Information Technology - Governance, Risk Management and Compliance (IT-GRC)

Course Title	Project Management
Course Number	ETM 545
Instructor	Mr. Jeffrey Busch
Term	Winter
Year	2011
Author(s)	Claudiu Rusnac

Project Disclosure

This project plan review is based upon an actual project done at a Fortune 500 corporation. I was involved as a subject matter expert in this particular project. Certain details were excluded to maintain confidentiality of the subject matter and not to reveal any confidential information regarding the specific implementation of the IT-GRC tool. The project was ~40% complete when this report was written.

Some of the details of this report are based upon subject matter expertise and implementation details.

This is to certify that I have completed this exam as an individual effort without seeking any form of assistance from others

1. Project Overview

1.1. Project Background

Managing Information Technology (IT) risk within large organization with disparate groups/business-units is a difficult task and presents many challenges. Ineffective risk management can expose the business to vulnerabilities, which result in fines, business loss, and possible the organizations brand recognition. By deploying an enterprise wide Information Technology Governance Risk and Compliance (IT- GRC) tool, organizations have the ability to identify, mitigate, and accept and manage risk to a reasonable level. Mandated by the Sarbanes-Oxley act of 2002, public traded corporations must implement internal security controls to sufficiently protect financial data. [1]

An IT-GRC [2] tool provides a central repository where individuals, at different levels within the organization, can disposition, address, and accept risk. By doing so, the organization can document and properly assesses its risk posture from an Information Technology (IT) system perspective.

1.2. Project Selection

The Information Risk Management (IRM) team manages a compliance program named: Information Security Risk Assessment (ISRA). This program is setup to identify information system assets and resources (electronic information systems), evaluating vulnerabilities / threats, identifying the risks and probable impacts, and analyzing the cost effectiveness of measures taken to reduce these identified risks. The IT-GRC tool is the centralized repository for completing this process.

Several years back a tool was developed in house to automate the ISRA process because the market for security tools was emerging, but none were mature enough to encompass the entire process. After using a custom developed tool for many years, the developers were not able to keep up on the requirements and expand the tool capabilities fast enough to keep up with the business demand and requirements.

A decision was made to transition off the custom build solution to a commercial off-the shelf (COTS) application. A core team was formed to select and implement an industry-best IT-GRC solution.

1.3. Project Goals and Objectives

This project focused on deploying an enterprise IT-GRC program that involved groups throughout several geographies and many different business units.

1.4. Business Requirements

- An access-controlled and metrics dashboard where corporate risk analysts and IT-security business unit liaisons can access and maintain policies, risk

assessments, task management/workflow, and other information they need to perform various risk and compliance functions within the organization.

- A comprehensive policy management solution that would enable the organization to centrally manage policies and map them to objectives and guidelines.
- A centralized compliance management solution that would enable the organization to document the control framework, assess design and operational effectiveness, and respond to policy and regulatory compliance issues. The solution should also help to identify risks to the business, evaluate them through online assessments and metrics, and respond with remediation or acceptance.
- A flexible solution that would enable the organization to manage relationships and dependencies within the enterprise hierarchy and infrastructure to support GRC initiatives.
- Reporting capabilities that will allow management to view enterprise reports that provide an overview of risk.
- Integration into operating system vulnerability data, operating system compliance data and web application vulnerability data. Results from these tools will be populated in the GRC tool to provide risk metrics, track remediation, reports and dashboard and measure results against the organizations policies and control procedures.

2. Terms and Definitions

See Appendix 9.1

3. Project Management

Project management within this organization is centrally managed from a coherence and structural perspective. The Project Management Office (PMO) defines the project methodology framework that the project managers use a basis to document and create a repeatable process.

The methodology defines a configurable set of tasks and deliverables that must be completed over the life cycle of a project. This methodology provides the set of deliverables that allows management to make informed business and technical decisions during the life of the project. The process, a series of phases, with core elements implemented in a repeatable way, to consistently produce predictable results.

