

Implementing Information Security Governance (ISG)

A Case Study: Entrust

The material provided in this document is for information purposes only. It is not intended to be advice. You shall be solely responsible for acting or abstaining from acting based upon the information in this document. ENTRUST DOES NOT WARRANT THE QUALITY, ACCURACY OR COMPLETENESS OF THE INFORMATION CONTAINED IN THIS DOCUMENT. THIS INFORMATION IS PROVIDED "AS IS" WITHOUT ANY REPRESENTATIONS, WARRANTIES, AND/OR CONDITIONS OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, BY USAGE OF TRADE, OR OTHERWISE, AND ENTRUST SPECIFICALLY DISCLAIMS ANY AND ALL REPRESENTATIONS, WARRANTIES AND/OR CONDITIONS OF MERCHANTABILITY, SATISFACTORY QUALITY, NON-INFRINGEMENT, TITLE AND FITNESS FOR A SPECIFIC PURPOSE.

Entrust is a registered trademark of Entrust, Inc. in the United States and certain other countries. Entrust is a registered trademark of Entrust Limited in Canada. All other Entrust product names and service names are trademarks or registered trademarks of Entrust, Inc. or Entrust Limited. All other company and product names are trademarks or registered trademarks of their respective owners.

Published July 2004

INFORMATION SECURITY GOVERNANCE

As a worldwide leader in identity and access management solutions, Entrust takes information security very seriously. Just as our customers depend on robust security solutions, so do we as a company. Given our leadership role and the increasing emphasis on cyber security, I directed Entrust's management team to review and improve our internal information security practices.

In doing so, we confirmed that cyber security is best viewed, not solely as a technology challenge, but as a corporate governance issue. Investments in cyber security should be tied to actual business risk in order to achieve maximum value and rational allocation of resources. Periodic risk assessment and reporting give visibility to business decision makers charged with implementation and oversight. Moreover, like quality assurance, information security requires continuous, incremental improvement over time.

We also discovered that the framework necessary to systematically integrate information security into corporate governance was lacking. Because it is imperative for industry to have an information security governance framework, Entrust approached the Business Software Alliance (BSA) to see how industry could best work together. At their recommendation, I co-chaired a task force of leading software companies that profiled a framework in its October 2003 report, Information Security Governance: Toward a Framework For Action.

As a result of the work with BSA, Entrust was asked to co-chair a blue ribbon Corporate Governance task force at the National Cyber Security Summit hosted by the Department of Homeland Security and the National Cyber Security Partnership. The goal of this task force was to achieve consensus on an information security governance framework with broad application to business, educational institutions and non-profit organizations. This report, Information Security Governance: A Call to Action, was released in April 2004.

Having spent considerable effort on this important issue, we wanted to share the Entrust experience in order to help others with their information security governance programs. The following pages cover the Entrust story, including the steps we took in developing, testing and implementing sound information security governance within our organization.

It is clear that information security is of critical importance. It is key to extending the enterprise to enable deep integration with partners, suppliers and customers while aiding compliance with regulations such as Sarbanes-Oxley. Importantly, information security also protects economically vital critical infrastructure from attack. I urge you to accept the challenge and immediately take steps to adopt Information Security Governance.



F. William Conner
Chairman and CEO



Table of Contents

1	Introduction	1
2	Creating an Information Security Governance Framework	3
2.1	Building on Existing Best Practices	3
2.2	The Missing Link	3
2.3	ISO 17799	4
2.4	The Quality Analogy	5
3	Information Security Governance in Action	6
3.1	Cycles of Continuous Improvement: Cycle One	6
3.2	Cycles of Continuous Improvement: Cycle Two	10
3.3	Cycles of Continuous Improvement: Cycle Three	11
4	Benefits of Implementing the ISG Framework	14
5	About Entrust	15
5.1	Entrust Customers	15
5.2	Entrust Solutions	16
	<i>Entrust Secure Identity Management Solution</i>	<i>16</i>
	<i>Entrust Secure Data Solution</i>	<i>17</i>
	<i>Entrust Secure Messaging Solution</i>	<i>17</i>

1 Introduction

Effective corporate governance has become an increasingly urgent issue over the last few years. Defined, corporate governance is the set of policies and internal controls by which organizations are directed and managed. Information Security Governance (ISG) is a subset of corporate governance that relates to the security of information resources.

Information security¹ is all too often perceived as a wholly technical issue rather than being put in the context of business risk. For companies, educational institutions, and non-profit organizations to make progress in securing their information assets, however, executives must make information security an integral part of core business operations. The best way to accomplish this goal is to embed ISG as part of the internal controls and policies that constitute corporate governance.²

Entrust became active in industry efforts to create an ISG framework several years ago. As a leader in identity and access management solutions, Entrust is often approached by customers seeking guidance on building, maintaining and managing information security. Simultaneously, Entrust was closely watching the development and introduction of Gramm-Leach-Bliley, the Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley, Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) and other government regulations.

