



## Risk Mitigation Policy Management

### *Policy Exception Process Support & Compliance Tool Development*

<b>Client:</b>	Fortune 100 Corporation (Worldwide INFOSEC Headquarters)
<b>Project:</b>	Risk Mitigation Policy Management
<b>Industry:</b>	Healthcare
<b>Solution Focus:</b>	Manage the Policy Exception Process develop Compliance Measurement Tool
<b>Technologies:</b>	MS Office Tools and Web Form Technology

---

#### **Executive Summary**

The Director of Information Security for a Fortune 100 International Healthcare Company requested our services to manage the Enterprise's Worldwide Information Security Policies. Our services included managing the following key responsibilities: Develop, implement and manage the on-going security policy exception process when a particular operating unit of the enterprise could not immediately comply with a specific policy requirement. Ensure that the Information Security intra-net portal is kept up-to-date with all relevant information and compliance tools. Provide additional expertise to develop self-assessment (compliance with policies) tools in order to provide the operating units a methodology and proven techniques to measure their individual company's security policy compliance.

#### **Business Situation**

The client has over 190 operating units who are managed autonomously. Sizes of the operating units ranged from very small (e.g. one location with one product line) to very large units with multiple global locations and products. Since there were significant proprietary pieces of information that support each operating unit, extreme sensitivity and awareness was enforced to protect all Business Critical Information.

#### **Solution**

Churchill & Harriman's proven experience and approach to provide this level of service can be characterized in the following major segments of this relationship:

- ◆ **Organizational Discovery:** Quickly learn the corporate structure and how it supports each Operating Unit. Determine the long-term goals of the Worldwide Information Security team and how they were reflected in the current Information Security Policies. Learn and understand the rationale for "approving" policy compliance exceptions.
- ◆ **Policy Management Support:** The Information Security policies were extremely detailed in their composition and stringent control techniques were required to manage the update and modification process. It was obligatory that all policy updates and modifications be reviewed and approved by key Worldwide Information Security individuals and, as appropriate, other key technical resources within the corporate organization. All policy changes were accomplished via an evolutionary process with each step rigorously controlled.

- ◆ **Policy Exception Process:** There were potentially over 200 sources of policy exceptions (e.g. Operating Units). The key objective was to ensure each exception was properly documented with the authorized approvals (at the Operating Unit level) before submission to Worldwide Information Security. Each incoming exception required a detailed review to ensure all critical questions were duly addressed. Our consultants formulated a recommendation (i.e. approve or disapprove) based on their own expertise and access to the Policy Exception database. It was required that individual Exceptions be duly tracked for anticipated future compliance and that any commonalities amongst other approved Exceptions be communicated to Worldwide Information Security prior to final processing.
- ◆ **Compliance (Self-Assessment) Tool:** Our analysis and development effort resulted in a business model that provided a methodology to yield detailed metrics related to an individual Operating Unit's compliance to the security policies. Three approaches were provided: *Site*, *Platform* and *Application*. Operating Unit's can utilize one or all three self-assessment approaches at various times during a calendar year. The results of these self-assessments were key to Worldwide INFOSEC and the Enterprise level CIO to determine the level of risk related to protecting the Enterprise's vast catalog of Business Critical Information.

### **Conclusion**

Churchill & Harriman was able to provide the valuable expertise needed to assist the client in making certain choices on approach, methodologies and anticipated utilization of the various services and tools WWIS is responsible to provide to the entire Enterprise.