The project manager is a member of the functional team, but uses tools and coaching from the PMO. The PMO provided a chairperson to the project to shadow the project documentation and validate that proper adherence to the defined methodologies. This is usually done because other business stakeholders need to sign-off during the phase gates.

The project manger for the IT-GRC deployment was selected because of his credentials. He was brought on as a contract resource to the project. The project manager is PMI certified and understands project management in an IT context. This particular resource has done many projects in the IT space at this particular company.

The project manager does not have formal authority to make project decisions. He participates more as a project resource. The functional manager owns all the resources (people/money) and has direct responsibility to see the project to completion. On this particular project, the project manager is responsible for: creating the schedule, validating that all resources line-up appropriately, scheduling meetings, and sending out project status.

4. Project Organization

The Information Risk Management (IRM) organization, which owns this project, has many extended business partners that are used as extend team members and stakeholders. Senior management within the IRM organization provides direction and work with other functional manager to get buy-in for the project. This is critical piece as they provide valuable input to the business requirements.

The IT-GRC tool deployment is sponsored at the IRM senior management level but has many stakeholders within other business units. The organizational structure of the project is matrix style. There are many (50+) extended team members. These team members are responsible to communicate to their functional managers and communicate status to their respective organizations outside of IRM. The organization of the project can visually be seen in Figure 4-1.

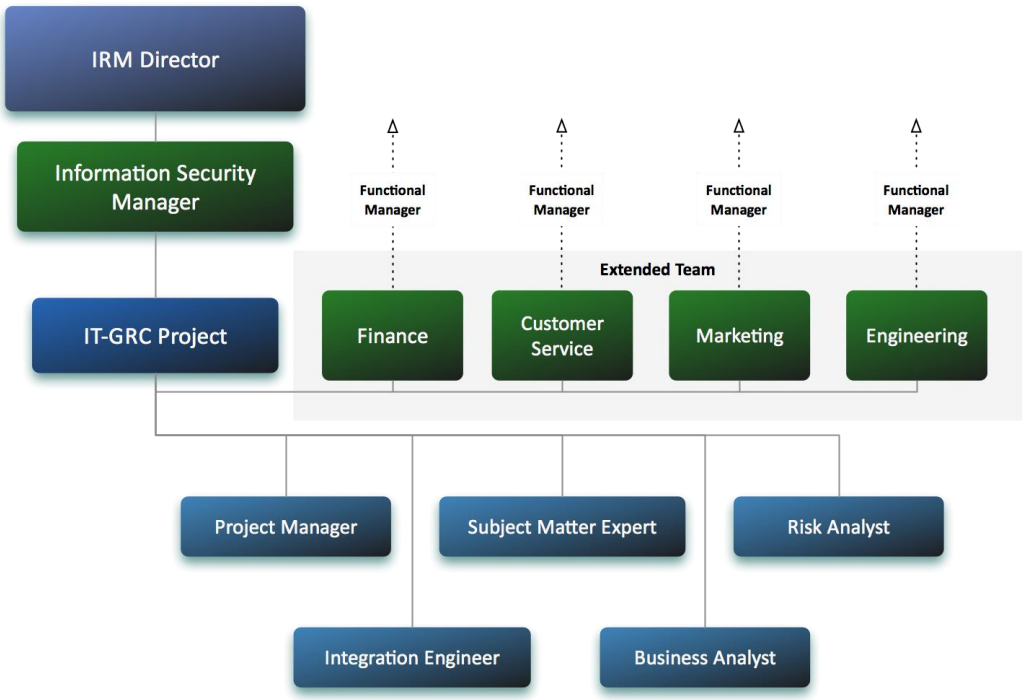

Figure 4-2 – Project Organization Structure - Matrix Structure

5. Scheduling & Cost

The project schedule was developed and maintained by the project manager with input from the functional manager who manages the resources. Identifying tasks and associating them with the time required to complete the respective task was used to produce the schedule. By compiling the task list and total hours, the schedule was built. The project completion date was derived by total hours. Certain tasks were combined and resources were shifted to provide more even workload. Figure 5-1 shows a high-level schedule that outlines the milestones required to complete the project.