As mentioned in this report's introductory letter, Entrust Chairman and CEO Bill Conner directed the management team to develop an internal information security governance program. As this process went forward and it became clear that there was no common ISG framework, Mr. Conner recognized that other organizations were undoubtedly faced with the same challenge.

At the request of the Business Software Alliance, Mr. Conner co-chaired a governance task force to address the ISG framework challenge and in October 2003 the BSA issued a report laying the foundation for an ISG framework.³

Building on the BSA findings, a Corporate Governance Task Force was formed at the National Cyber Security Summit in association with the Department of Homeland Security. The National Cyber Security Partnership's (NCSP) Corporate Governance Task Force issued its report in April 2004, launching a full Information Security Governance Framework.

Throughout, Entrust has played an active role in developing, testing and refining the framework. The process and the lessons we learned may help other organizations of all sizes to establish their own ISG programs.

Before proceeding with the story of Entrust's experience, it seems valuable to share the process output. At the core of governance is the ability to assess risks, remediate them appropriately and report periodically on progress. Keeping the reporting process as simple

¹ As used here, the term Information Security means protecting information and information systems from unauthorized use, disclosure, disruption, modification or destruction to provide confidentiality, integrity and availability.

² "Information Security Governance: A Call to Action", National Cyber Security Partnership Governance Task Force, April 2004, p.1, www.cyberpartnership.org ("NCSP Task Force Report").

³ "Information Security Governance: Toward a Framework for Action", Business Software Alliance, October 2003, www.bsa.org/usa/policy/index.cfm ("BSA Task Force Report").

as possible is vital. The following chart is an example of the summary reporting presented to the organization's Board of Directors.

Information Security Summary Report			
Security Practices	Risk Level*		
<i>(based on ISO 17799 chapters)</i>	R	Y	G
Security Policy	0	1	1
Organizational Security	1	3	1
Asset Classification & Control	1	0	2
Personnel Security	1	4	4
Physical & Environmental Security	2	4	12
Communications & Operations Management	2	10	20
Access Control	4	12	14
Systems Development & Maintenance	0	2	11
Business Continuity Management	1	2	2
Compliance	2	5	3
TOTAL <i>(*sample numbers only)</i>	14	43	70

The chart clearly and concisely presents the types of risk, based on the ISO 17799 chapter headings, and their criticality, communicated by a simple Red (High), Yellow (Medium or Moderate) and Green (Low or Acceptable) lexicon. The numbers represent a rollup of the 127 elements that compose the ten ISO 17799 chapters. This simple but comprehensive view, backed by the detailed steps of an information security governance program, enables the Board, CEO, CIO and business unit executives to quickly:

- understand the state of an organization's information security
- identify the top issues
- see the progress made since the last reporting period

The following pages discuss how this summary chart was developed and used within our organization and by the Board of Directors, as Entrust incorporated Information Security Governance into our corporate governance process.

2 Creating an Information Security Governance Framework

2.1 Building on Existing Best Practices

Entrust realizes that in order to be widely adopted, an Information Security Governance framework should be built on existing frameworks and accepted best practices. A brand-new framework built from scratch would not likely be extensively embraced and put into practice.

Therefore, the first step Entrust pursued was an extensive literature review to examine existing information security best practices guidance and related issues of governance. Sources reviewed included:

- Technology orientation – SANS Institute, CERT
- Security Professional Certification – CISSP
- Audit and Governance aspects – FISCAM, OECD, IT Governance Institute (COBIT), Gartner
- Other government initiatives – HIPAA, GAO, OMB, National CyberSpace Strategy, eGov Strategy, FISMA
- Other countries (cursory scan only) – Canadian, UK, Australia, Japan, Singapore
- Other information sources – GASSP, SANS library, Business Round Table, ISO, NIST

To frame an analysis, a methodology from business process re-engineering was employed looking at People, Process and Technology aspects as they relate to Operational, Tactical and Strategic objectives. Each source was mapped to the matrix and analyzed for coverage and suitability as a governance framework that would be readily adopted by a broad range of organizations.

2.2 The Missing Link

All too often, information security programs fail to involve executive management in the risk assessment and remediation process. Since weaknesses in information security create real business risk, responsibility for information security ultimately lies not just with the CIO, but also with executive management, including the CEO and the Board of Directors. Only executive management can determine an acceptable risk profile, focus information security investments appropriately and drive results.

After reviewing the literature on information security, we determined that ISO 17799 provided the best overall fit. Even ISO, however, fails to address management involvement in information security beyond stating its importance. Indeed, the security literature remains weak when it comes to articulating Strategic People and Process issues.

However, the US government's FISMA, the Federal Information Security Management Act of 2002, and its predecessor the Government Information Security Reform Act, effectively addressed these areas for government agencies. After a review of FISMA, it was clear that the concepts could easily be translated into guidance the private sector could adopt. FISMA, adapted for the private sector, served as the basis for completing the emerging ISG framework as shown below.

