

CUSTOMER TYPE:

Professional Services firm

THE CUSTOMER:

Customer is a leading provider of professional technology services to government, education and mid-market commercial customers in the largest IT markets nationwide.

Customer provides a broad range of solutions that address the critical business needs of organizations today, such as IT security, voice and data convergence (VOIP), enterprise access and technology management.

Customer helps organizations reduce the complexity of their environments by delivering cohesive solutions that make information more secure, accessible and manageable today, with the extensibility and built-in functionality to meet future growth and development.

Based on customer's reputation of being a leading provider of professional technology services and IT security solutions; the State of Florida Technology Office awarded customer a contract to provide comprehensive risk assessments for state agencies. The initial contract term is two years, with an additional one-year renewal option.

Through a competitive bid process involving several national security firms, this customer was one of only two contractors selected to provide these comprehensive risk assessments to government agencies throughout Florida State.

Each state government agency is mandated to conduct assessments from a pre-qualified contractor in order to identify security threats to data and information technology resources.

THE CHALLENGE:

Customer required a cost-effective, repeatable and easy to use automated tool that will facilitate the successful completion of each assessment in less than 5 days per agency in a consistent manner with uniform reporting capabilities, and also integrate well with the Octave Methodology being used to perform the initial high-level risk assessments. The tool selected was required to assess each agencies environment against the internationally accepted information security management best practices specified in ISO/IEC 17799:2005, as well as US centric regulatory compliance requirements such as NIST 800-53 (FIPS 200), HIPAA Security and California SB-1386 etc.

THE SOLUTION:

eFortresses Compliantz tool allows consultants, Information security staff and Auditors to measure an organization's security and compliance posture by providing a report on where an organization is non-compliant to internationally accepted Information Security Management best practices specified in ISO/IEC 17799:2000, ISO/IEC 17799:2005 and ISO/IEC 27001:2005 plus applicable regulatory compliance requirements such as HIPAA Security, GLB Act, Sarbanes-Oxley Act (SOX), California SB-1386, PCI Data Security Standard (Visa CISP), FACT Act, NIST 800-53 (FIPS 200), together with detailed recommendations and a clear roadmap on how to improve their security posture and become compliant with best practices and regulatory compliance requirements.

Compliantz uses automation to "crunch" responses from the security assessment and compare them with best practices and applicable regulatory compliance requirements before producing Executive Dashboards and detailed reports which consists of pictorial representations in the form of bar and pie charts as well as a detailed risk mitigation plan to improve the security posture over time.

A very brief demo of the eFortresses Compliantz tool to this customer's Chief Security Officer (CSO) was enough to demonstrate the intrinsic value of the tool and ensure immediate product selection.



THE RESULT:

Considering the limited timeline associated with the delivery of the agency assessments, customer decided to go ahead and use the eFortresses Compliantz tool to perform a preliminary security assessment for one of the Florida state government agencies; the immediate feedback received from this agency was excellent and almost immediately customer made the decision to procure additional licenses to perform assessment for up to 24 Florida state government agencies, over a six month period. This resulted in 24 completed assessments within a period of 6 months, thereby achieving tremendous savings in cost and time plus customer satisfaction.

CUSTOMER TYPE:

Professional Services firm

THE CUSTOMER:

Customer delivers professional services in the areas of internal audit, technology risk management, tax, finance and accounting. Customer serves clients, including more than half the Fortune 500, through highly experienced, salaried professionals working from offices across North America and Europe.

Customer technology risk management professionals are formally trained in information security, IT audit and compliance, and business continuity approaches. Customer focus on information security assessment and controls relating to information technology environments, and are experts at eliminating or minimizing the impact of unplanned interruptions and ensuring the continuity of critical business services.

THE CHALLENGE:

Customer saw the need to send all it's professionals on a cost-effective training and certification program that will empower them to gain a more holistic view of Information Security & Regulatory compliance beyond Sarbanes-Oxley Act (SOX) and also empower them to assist clients in building a more sustainable information security & compliance programs, based on best practices of ISO/IEC 17799, COBIT, COSO, ITIL and be able to map these standards to multiple regulations.