Microsoft Project was used to create the schedule and assign resources to the various tasks. The schedule provided insight in resource constraints. Certain team members were over allocated for some tasks. By using MS project, the project manger was able to re-assign tasks or spread out the timeline to alleviate resource contention.

Weekly core team meeting are held to review the schedule and determine whether tasks are on schedule. The schedule was re-adjusted based upon team member feedback. In some cases where tasks were overdue, the project manger would adjust the timeline to retrofit any adjusted time needed. In certain scenarios some project tasks were shortened to account for additional time on other tasks.

5.1. Project Timeline

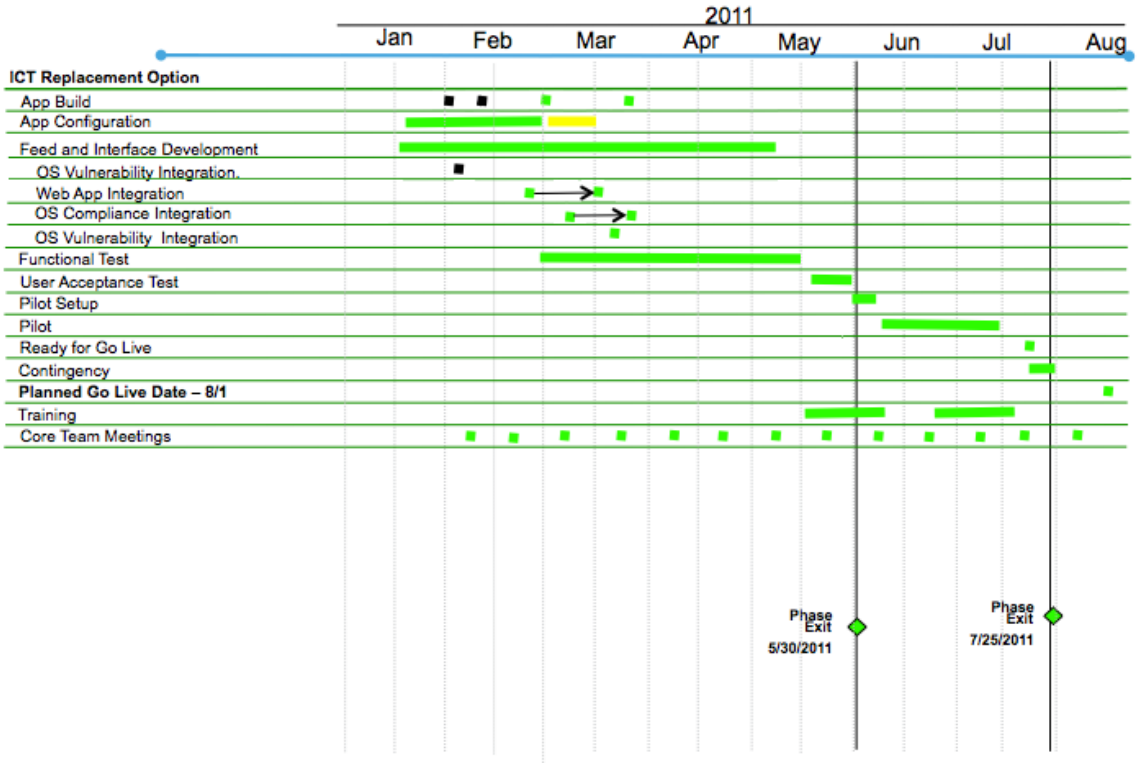

Figure 5-2 – Project Timeline

5.2. Project Costs

The only documented or tracked costs were from the software purchase. This was a one-time cost of ~$220,000 with an annual 22% (~$49,000) maintenance/support contract. The allocated budget was part of an investment fund that was prioritized in the prior year to be spent on operational efficiencies. The support contract become a line item in the IRM sustain budget.

All the people resources assigned to this project were all internal salaried employees. Since employees do not track their time, tracking overruns in the project costs was difficult.

6. Work Breakdown Structure

The work breakdown structure (WBS) was developed as a team. This task was done simultaneously with the creation of schedule. The project manager facilitated several sessions with different team members to identify the tasks/hours required to complete each task/subtasks.