	Operational	Tactical	Strategic
People	ISO 17799	ISO 17799	FISMA (adapted)
Process	ISO 17799	ISO 17799	FISMA (adapted)
Technology	ISO 17799	ISO 17799	ISO 17799

2.3 ISO 17799

ISO 17799 was chosen as the “best” reference because of its combination of comprehensiveness and its international level of acceptance, including rapidly growing usage in North America. ISO 17799 was written solely for information security practices within a business as a whole, is not IT exclusive, and is built around policy and process. These characteristics made ISO 17799 an ideal reference for ISG.

Two other commonly referenced works, COBIT⁴ and COSO⁵, were also thoroughly examined. While both documents bring valuable insight and deserve a space on the reference shelf, ISO 17799 is the better reference for the purpose of Information Security Governance. COBIT is a larger reference set, however this comprehensiveness can make implementation onerous. Secondly, COBIT is directed toward a CIO audience and focuses on efficiency and effectiveness of the IT environment rather than information security tied to business risk. COSO is an excellent internal control framework, but provides minimal guidance and has not been adequately updated to reflect security environment changes since it was written in 1992.

Following this basic analysis, the Business Software Alliance Governance Task Force took these recommendations, vetted them against twenty-one additional resources and ultimately came to the same conclusion. The BSA report, which included a basic ISG framework, was published in October 2003.⁶ Further ratification of this direction came from the NCSP Corporate Governance Task Force that accepted the BSA findings and built upon them for the Information Security Governance Framework published in April 2004.⁷

⁴ *Control Objectives for Information and Related Technology*, IT Governance Institute and the Information Systems Audit and Control Association

⁵ *Internal Controls – Integrated Framework*, Committee of Sponsoring Organizations of the Treadway Commission

⁶ BSA Task Force Report

⁷ NCSP Task Force Report

2.4 The Quality Analogy

During the NCSP task force discussions, the parallels to the quality movement became vividly clear, and this policy model was adopted for the framework. Task force members quickly realized that, like quality, Information Security is a continual improvement process where perfection is desired but rarely and fleetingly achieved. By making incremental improvements over time, significant and measurable progress has been made at Entrust. Periodic cycles of assessment, remediation and reporting result in continual improvement.

Like a quality drive, the assessment process can appear to be a massive task and it is easy to become trapped in volumes of detail. Therefore, as with quality guidance, it is important to keep the process as simple as possible. Entrust refused to succumb to “paralysis by analysis”, and maintained focus on improving the organization’s security posture rather than performing complex risk analyses. This process began with identifying the biggest and most impactful items first, where the business need was greatest.

With lessons learned from a decade of security experience, Entrust is well aware that Information Security is a journey, not a destination. Changes in technology and environmental threats can emerge overnight, resulting in new vulnerabilities that need to be addressed. Therefore, an organization is never “finished”, but must continually re-assess and remediate.

Like the quality manager, the security manager monitors the environment, provides regular assessments, and makes recommendations for improvement, but the business managers determine where investments will be made and which issues will be dealt with first. This approach was very effective at Entrust in creating buy-in from internal stakeholders for the ISG program. It also relieved some of the angst in the IT organization because it formalized reality – if the business didn’t buy into the need for an investment, it usually didn’t happen.

Finally, it is important to note that in information security, like quality, technology plays a secondary role behind process and procedures. This point is reinforced in ISO 17799, where two-thirds of the elements focus on policy, process and procedures.

3 Information Security Governance in Action

From the beginning, Entrust has worked to ensure the framework would be actionable, effective and acceptable to a wide, global audience as a best practice. This involved not only task force participation, but also many one-on-one discussions with customers from leading e-Governments and Global 2000 organizations, as well as several open, townhall-format meetings with a broad range of industry representation.

What follows is a collection of key elements for success, or lessons learned, that emerged from those discussions, as well as our experience putting them into action within Entrust.

3.1 Cycles of Continuous Improvement: Cycle One

The first step organizations need to take is defining the roles and responsibilities for information security governance. The ISG framework lists the critical responsibilities and the NCSP report provides additional guidance for mapping them to organizations of various sizes and structures. To put the framework in place, Entrust had to review existing governance policies and determine if the proper roles and responsibilities were assigned and well understood.

3.1.1 Assigning responsibility and accountability

Maintaining the analogy to quality, and consistent with many security best practices, the first step should be a high-level assessment of information security policies and responsibilities. At Entrust, the first iteration of the security review lasted approximately half a day. The CIO and members of the physical and information security teams participated, reviewing the results with executive management. The intent of the session was to determine areas that were vague, unknown or undefined.

Using ISO 17799, the team rated the company on each element using a simple Red/Yellow/Green indicator for each. Where the answer was not immediately known, that item was marked as Red – if the policies and responsibilities weren't crystal clear to the people directly involved with information security in the business, then it was a problem that needed to be fixed. [See example table on next page.]

Following the first pass, 25 of 127 items were identified as Red, the majority of which were unknown or unclear. Members of the team were assigned to research the Red items and most resulted in simple awareness and clarification activities; these were addressed quickly and required little effort. Using the ISG framework as a guide, Entrust documented its Information Security Program, defining and clarifying many of these responsibilities and program processes.