THE SOLUTION:

eFortresses - Holistic Information Security Practitioner (HISP) certification course:

This course has been endorsed by ISSA (Information Systems Security Association) and ISACA (Information Systems Audit and Control Association) this class earns 35 CPEs for each attendee. This is the only class available today that provides practical education in best practices for Information Security Management, Information Systems Auditing and multiple Regulatory Compliance requirements and how to map multiple regulatory requirements to the internationally accepted best practices framework of ISO/IEC 17799. The class covers ISO/IEC 17799:2005, COBIT, COSO and ITIL then explains a methodology to map regulations such as Sarbanes-Oxley Act, HIPAA Security, GLB Act, California SB-1386, FISMA (NIST 800-53), FACT Act, Visa CISP/PCI to the ISO/IEC 17799:2005 framework.

Attendees will gain the knowledge to help their companies or clients implement processes, procedures and policies, for a solid information security program and compliance with applicable regulations.

THE RESULT:

Customer's sent a total of 12 Professionals from its Atlanta office in batches of 2-5 to eFortresses public HISP classes throughout 2005. Most of these professionals were very excited about the prospect of being "sponsored" to learn new skills and to be paid for downtime away for projects, for continuous professional development and skills enhancement.

Each professionals' enthusiasm and value derived from the HISP class resulted in these professionals being able to almost immediately provide additional value to clients.

Each professional is now looking forward to completing the HISP Certification process.

CUSTOMER TYPE:

Financial and Insurance Services

THE CUSTOMER:

Customer is a US Fortune 500 organization and is ranked the 4th largest financial services organization in the world.

Customer's businesses in the United States offer individual, business and institutional customers innovative financial products and services in insurance, investment, asset management and Internet banking.

Customer's U.S. Financial Services and Investment Management Group comprise the operating units of Insurance - which also encompasses businesses in Canada and Latin America. Customer's provides retail and institutional clients with products and services in retirement services, annuities, life insurance, employee benefits, mutual funds, financial planning, reinsurance and institutional markets. Customer has over 200,000 financial professionals in the U.S, holds top 10 rankings in its major product lines and has 14 million customers in the US.

THE CHALLENGE:

In 2002, customer was mandated by its European head office to adopt policies based on ISO/IEC 17799 and has made commendable efforts over the years to publish and enforce these policies at its business unit level, by appointing Business Security Officers with oversight and implementation responsibilities.

Customer saw the need to provide in-house training session to its Business Security Officers that will empower them to gain a more holistic view of Information Security & Regulatory compliance beyond Sarbanes-Oxley Act (SOX), help them understand the "why" behind it's enterprise security program and also empower them in building a more sustainable information security & compliance programs, based on best practices of ISO/IEC 17799, COBIT, COSO and map these standards to multiple regulations, particularly Sarbanes-Oxley Act requirements.

THE SOLUTION:

eFortresses - Holistic Information Security Practitioner (HISP) certification course:

This course has been endorsed by ISSA (Information Systems Security Association) and ISACA (Information Systems Audit and Control Association) this class earns 35 CPEs for each attendee. This is the only class available today that provides practical education in best practices for Information Security Management, Information Systems Auditing and multiple Regulatory Compliance requirements and how to map multiple regulatory requirements to the internationally accepted best practices framework of ISO/IEC 17799. The class covers ISO/IEC 17799:2005, COBIT and COSO then explains a methodology to map regulations such as Sarbanes-Oxley Act, HIPAA Security, GLB Act, California SB-1386, FISMA (NIST 800-53), FACT Act, Visa CISP/PCI to the ISO/IEC 17799:2005 framework.

Attendees will gain the knowledge to help their companies or clients implement processes, procedures and policies, for a solid information security program and compliance with applicable regulations.

THE RESULT:

Our in-house HISP training class delivered to this customer involved over 25 Security Officers, consisting of ISOs, CSO and Business security officers. In addition to the knowledge imparted to these security officers, our HISP training class also stimulated brainstorming on internal security issues and fostered communications, and also served as an effective information security forum. The feedback received from the officers clearly indicated that the class enabled them to now understand the "why" behind the company's enterprise security program and made them more committed to their enterprise security program.