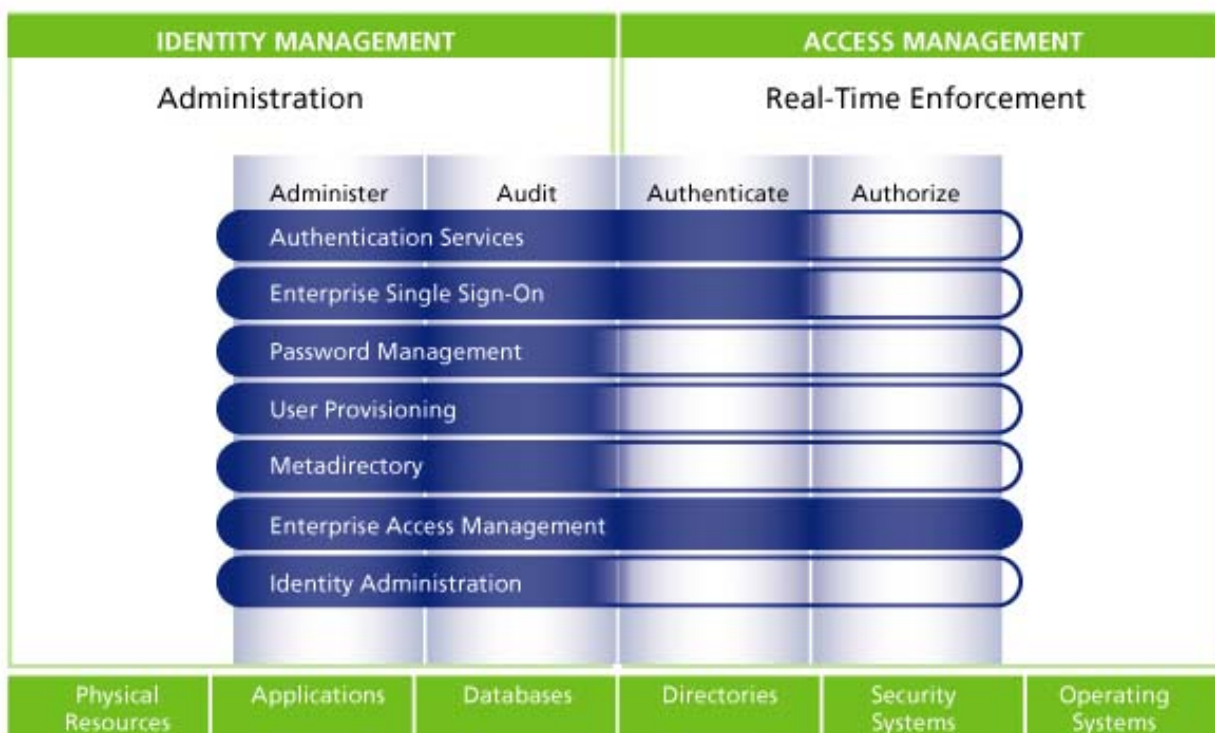
Costs continue to rise when companies deploy multiple security devices that increase management oversight and decrease employee productivity. An average employee, for example, spends some 16 minutes a day logging-on to PCs, email, databases and other networks, according to a PriceWaterhouseCoopers report. Costs continue to rise every time an employee loses a card, forgets a password or leaves the company.

A recent Gartner poll revealed 58 percent of consumers who shop, bank or pay bills online are "very concerned" about online security and only 22 percent believe banks are "extremely competent" in protecting their information. In another study, Javelin Strategy reports consumers by an 8-to-1 margin are letting fears of identity theft affect their use of more advanced online financial services.

The Gartner Groups warns, "Unless consumers' security concerns are adequately addressed, the recent annual growth rates of 20 percent or more will shrink more than they would based on the nature of the expanding user base. If antidotes are not implemented, consumer trust will erode and annual U.S. e-commerce growth will slow to 10 percent or less by 2007."

As they evaluate their ability to comply with the regulations, companies also need to recognize the enormous cost of security breaches – using this window of time, to strengthen all aspects of their security.

A good place for a business to start relates to the Four “A’s” of Information Security. Companies must first ensure that users are properly identified and that these identities are validated to IT resources – authentication. Then, once identification is validated, the roles that each user has must correlate to the access assigned within the enterprise – authorization. This information must be consolidated to provide a holistic view and effective way to manage user access – administration. Finally, IT management must ensure that all activities associated with user access are documented for monitoring, regulatory and investigative purposes – audit. With these processes instilled, companies will be able to conduct real-time enforcements and effective IT security management.



Source: Gartner Research (November 2003)

## ActivCard Solutions

The suite of solutions from ActivCard delivers integration for strong authentication and trusted digital identities, which increases a company’s ability to comply with regulations, while shoring up many long-standing areas of vulnerability in IT administration and operations. Each solution can be deployed either as a point solution to meet a specific and immediate need, or they can be seamlessly integrated to provide superior administrative and cost efficient IT security for compliance.