3.1.2 Lesson #1: Keep the Process Simple

It is easy to become overwhelmed by trying to measure each risk in a granular fashion. Time and resources spent to exhaustively document levels of risk can be better spent in remediating problem areas, so keep it simple. Start with a simple subjective risk assessment. In the words of the US Office of Management and Budget (OMB A-130 Appendix III):

*"In the past, substantial resources have been expended doing complex analyses of specific risks to systems, with limited tangible benefit in terms of improved security for the systems. Rather than continue to try to precisely measure risk, security efforts are better served by generally assessing risks and taking actions to manage them"*⁸

	Risk Level*			Commentary
	R	Y	G	
<i>(based on ISO 17799 chapters)</i>				<i>(relevant notes)</i>
(3) Security Policy	0	1	1	Subtotal of chapter
(3.1) Information Security Policy				
(3.1.1) Information security policy document			1	
(3.1.2) Review and evaluation		1		
(4) Organizational Policy	3	3	4	Subtotal of chapter
(4.1) Information Security Infrastructure				
(4.1.1) Management information security forum			1	
(4.1.2) Information security co-ordination		1		
(4.1.3) Allocation of information security responsibilities		1		
(4.1.4) Authorization process for info. processing facilities	1			
(4.1.5) Specialist information security advice	1			
(4.1.6) Co-operation between organizations		1		
(4.1.7) Independent review of information security	1			
(4.2) Security of Third Party Access				
(4.2.1) Identification of risks from third party access			1	
(4.2.2) Security requirements in third party contracts			1	
(4.3) Outsourcing				
(4.3.1) Security requirements in outsourcing contracts			1	
... through Chapter 12, "Compliance"				
TOTAL	30	50	47	

**Sample numbers only*

3.1.3 Lesson #2: Use a Straightforward Red/Yellow/Green Ranking

Again, do not spend time extensively rating risk. Use the simple and common lexicon of Red (High), Yellow (Medium or Moderate) and Green (Low or Acceptable). This will help the organization focus on areas of greatest risk. By using a R/Y/G lexicon, those who are

⁸ "Security of Federal Automated Information Resources", US Office of Management and Budget Circular No. A-130, Appendix III, http://www.whitehouse.gov/omb/circulars/a130/a130appendix_iii.html

implementing and reviewing the process are able to quickly understand the severity or urgency. Remember that the audience is executive management and the board, and while operational groups may need to understand relative priorities, the executive team does not need to know what shade of Yellow something might be. The National Institute of Standards and Technology (FIPS 199) can help you define the three levels. For example, “high” risks are defined as follows:

“...the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries...”⁹

3.1.4 The Board of Directors

Entrust’s Board of Directors, particularly the Governance Committee, was very supportive of the ISG process and enthusiastic about the increased information it provides to aid in oversight and decision-making. The Board was briefed regularly throughout the development and implementation of the ISG Framework, and is now updated with a progress and status report at each quarterly Board meeting.

The Entrust Board of Directors plays an active role in the ISG process. The wide scope of privacy and security-related regulations represent a significant business risk to most organizations, and the Board should encourage the development and implementation of a comprehensive information security program. The level of risk varies based on numerous factors such as industry, geography and IT environment. The Entrust Board ensures that the level of investment in information security is consistent with organizational strategies and risk profile.

“Entrust is setting the bar regarding Information Security Governance. The ISG quarterly reporting to the Corporate Governance Committee has been an invaluable tool that enables the Board to fully understand potential risks and the activities being pursued to address those risks.”

--Governance Committee Chair, Entrust Board of Directors

3.1.5 The CEO

In the Entrust case, Bill Conner initiated the ISG program, so creating CEO buy-in was not an issue. Mr. Conner is responsible for assigning responsibility for the various functions, overseeing ISG compliance and designating an individual as the senior information security officer (in this case, that responsibility was assigned to the CIO). Finally, the CEO has the responsibility of ensuring that reports to the Board occur on a regular basis, and include a summary of evaluation findings, significant deficiencies and the associated plan of remedial action.

⁹ Standards for Security Categorization of Federal Information and Information Systems, National Institute for Standards and Technology Publication 199, February 2004, <http://csrc.nist.gov/publications/fips/>

"I feel passionately that the road to information security governance goes through corporate governance. Like all governance issues, risk assessment, reporting and accountability are essential, and I take my responsibility for ISG very seriously. ISG has been a critical part of Entrust's risk management and compliance, and it provides me great confidence when reporting to the corporate Board."

--Bill Conner, Entrust Chairman and CEO

3.1.6 Executive Team Members/Business Unit Heads

The executive team members and business unit heads reporting directly to the CEO are responsible for overseeing the organization's security policies and practices. They ensure that information security management processes are integrated with strategic and operational planning processes and that the organization develops and maintains an information security program. The management team must see that security protections are provided commensurate with the risk and magnitude of harm from a potential security breach. They also mandate regular reports from the CIO and their senior managers assessing the effectiveness of the program as well as progress of remedial actions.

