



GLBA And The Suitability of CRAMM

SIEMENS

Global network of innovation

Insight Consulting

Management in Confidence

TABLE OF CONTENTS

1. INTRODUCTION.....1

2. WHAT IS GLBA ?.....1

3. WHAT GLBA INVOLVES1

4. THE GLBA SAFEGUARDS FRAMEWORK.....2

4.1. GLBA & RISK 2

4.2. GLBA & ENFORCEMENT AND COMPLIANCE 2

4.3. BS7799 & ISO/IEC 17799 2

5. SUMMARY OF CRAMM.....3

6. USING CRAMM ON GLBA PROJECTS4

7. GLBA CONTROLS.....4

1. INTRODUCTION

This briefing note has been compiled to demonstrate CRAMM's capabilities and constraints in supporting the achievement of GLBA compliance.

2. WHAT IS GLBA ?

'GLBA' is the 'Gramm-Leach-Bliley Act' passed in the USA to safeguard customer information, whether electronic or paper-based, maintained by or on behalf of state member banks and bank holding companies and their non-bank subsidiaries, except for brokers, dealers, persons providing insurance, investment companies and investment advisors¹. It also applies to customer information maintained by or on behalf of Edge corporations, agreement corporations and uninsured licensed branches or agencies of foreign banks.

In order for USA-based institutions to comply with GLBA requirements, they are required to be examined (audited) in terms of their compliance against the requirements of the Act by the relevant regulatory authority.

3. WHAT GLBA INVOLVES

The key requirements in order to comply with GLBA are:

- ◆ **Protection of Non-public Personal Information** – This requires that a **Privacy Obligation Policy** be in place and is reviewed regularly;
- ◆ **Financial Institution Safeguards** covering 'the security and confidentiality of customer records'; to protect such records against any anticipated threats and hazards that could compromise the security or integrity of the records; and protect such records or information against any unauthorised access or use which could result in substantial inconvenience to any customer;
- ◆ **Obligations with respect to the disclosure of personal information** – covers the notice requirements, opt-out specifications, exceptions and limits on the re-use of information. It includes limitations on sharing of information for marketing purposes;
- ◆ **Disclosure of Institution Privacy Policy** – The aspects covered in this section are the responsibilities placed on institutions in advising their customers, at least annually, of their policies and practices relating to the disclosure of customer information and the information that is included in such notifications to customers;
- ◆ **Enforcement** – This describes the regulatory bodies who are empowered to enforce the requirements of the Act;

Inherent within the Act is the need to conduct a risk assessment and then continue to maintain an 'oversight' of the risks to ensure that the safeguards implemented continue to meet the assessed risks.

¹ Separate regulations or guidelines issued by the appropriate regulatory agency regarding information security may apply to these subsidiaries

4. THE GLBA SAFEGUARDS FRAMEWORK

These are provided in detail within the Guidance provided by the relevant Regulatory Bodies governing the activities and operations of the various financial institutions.

However, the general aspects covered by the majority of institutions include:

- ◆ Administrative Safeguards;
- ◆ Physical Safeguards;
- ◆ Technical Safeguards.

These general safeguards are attached and analyzed at the end of this paper, showing how CRAMM assists in delivering the required controls in each of the relevant areas.

4.1. GLBA & RISK

Risk is typically the basis recommended for ensuring that IT systems handling, storing, manipulating and transmitting essential or critical data are appropriately protected. This too is the common ground with Corporate Governance, for which GLBA can be depicted as the USA's 'Financial Institution Information Governance' component, sitting alongside / overlapping with the Corporate Governance agenda.

It is Insight's understanding that Financial Institutions are required to implement a comprehensive *written* information security programme appropriate to the size, complexity and nature and scope of the institutions activities. It is further understood that all the elements of the programme should be implemented and managed in a coordinated manner and that implementation across the various parts of the institution should be based of what is appropriate.

Based on the results of the risk assessment, a decision is taken to determine whether the impact warrants the implementation of appropriate controls or countermeasures to 'address' the level of risk.

4.2. GLBA & ENFORCEMENT AND COMPLIANCE

A final requirement is for the Institution to be subject to regular inspections by the relevant functional regulators. The implicit expectation of the Act is that the Inspection of the Management System is of a working / established system rather than a newly created system ready to be implemented.

4.3. BS7799 & ISO/IEC 17799

BS7799 contains 2 components or parts. Part 1 provides a list of controls / safeguards that are accepted good practice. This part has also been adopted as ISO/IEC 17799. Part 2 of the standard provides a process and model for an Information Security Management System (ISMS) founded upon effective an effective, on-going, risk analysis and management process.

Certification is available against part 2 with about 120 organisations holding such status, although c.60% are presently UK based. BS 7799 Part 2 does not currently have an ISO equivalent but ratification of Part 2 as either ISO/IEC 17799 Part 2 or as ISO/IEC 27799 is expected shortly. Adoption of this standard is growing internationally, including in the USA through Global Organisations, in part no doubt driven by HIPAA & GLBA requirements.

5. SUMMARY OF CRAMM

The CRAMM Version 5 'Expert' Toolkit, released in January 2003, is a comprehensive Information Security Support Tool and data repository that is presently in use in over 600 locations for over 430 organisations in 24 countries and 21 business sectors.

It has been used extensively within the UK National Health Service (NHS) and various financial sector organisations to manage the risks to personal and healthcare information and to support the achievement of the Information Governance goals of Patient Privacy, Data Protection, Freedom of Information, Data Quality and Security. Some banks have also used it to develop specific Risk Models to ensure that all banking entities in a specific geographic region meet a common minimum standard and achieve reasonable compliance against the requirements of BS 7799.