### Enterprise Access Card Solution

ActivCard Enterprise Access Card integrates with existing IT infrastructure to streamline the issuance and administration of trusted, multi-function digital ID cards. The solution dramatically enhances IT

security by protecting digital credentials on smart cards. Combined with the ActivCard ActivClient™ software, the solution includes secure email, secure remote access, digital signatures and secure web access.

### **Secure Remote Access Solution**

ActivCard Secure Remote Access utilizes a strong, scalable authentication server offering full authentication, authorization and administration services that integrate easily into a company's existing infrastructure. These services protect a company's assets and network security by ensuring and tracking user identity across a network accessed from anywhere.

### **Single Sign-On Solution**

ActivCard Single Sign-On delivers a secure, centralized methodology for eliminating password deficiencies, managing login and protecting a company's assets. Through automated password management and multi-factor authentication capabilities Single Sign-On ensures that sensitive data is safeguarded from internal and external threats, an ideal answer to the new compliance regulations.

## **About ActivCard**

---

ActivCard (Nasdaq: ACTI) is a global provider of identity assurance solutions that, when integrated into an identity management system, allow customers to issue, use and manage trusted digital identities. ActivCard solutions include secure remote access, single sign-on, enterprise access cards, and multi-channel identification and verification. Globally, over seven million users at corporations, government agencies, and financial institutions use ActivCard solutions to safely and efficiently interact electronically. Headquartered in Fremont, Calif., ActivCard has development centers in the US, France, and the United Kingdom and sales and service centers in more than nine countries. For more information, visit [www.activcard.com](http://www.activcard.com).

### Legal Information and Notice

**ActivCard Intellectual Property:** This document or deliverable(s) contain proprietary information of ActivCard Corp. and/or its subsidiaries and affiliates (collectively, "ActivCard") embodying confidential information, ideas, and expressions, no part of which may be reproduced or transmitted in any form or by any means, electronic, mechanical, or otherwise, without prior written permission from ActivCard. This document may not be modified, copied, distributed, transmitted, displayed, performed, reproduced, published, licensed, derivative works created therefrom, transferred, or sold unless expressly agreed by ActivCard. The furnishing of this document does not imply or expressly provide a license to any of ActivCard intellectual property.

**Copyright Notice:** Copyright © 2005 ActivCard, Inc., 6623 Dumbarton Circle, Fremont, California 94555 USA. All rights reserved. This document and ActivCard software products are protected by United States copyright laws and international treaty provisions.

**Trademarks:** ActivCard, ActivCard (logo) and/or other ActivCard products or marks referenced herein are either registered trademarks or trademarks of ActivCard in the United States and/or other countries. The absence of a mark, product, service name or logo from this list does not constitute a waiver of the ActivCard trademark or other intellectual property rights concerning that name or logo. The names of actual companies, trademarks, tradenames, service marks, images and/or products mentioned herein may be the trademarks of their respective owners. Any rights not expressly granted herein are reserved.

**Patents:** ActivCard may have patents, pending patent applications, and/or other intellectual property rights covering subject matter contained in this document or deliverable(s).

**Export Control:** ActivCard products, programs, or services referenced in this publication may not be available in all countries in which ActivCard operates due to export restrictions or changes in market conditions. Recipient agrees to comply fully with all relevant export laws and regulations, including but not limited to the U.S. Export Administration Regulations (collectively, "Export Controls"). Without limiting the generality of the foregoing, Recipient expressly agrees that it shall not, and shall cause its representatives to agree not to, export, directly or indirectly, re-export, divert, or transfer the software, programs, documentation, materials, specifications or any direct product thereof to any destination, company or person restricted or prohibited by Export Controls. In the event that Recipient provides the software, programs, documentation, materials, specifications or any direct product thereof to a third party located in any destination outside the country of delivery by ActivCard, Recipient shall ensure that it enters into a written agreement with such third party that protects ActivCard rights and interests to the same extent protected hereunder and specifies ActivCard as a third party beneficiary. Recipient agrees to provide a copy of such agreement to ActivCard at ActivCard's request and to assist ActivCard, at Recipient's expense, in enforcing ActivCard's rights if ActivCard is not recognized as a third party beneficiary in the applicable jurisdiction.

**Disclaimer:** This publication is intended for informational purposes only. ActivCard makes no warranties, express or implied in this document. Furthermore, the information contained in this document has not been submitted to any formal testing and is distributed 'AS IS'. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the recipient's ability to evaluate and integrate them into an operational environment. While each item may have been reviewed by ActivCard for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Attempts to adapt these techniques to any environment are done so at their own risk. Information in this publication was developed in conjunction with the use of the hardware, software, and networking arrangements specified and is thus limited in application to those specific hardware and software products and levels. The information contained herein is not intended as a specification of any programming interfaces that are provided by ActivCard. This document is subject to change without notice and does not represent a commitment on the part of ActivCard. This document may contain information about product functionality not available in your product release.

[www.activcard.com](http://www.activcard.com)

**ActivCard, Inc.**

TEL: +1 (510) 574 0100

FAX: +1 (510) 574 0101

[info@activcard.com](mailto:info@activcard.com)

CR.WP.L.03/05.PDF