

IT Regulatory Compliance in North America

by Alan Calder



Copyright IT Governance Ltd
Provided by IHS Markit under license with IT Governance Ltd. See [www.itgovernance.co.uk/terms-and-conditions](#) for full terms and conditions.
No reproduction or networking permitted without license from IHS.

Full document details: ITG 2007

IT Regulatory Compliance in North America

A Pocket Guide

Copyright IT Governance Ltd

Provided by IHS Markit under license with IT Governance Ltd. See [www.itg.co.uk/terms](#) for full terms and conditions.
No reproduction or networking permitted without license from IHS.

[Full document details: ITG 2007](#)



Documents

Document Sharing Hub

ITG POCKET GUIDES

Future titles will cover the following subjects:

Practical Information Security series

A Dictionary of Information Security Terms,
Abbreviations and Acronyms
ISO 27001 Assessment without tears
ISO 27001: a Pocket Guide
Risk Assessments for Asset Owners

Practical IT Governance series

Enterprise Architecture
Information Governance
Information Security Governance
IT Audit
IT Governance
IT Governance Frameworks
IT regulatory compliance in the UK
Project Governance
The Integrated Management System

Practical Governance series

BASEL 2
Business Continuity
Corporate Governance in the UK (Turnbull)
Corporate Governance in the US (Sarbanes-Oxley)
Enterprise Risk Management (ERM)
Operational Risk



IT Regulatory Compliance in North America

A Pocket Guide

ALAN CALDER

Copyright IT Governance Ltd



IT Governance Publishing



Documents

Document Sharing Hub

Copyright IT Governance Ltd

Provided by IHS Markit under license with IT Governance Ltd. See=, User=,

No reproduction or networking permitted without license from IHS.

Full document details: ITG 2007

PUBLISHER'S NOTE

Every possible effort has been made to ensure that the information contained in this book is accurate at the time of going to press, and the publishers and the author cannot accept responsibility for any errors or omissions, however caused. No responsibility for loss or damage occasioned to any person acting, or refraining from action, as a result of the material in this publication can be accepted by the publisher or the author.

First published in the United Kingdom in 2007 by IT Governance Publishing.

Apart from any fair dealing for the purposes of research or private study, or criticism or review, as permitted under the Copyright, Designs and Patents Act 1988, this publication may only be reproduced, stored or transmitted, in any form, or by any means, with the prior permission in writing of the publisher, or in the case of reprographic reproduction in accordance with the terms of licences issued by the Copyright Licensing Agency. Enquiries concerning reproduction outside those terms should be sent to the publishers at the following address:

IT Governance Publishing
IT Governance Ltd
Unit 3, Clive Court
Bartholomew's Walk
Cambridgeshire Business Park
Ely
CB74 EH

www.itgovernance.co.uk

© Alan Calder 2007

ISBN 978-1-905356-32-4



Documents

Document Sharing Hub

CONTENTS

CHAPTER 1: Introduction	8
CHAPTER 2: US Legislation	10
CHAPTER 3: Corporate Governance	12
Sarbanes-Oxley.....	12
CHAPTER 4: Basel 2	17
CHAPTER 5: Breach Notification.....	19
CHAPTER 6: Online Personal Privacy	22
The Children’s Online Personal Privacy Act 1998 (‘COPPA’).....	22
The California Online Privacy Protection Act 2004 (‘OPPA’)	23
CHAPTER 7: Workplace Privacy	24
CHAPTER 8: HIPAA.....	26
CHAPTER 9: GLBA	28
The Fair Credit Reporting Act (‘FRCA’)	30
CHAPTER 10: Anti-spam Legislation	32
CAN-SPAM Act.....	32
CHAPTER 11: Federal Information Security Management Act (‘FISMA’)	34
FISMA Implementation Project.....	35
CHAPTER 12: FFIEC	36
CHAPTER 13: EU Regulation	38
The Safe Harbor framework	38
CHAPTER 14: PIPEDA	40



Documents

Document Sharing Hub

Contents

CHAPTER 15: Intellectual Property Rights (IPR) .44

CHAPTER 16: Safeguarding of Organizational
Records.....46

Appendix: IT Governance Resources 50

.....