"As CFO, I am held personally responsible for compliance with government regulations such as Sarbanes-Oxley. The ISG process has greatly strengthened my confidence regarding Entrust's internal controls, and also that of our auditors. ISG also helps Entrust to make appropriate investment decisions about information security based on risks."

--David Wagner, Entrust Chief Financial Officer

3.1.7 The CIO

Entrust's CIO took the lead in developing and driving Entrust's Information Security Program. Similar to the role of a Quality Officer in a quality program, the CIO drives the initiative and assists the business units in their security efforts. He makes recommendations on where investments should be made, but the business unit management is ultimately responsible for assessment of the risk and the business investment decisions.

The CIO also is a business manager, responsible for the security of the organization's shared infrastructure and applications such as the computer network and e-mail system. In this role, he is responsible for the assessment of risk and magnitude of potential harm of a security failure, and the implementation of appropriate protections.

"The clarification of responsibilities and the quality analogy really helps when security investments are being considered – the business must decide whether the magnitude of the risk warrants the investment, it should not arbitrarily be restricted by the size of the security or IT budget. This doesn't mean they will always make the investment, but the decision is theirs to make, and the ISG process ensures they are involved in the assessment, and the decisions are made relative to the business need."

--Mike Sullivan, Entrust Chief Information Officer

3.1.8 Senior Managers

The head of each organizational unit is responsible for information security of the systems under their control, and the framework recognizes that they will delegate to senior managers in their organization. With the assistance of information security specialists, business unit heads must perform an assessment of risk and implement policies and procedures to reduce information security risks to an acceptable level. Within Entrust, on our third round of the ISG program, seventeen business groups are participating with security risk assessments of their own, and the CIO is merging the results for a company-wide perspective.

"I was pleasantly surprised at how collaborative the ISG process was. It was not the IT group coming in to tell me what to do; my team and I were able to make key decisions about our information security using their guidance. While the process ratified the measures already in place, I definitely understood more clearly the level of risk the group had assumed and could rationally determine whether this was acceptable or whether it required some level of response."

--Greg Wheaton, Director of Customer Operations

3.2 Cycles of Continuous Improvement: Cycle Two

The second review occurred roughly five months later. This was a more extensive review lasting five days and reviewing Entrust's general practices -- what people actually do rather than what the policies say. The key information systems and resources were quickly identified for each business group as part of a general scoping exercise, and a second cycle of ISO element assessment was completed. After the red/yellow/green rankings were merged, eight Red items remained, mostly process concerns.

3.2.1 Lesson #3: Use an Iterative Process With Progressive Detail

By using an iterative process that begins at a high level, the Entrust program did not bog down in excessive detail before delivering some results. With each iteration, the review can address another layer of detail -- this is a model of continuous improvement. As one customer related their experience: "we have to keep telling ourselves not to try to boil the ocean". Begin simply, identifying the largest risks first. The US General Accounting Office (GAO/AIMD 00-33) cites this as a critical success factor:

*"Rather than conducting one large risk assessment covering all of an entity's operations at once, the [best practice] organizations generally conducted a series of narrower assessments on various individual segments of the business. As a result, the scope of each assessment was limited to a particular business unit, system, or facility, or to a logically related set of operations."*¹⁰

¹⁰ "Information Security Risk Assessment: Practices of Leading Organizations", US Government Accounting Office GAO/AIMD-00-33, November 1999, http://www.gao.gov/special_pubs/ai00033.pdf

3.2.2 Lesson #4: Identify key systems

Before you begin an assessment, define the scope of your assessment around the key information systems and resources that are used by the business group to accomplish its mission and objectives. In many organizations, every system is connected in some way to other systems. Without clarifying the scope up front, you may experience confusion during the assessment and participants may have different interpretations. The National Institute of Standards and Technology recognizes this as a critical step and provides some guidance (NIST SP 800-18) in delineating your systems:

“A system is identified by constructing logical boundaries around a set of processes, communications, storage, and related resources. The elements within these boundaries constitute a single system requiring a security plan. Each element of the system must be under the same direct management control, have the same function or mission objective, have essentially the same operating characteristics and security needs, and reside in the same general operating environment.”¹¹

3.3 Cycles of Continuous Improvement: Cycle Three

The third cycle consisted of one or two day reviews with each business group. As with the previous cycles, the team reviewed policy, roles and practices in the group. They started by identifying the business group’s mission and objectives relative to the company’s mission and objectives.