The risk models provide the following integrated functionality:

- ◆ For BS7799 compliance or certification:
 - ◆ Initiation and scoping of compliance;
 - ◆ Gap Analysis;
 - ◆ Action Planning (consistent with GLBA's 'Security Program');
 - ◆ Security Improvement Programme (consistent with GLBA's 'Program');
 - ◆ Statement of Applicability (providing a summary of the current compliance level);
 - ◆ Treatment of control Objective Reporting;
 - ◆ Compliance Checking (consistent with GLBA's 'Enforcement');
 - ◆ Risk re-assessment (consistent with GLBA's 'Oversight').

- ◆ For Information Security Risk Assessment;
 - ◆ Asset Identification;
 - ◆ Dependency Modelling;
 - ◆ Business Impact Assessment;
 - ◆ Threat and Vulnerability Assessment;
 - ◆ Calculation of Measures of Risk;
 - ◆ Calculation of Justified and Appropriate Countermeasures;
 - ◆ Countermeasure Gap Analysis including status reporting based upon management decisions for which supporting justifications can be collected;
 - ◆ Risk Management Decision Support;
 - ◆ Risk Treatment Reporting;
 - ◆ 'What If ?' Support.

- ◆ For Information Security Management;
 - ◆ Recovery Requirements Reporting;
 - ◆ Security Documentation ‘Wizards’;
 - ◆ Functionality to support Outsourcing;
 - ◆ Functionality to support Business Continuity Management Strategy Development.

In addition to handling financial impacts, CRAMM’s Business Impact Assessment, being qualitative, also handles ‘soft impacts’, such as reputational loss, embarrassment, personal safety (i.e. loss of life) and legal breach etc. in a consistent manner.

CRAMM’s threat and vulnerability assessment addresses all known threats to IT systems of all types whether technical, physical, logical, human or communications and can support the assessments with detailed questionnaires or user-entered opinions.

As can be seen on the safeguards tables below, the CRAMM Countermeasure Library covers all of the safeguards required by GLBA and many more that GLBA has overlooked.

6. USING CRAMM ON GLBA PROJECTS

The stark and strong conclusion can be made that GLBA compliance or certification can successfully and comprehensively be delivered by application of the BS7799 ISMS Model and supporting processes.

In turn therefore, it can be equally strongly asserted that the adoption of CRAMM Version 5 is appropriate for GLBA, fully supporting as it does both the BS 7799 and GLBA Process models and key concepts.

7. GLBA CONTROLS

Topic	Aspect	Comment
Board Involvement		
	Corporate Information Security Program	Integral part of method & of the Cm Database
	Appropriate to size of Institution	In-built capability within the Toolkit
	Program Implementation	Addressed as part of the Countermeasure database ²
	Program Elements	Addressed as part of the Countermeasure database
	Assigned Security Responsibility	Addressed as part of the Countermeasure database
	Coordination of Programs	Addressed as part of the Countermeasure database

² This means that there are controls within the countermeasure database that will provide varying degrees of strength depending on the assessed level of risk (i.e. result of the risk assessment process)

Management in Confidence

Topic	Aspect	Comment
	Reporting & Review	Addressed as part of the Countermeasure database
Risk Assessment Process		
	Structure/Method	Inherently structured and consistent in its implementation and use
	Consistent	As above
	Assets, Threats, Vulnerabilities	Incorporated into method
	Formal Process	Yes
	Asset valuation	Integral part of method
	Threat Identification	Integral part of method with over 30 listed
	Justified Impact Analysis	Integral part of method
	Measure of Risk Analysis	Integral part of method
	Risk Treatment & Prioritisation	Integral part of method
Security Management & Control		
	Internal Controls	Addressed as part of the Countermeasure database
	Policies	Addressed as part of the Countermeasure database
	Access Controls (Logical)	Addressed as part of the Countermeasure database
	Access Controls (Physical)	Addressed as part of the Countermeasure database
	Encryption	Addressed as part of the Countermeasure database
	Security input for System Changes (Change Control)	Addressed as part of the Countermeasure database
	Segregation of Duties	Addressed as part of the Countermeasure database
	System & Network Monitoring	Addressed as part of the Countermeasure database
	Incident Detection	Addressed as part of the Countermeasure database
	Incident Response	Addressed as part of the Countermeasure database
	Data & System backup	Addressed as part of the Countermeasure database
	Business recovery	Addressed as part of the Countermeasure database
	Staff Training & Awareness	Addressed as part of the Countermeasure database
	User Training	Addressed as part of the Countermeasure database
	Security Testing (Independent)	Addressed as part of the Countermeasure database
	Test Review	Addressed as part of the Countermeasure database
Service Providers		
	Selection of Service Providers	Considered within the BIA, Risk Assessment and controls within the Cm Database
	Information Exchange	Integral part of the method
	Contracts (Security Requirements)	Integral part of the method

Management in Confidence

Topic	Aspect	Comment
	Performance & Security Monitoring	Addressed as part of the Countermeasure database
	Financial Stability of Provider	Not covered explicitly, other than where Cmeasures not implemented and thus risks not adequately managed.
Information Security Program		
	Program flexibility	Integral part of the method
	Technology Changes	Addressed as part of the Countermeasure database
	Information Sensitivity	Addressed as part of the Countermeasure database
	New Threats	Addressed as part of the ongoing support and update of CRAMM
	Business Changes (mergers, etc.)	Part of the requirement for regular risk reviews and also addressed as part of the Countermeasure database
	New Systems (development, etc.)	Addressed as part of the Countermeasure database
Audit		
	Reporting	Addressed as part of the Countermeasure database
	Remedial Action	Addressed as part of the Countermeasure database