CHAPTER 1: INTRODUCTION

A key challenge for all IT executive teams is to ensure that the organization avoids breaches of any criminal or civil law, as well as any statutory, regulatory or contractual obligations, and of any security requirements.

Control A.15.1.1 of ISO/IEC27001:2005 (the best-practice information security management standard) provides guidance that is relevant to the IT governance of every organization. It says that the organization should explicitly define and document the statutory, regulatory and contractual requirements for each of its information systems, and that this documentation should be kept up-to-date to reflect any relevant changes in the legal environment.

The specific controls and individual responsibilities to meet these requirements should be similarly documented and kept up-to-date, and should be linked to the list of all the data assets and processes in the organization, together with their ownership details.

The outline of relevant legislation in this Pocket Guide is not intended to be authoritative: the US legal system is a complex one that has evolved over hundreds of years.

Current legal advice must be taken from qualified, specialist legal counsel if an organization wants or needs to rely on any matter identified here.



Documents

Document Sharing Hub

1: Introduction

Equally, it should be noted that this Pocket Guide deals with key current compliance issues for organizations based or operating in or supplying customers in the United States. Laws are likely to be different in other countries and, therefore, organizations who are based elsewhere should take specialist local advice. Organizations based in the United States with operations elsewhere in the world will need to deal with the US requirements as well as those of the foreign countries in which they operate and, again, specialist legal advice should be taken.

Web trading (even for US-domiciled corporations) could potentially take place in a multitude of countries and the law in this area is constantly changing and developing. Any organization that is trading across the web without limits on who may access its website should take specialist advice to ensure that contractual and trading terms are watertight and that issues of jurisdiction and which law (that of the country in which the server is based, or the organization is based, or the customer is based, or to which delivery is made) will apply to any transaction have been resolved, and to ensure that there is an appropriate acceptance and/or waiver of liability on the entrance to the website.

State-level privacy laws across the United States may have relevance to e-commerce businesses throughout the world.



Documents

Document Sharing Hub

CHAPTER 2: US LEGISLATION

Legislation and regulation that is relevant to North American organizations includes:

- The Sarbanes-Oxley Act, primarily a corporate governance act but with significant regulatory implications – see chapter 3, below
- Basel 2, which primarily affects banks and major financial institutions and has extensive IT compliance implications – see chapter 4, below
- The Californian Senate Bill 1386, which requires notification of breaches of personal data security, and a host of similar state-level laws – see page 19, below
- Online personal privacy legislation, including the California Online Privacy Protection Act 2004 ('OPPA'), which requires websites serving Californians (irrespective of their geographic or jurisdictional location) to comply with strict privacy guidelines – see page 23, below
- The Financial Services Modernization Act, usually called the Gramm-Leach-Bliley Act ('GLBA'), which deals with consumer financial data – see chapter 9, below
- The Fair Credit Reporting Act ('FCRA'), designed to protect people from identify theft – see page 30, below
- The Health Insurance Portability and Accountability Act ('HIPAA'), which requires healthcare organizations to protect and keep up-



Documents

Document Sharing Hub

2: US Legislation

to-date, their patients' healthcare records – see chapter 8, below

- The Federal Information Security Management Act ('FISMA') – see chapter 11, below
- The Federal Financial Institutions Examination Council (FFIEC) standards on 'Authentication in an Internet Banking Environment' – see chapter 12, below
- Canada's Personal Information Protection and Electronic Documents Act ('PIPEDA') – see chapter 14, below

Copyright IT Governance Ltd
Provided by IHS Markit under license with IT Governance Ltd
No reproduction or networking permitted without license from IHS



Documents

Document Sharing Hub

CHAPTER 3: CORPORATE GOVERNANCE

Sarbanes-Oxley

The Sarbanes-Oxley Act of 2002 (SOX), introduced in the United States in the aftermath of Enron, has important IT governance implications for listed American companies, their foreign subsidiaries and foreign companies that have US listings. It applies to all Securities and Exchange Commission ('SEC')-registered organizations, irrespective of where their trading activities are geographically based. Compliance is mandatory and there are significant potential sanctions for individual directors.