The scope was further refined by identifying the information systems and resources needed to accomplish those objectives. As shown in the example dependency matrix below, each

Function	Network - LAN	Network - WAN	Network - Internet	Network - Remote Access	Telecom - ACD	Telecom - Voice	Computers	Email	Directory Services	ERP	HRIS	Extranet	Development Tools	Legal Files	[...]
Sales	M	L	L	H	H	M	M	M	H	L	M	H	0	0	
Marketing	H	H	M	H	H	H	L	H	H	H	M	H	0	M	
Customer Support	H	L	M	H	H	H	M	H	H	M	H	H	0	0	
Operations	H	L	M	H	H	H	M	H	H	M	0	0	0	H	
Development	H	L	M	M	H	M	M	M	H	M	0	M	H	M	
HR	H	L	H	H	M	H	M	H	H	H	H	H	0	0	
IS/IT	H	H	M	H	H	H	M	H	H	H	H	0	0	L	
Professional Services	M	L	M	L	L	H	L	M	H	M	H	0	H	L	
[...]															

¹¹ NIST Special Publication 800-18: Guide for Developing Security Plans for Information Technology Systems, National Institute for Standards and Technology, Dec 1988, <http://csrc.nist.gov/publications/nistpubs/800-18/Planguide.PDF>

business unit was asked to rate the impact of a failure in Confidentiality, Integrity or Availability for each system. Their key resources were defined as those rated “high”, where the business unit would be seriously impacted by a security failure of the system.

The CIO consolidates the assessments and delivers the summary to the executive management team, along with an assessment of effectiveness of the overall program.

3.3.1 Lesson #5: Communicating Risk

There are a number of methods to describe risk, but since management must make decisions with the information, it is best to keep the description in a plain sentence format that will be readily understood.

Vulnerability x Threat x Impact

Example: “Inconsistent account disabling procedures [**vulnerability**] could allow a disgruntled ex-employee access to confidential information that could be deleted, modified or stolen [**threat**] resulting in lost productivity, erroneous reporting or loss of intellectual property [**impact**].”

Expressing risk using this method makes it easy for the stakeholders to understand and the business impact of the risk can be readily assessed. A numerical or other scale approach requires interpretation, making it less intuitive for business management to determining acceptable risk levels.

3.3.2 Lesson #6: Maintain a Transparent Process

Each independent organizational unit should assess, remediate, and report on its information security program. Additionally and where appropriate, each year an independent information security program evaluation should be completed in accordance with generally accepted auditing standards and the results reported to the Board of Directors/Trustees. That independent view is critical for a truly transparent governance process, as confirmed in the US General Accounting office guidance (GAO/AIMD 98-68):

“The ability to independently voice security concerns to senior executives was viewed as important because such concerns could often be at odds with business managers’ and system developers’ desires to implement new computer applications quickly and avoid controls that would impede efficiency, user friendliness, and convenience. This ability to elevate significant security concerns to higher management levels helped ensure that risks were thoroughly understood and that decisions as to whether such risks should be tolerated were carefully considered before final decisions were made.”¹²

¹² “Information Security Management”, US General Accounting Office GAO/AIMD-98-68, May 1998, <http://www.gao.gov/archive/1998/ai98068.pdf>

3.3.3 Lesson #7: Create a Concise Board Summary Report

For effective reporting to executives and the Board of Directors, a summary description backed by detailed action plans is most effective. The key is to present information in a clear and simple way, yet convey the structure and comprehensiveness of the work performed.

Information Security Summary			
Security Practices	Risk Level*		
<i>(based on ISO 17799 chapters)</i>	R	Y	G
Security Policy	0	1	1
Organizational Security	1	3	1
Asset Classification & Control	1	0	2
Personnel Security	1	4	4
Physical & Environmental Security	2	4	12
Communications & Operations Mgmt	2	10	20
Access Control	4	12	14
Systems Development & Maintenance	0	2	11
Business Continuity Management	1	2	2
Compliance	2	5	3
TOTAL <i>(*sample numbers only)</i>	14	43	70

As shown in the introduction, the Entrust Board report is presented in the above table. This summary represents the roll-up of the detailed chart shown on page 7. Each chapter heading from the ISO 17799 best practices is shown with the assessment total count of red, yellow and green items from that chapter. This format enables the executives or the Board to quickly assess risk levels in the major topic areas, recognize the structure behind the assessment, and monitor improvements across reporting periods. Additional materials are also provided, outlining remedial action, updates from previous periods, and an indication of the level of risk accepted by the business.

3.4 Next Steps

Having developed and applied the ISG methodology internally, Entrust continues to work with various associations, corporations, government agencies and working groups to see that ISG is widely embraced.

Entrust also continues to implement and refine an internal ISG process including quarterly Board of Directors reporting, business unit risk analysis and remediation, and employee awareness and training. The efficiency, cost and security benefits from Entrust's ISG program have been significant and are expected to continue to accrue into the future.

4 Benefits of Implementing the ISG Framework

The benefits derived by organizations that implement the ISG framework go beyond facilitating compliance with applicable legislative, regulatory and contractual requirements. ISG and its associated information security program also result in tangible business benefits, including:

- **Improved internal processes and controls:** Authentication, authorization and auditability of the people, devices and applications on the network improve efficiency and effectiveness of business processes.
- **Potential for lower audit and insurance costs:** Better governance and the ability to demonstrate an auditable, complete ISG program can result in lower insurance costs and decreased audit costs.
- **Market differentiation through a continuous improvement process:** Industry first resisted quality-improvement processes as added cost, but soon evolved to embrace it as a method for improving productivity and customer loyalty. Ultimately, quality became a market differentiator. Over time, an ISG program may also provide results that help determine a market leader.
- **Self-governance as a better alternative than regulation:** Implementation of an industry-led solution based on open standards and best practices will help mitigate the requirement for new governmental regulation. Should new legislation emerge, organizations that have invested in an ISG program are likely to benefit.