	Section		
	302	404	409
Requirement	Quarterly certification of financial reports Disclosure of all known control deficiencies Disclosure of acts of fraud	Management's annual certification of internal controls Independent accountant must attest report Quarterly reviews of updates / changes	Monitor operational risks Material event 'Real-time' implications – 4 business days allowed for report to be filed
Responsibility	CEO CFO	Management Independent accountant / auditor	Management Independent accountant / auditor



Documents

Document Sharing Hub

3: Corporate Governance

While the Act lays down detailed requirements for the governance of listed corporations, the three highest profile and most critical sections – which were implemented in phases – are 302, 404 and 409.

The SEC, which is responsible for implementation of SOX, has relevant information available at www.sec.gov/spotlight/sarbanes-oxley.htm, and the Sarbanes-Oxley website itself is at www.sarbanes-oxley.com.

Internal controls and audit

The management's Internal Control Report needs to include an assessment of the effectiveness of internal controls, as well as the procedures of the issuer for financial reporting.

- Internal controls have to be established and maintained. These must ensure that material information regarding the company (including consolidated subsidiaries) is known by the certifying officer (CEO and CFO), as well as others in the company.
- The effectiveness of the company's internal controls must be evaluated by the certifying officer. The report should include their conclusions with respect to the effectiveness of the internal controls.
- Disclosure must be made to the company's auditors and audit committee of all significant deficiencies in the company's internal controls.
- Disclosure must be made to the company's auditors and audit committee of any fraud (whether or not material) involving management

Documents



Document Sharing Hub

3: Corporate Governance

or other company employees who play a significant role in the company's internal control system.

- The Internal Control Report should disclose any changes that could significantly affect the company's internal controls since the date when such controls were last evaluated.

One widely used internal control framework is known as the COSO framework or, to give it its own title, the 'Internal Control – Integrated Framework', which contains the recommendations of the Committee of Sponsoring Organizations of the Treadway Commission (www.coso.org). The sponsoring organizations include the American Institute of Certified Public Accountants (AICPA), the Institute of Internal Auditors, the Institute of Management Accountants and the American Accounting Association. The PCAOB (Public Company Accounting Oversight Board, at www.pcaobus.org, created under SOX to oversee the activity of the auditors of public companies in the United States) expects the majority of public companies to adopt the COSO framework and its Auditing Standard No 2, dealing with audit of internal control over financial reporting, assumes that the COSO framework (or one substantially like it) will have been adopted.

Auditing Standard No 2 contains, at paragraph 15, a key statement:

'Not all controls relevant to financial reporting are accounting controls. Accordingly, all controls that could materially affect financial reporting, including controls that focus primarily on the



Documents

Document Sharing Hub

3: Corporate Governance

effectiveness and efficiency of operations or compliance with laws and regulations and also have a material effect on the reliability of financial reporting, are a part of internal control over financial reporting.’

COSO identifies two broad groups of IT systems control activities:

- general controls, and
- application controls.

General controls are those controls which ensure that the financial information from a company’s application systems can be relied upon. General controls exist most commonly as part of an Information Security Management System (such as that identified in ISO27001/ISO17799).

Application controls are embedded in the software to detect or prevent unauthorized transactions. Such controls can be used to ensure the completeness, accuracy, validity and authorization of transactions.

Paragraph 50 of Auditing Standard No 2 says:

‘information technology general controls over program development, program changes, computer operations, and access to programs and data help ensure that specific controls over the processing of transactions are operating effectively’.

Auditing Standard No 2 (paragraph 52) requires evaluation of the effectiveness of company-level controls at the outset of the audit engagement, on the basis that it is the company-level controls that have such a ‘pervasive impact on controls at the process



Documents

Document Sharing Hub

3: Corporate Governance

transaction or application level'. These company-level controls include consistent policies and procedures and codes of conduct. The auditing standard specifically refers to the existing standard, *Consideration of Internal Control in a Financial Statement Audit*, issued by the AICPA in 1990, because it sets out clearly the effect of information technology on internal control over financial reporting.

SEC regulations

There are many SEC regulations that are important to publicly listed companies and which require compliance. These include the SEC's regulation FD, which bars selective disclosure of material non-public information.