Laws and Regulations Related to Information Security

- US Sarbanes-Oxley Act
- US Health Insurance Portability and Accountability Act (HIPAA)
- US Gramm-Leach-Bliley Act (GLBA)
- US Federal Information Security Management Act (FISMA)
- Canadian Personal Information Protection and Electronic Documents Act (PIPEDA)
- EU Directive on Data Protection (EU Data Directive)
- California Security Breach Information Act (SB1386)

Through implementation of the ISG framework, Entrust was able to capitalize on many of these benefits. The improved business processes resulted in greater operational efficiency in many cases, and the resources expended toward compliance with a variety of regulations, including Sarbanes-Oxley was considerably reduced. Adoption of ISG also resulted in positive impact on the bottom line from lower insurance costs and lower auditing costs.

5 About Entrust

Entrust, Inc. is a world-leading provider of Identity and Access Management solutions. Entrust software enables enterprises and governments to extend their business reach to customers, partners and employees. Entrust's solutions for secure identity management, secure messaging and secure data increase productivity and improve extended relationships by transforming the way transactions are done online.

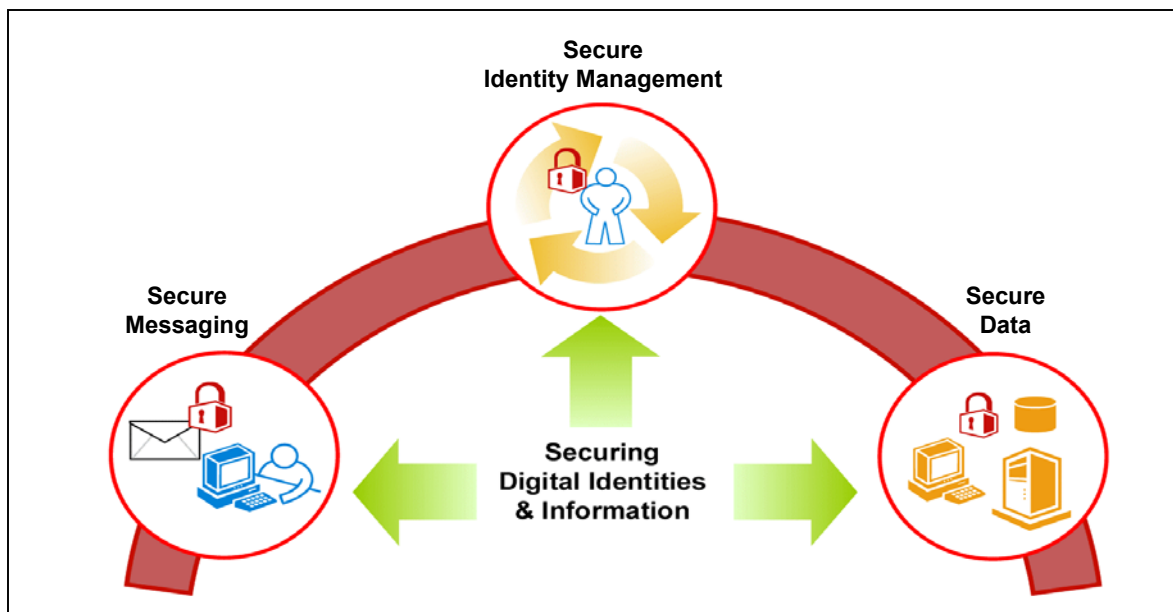
5.1 Entrust Customers

Over 1250 major government agencies, financial institutions, governments and Global 1500 enterprises in more than 50 countries have purchased and deployed the Entrust secure messaging, secure data and secure identity management software solutions that integrate into the broad range of applications organizations use today to leverage Internet and enterprise applications to improve productivity. More than 50 percent of the Fortune 100 are Entrust customers or partners. With an aggregate of over 100 patents and patents pending, Entrust takes the initiative in authoring and driving industry standards boards and technology forums.

Entrust has a long and distinguished list of customers who are market leaders in their respective industries. These companies, many with large scale deployments, are realizing value by using our solutions to extend their enterprises, protect their transactions and facilitate compliance with applicable laws and regulations.

<p>Healthcare</p> <ul style="list-style-type: none"> • Merck • Novartis International • GlaxoSmithKline • Kaiser Permanente • Blue Cross Blue Shield MI • Baptist Health Systems • UK National Health Service ... and over 50 more 	<p>Government</p> <ul style="list-style-type: none"> • US Dept. of Homeland Security • US Dept. of Energy • US Dept. of State • Govt. of Canada • HM Customs & Excise (UK) • Danish Government • Spanish Mint ... and over 300 more
<p>Financial Services</p> <ul style="list-style-type: none"> • Citibank • Capital One • JP Morgan Chase • Prudential • Egg Bank • Lloyds TSB • Credit Suisse ... and over 150 more 	<p>Large Enterprise</p> <ul style="list-style-type: none"> • Cox Communications • Delta Airlines • Hughes Network Systems • Lowe's Home Centers • Vodafone • Verizon • 3 (formerly H3G) ... and over 700 more

5.2 Entrust Solutions



Entrust Secure Identity Management Solution

Organizations today need to extend access to corporate resources to an ever-growing number of employees, partners, suppliers and customers. Effectively managing the increasing number of users is a significant challenge in itself, adding to this challenge is the complexity of delivering access to enterprise resources in multiple ways such as client-server, Web and Web Services applications.

Further adding to the challenge is the increasing number of Web Services applications and network devices required for the deployment and management of identities in an accountable and auditable manner. Enterprises and governments are also faced with intense pressure for increased accountability, driven by legislation as well as shareholder demands for more effective corporate governance. The dramatic rise in information and identity theft further underlines the need for a secure identity management solution. More effective internal controls, including the use of strong authentication, authorization and single sign-on (SSO), and centralized provisioning, can help organizations to comply with critical pieces of legislation such as Sarbanes-Oxley while at the same time realizing business benefits like cost reductions and increased levels of service.

The Entrust Secure Identity Management Solution consists of a suite of market-leading identity and access management products, which, in combination or deployed in modular stages, help organizations easily manage identities and access to information while decreasing costs. It can also improve the ability of organizations to enable legislative and corporate governance compliance. Supporting a broad range of client-server, Web and Web Services environments, the solution enables organizations to lower the costs associated with deploying and managing user, application and device identities while making it easier to securely access applications and information over the Internet. Through best-of-breed capabilities, the solution is easy to deploy and operate, includes secure administration, and cost-effectively scales to address large user populations.

Entrust Secure Data Solution

Applications such as enterprise resource planning, supply chain management, customer relationship management, workflow and e-forms have been migrated online to improve productivity and reduce paper costs and overheads. However, many organizations use only basic security solutions, such as a password, to secure these applications—a level of security that is inadequate for sensitive business information. Furthermore, enterprises are typically not securing the sensitive information in files and folders stored on desktops, laptops, enterprise servers or other electronic devices. This information is often left open to theft by insider and outside attackers. This lack of protection for sensitive information is resulting in identity theft attacks and the compromise of other types of sensitive information, including strategic business plans and customer information.

The Entrust Secure Data Solution consists of a comprehensive, highly scalable suite of data security products and services that help organizations mitigate the risk of data loss, corruption and disclosure so they can confidently capitalize on new technologies that enable greater stakeholder collaboration and, ultimately, business growth. It helps organizations secure sensitive and valuable information stored on computers, mobile devices, and corporate networks. The solution can also be a useful tool to help organizations meet their obligations under new legislative regulations that mandate stronger data security controls, without unduly burdening the people and processes that make use of this critical data.

Organizations can realize the promise of secure data through encryption that provides end-to-end data protection and privacy; through authentication, which strongly identifies the requesting users, device or application before releasing sensitive data; through policy-based access control, which manages individual user access rights to data and applications based on corporate policy; and through digital signatures which improves accountability for data transactions and protects the integrity of data involved in a transaction. Many organizations also provide data integrity through secure file transfer.

Entrust Secure Messaging Solution

E-mail has become the number one productivity tool for organizations, offering a low cost way to share information and accelerate decision-making. E-mail is fast and convenient, but not without inherent risks. In order to mitigate the risks of communicating valuable information, organizations need to secure sensitive e-mails. Unauthorized access to client records, sales forecasts, intellectual property or other valuable information can do significant damage to an organization's brand and competitive position. And with recent government regulations such as Sarbanes-Oxley, HIPAA, GLB and California SB 1386, the need to secure e-mail communications becomes an important element of regulatory compliance.

By transparently adding "end-to-end" security to e-mail applications such as Microsoft Outlook and Lotus Notes, the Entrust Secure Messaging Solution may help mitigate risk and comply with government regulations regarding sensitive e-mail communications.

The Entrust Secure Messaging Solution contains the following key attributes:

- ▶ Seamlessly adds security to popular e-mail software programs; turning them into more secure communications vehicles;
- ▶ Offers flexible, standards-based options for secure communication with employees, partners and customers;

- ▶ Transparently manages security on behalf of the user to make it easy to send and receive secure e-mail;
- ▶ Delivers enhanced security that provides encryption and digital signature technology;
- ▶ Allows users to identify senders and recipients of e-mail communications with greater confidence;
- ▶ Verifies the integrity of message content and protects the privacy and confidentiality; and
- ▶ Capitalizes on mobile communications by extending security to Blackberry wireless handhelds.