Even though a traditional WBS wasn't created during the project, a task list was created and outlined in the schedule. Below (Figure 6-1) is a partial WBS that was created for a particular task (data integration.)

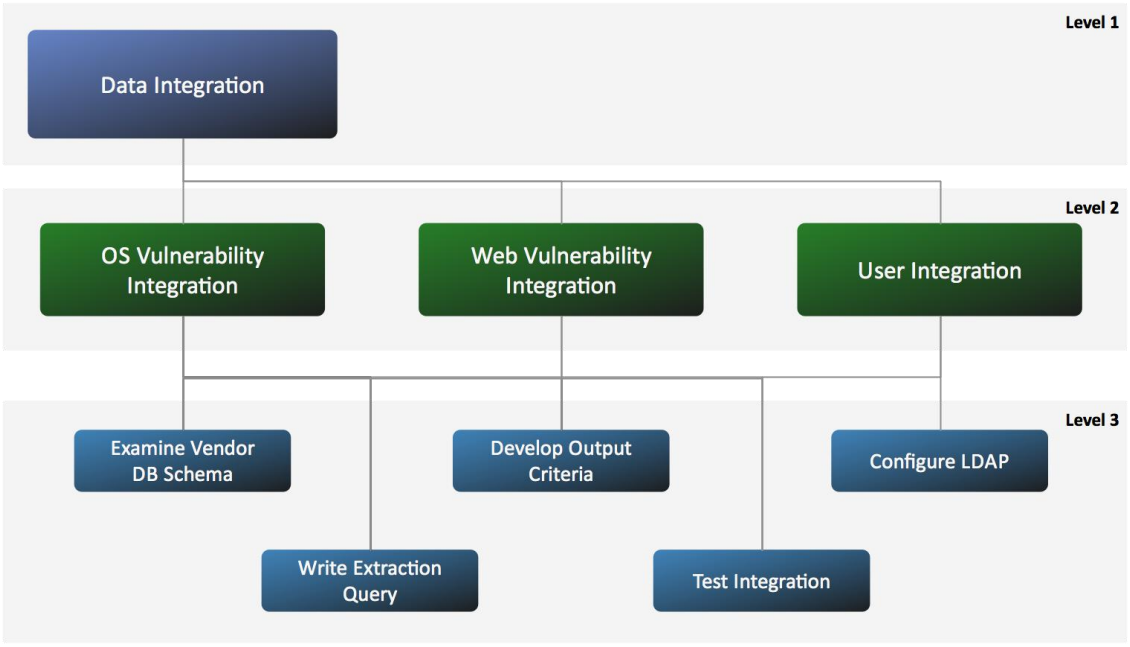

Figure 6-2- Partial Work Breakdown Structure

7. Responsibility Matrix

The project team developed a responsibility matrix during the initial phase of the project. The extended responsibility matrix had individual names assigned to each role.

Role	Responsibility
Project Manager	**The Project Manager is responsible for directing, controls, administering, and regulating a project. The project manager ensures that the scope, schedule, cost and project success factors are met.** ▪ Responsible that all aspects of the project have been assigned and performed. ▪ Ensures that the direction of the project continues to be in line with the original mission and goals. ▪ Holds team member accountable for following project standards and methodologies ▪ Communicates with project sponsors and stakeholders and extended team members. ▪ Reports project status to project sponsors and stakeholders. ▪ Manages project schedule in accordance with each phase. ▪ Coordinates efforts of project contributors, communicates expectations to team members. ▪ Identifies and facilitates project issues – escalating when necessary. ▪ Responsible for managing to project priorities constantly performing project risk assessment and control. ▪ Ensures that project resources are utilized properly to meet scope and timelines. ▪ Follows project methodology standards.

Subject Matter Expert	**The Subject Matter Expert is responsible to providing his or her expertise on technical aspects of the project. Work with the vendor and core team to identify and resolve technical problems.** ▪ Provide technical direction to the core team. ▪ Evaluate and propose technical solutions to simplify process flow within the context of the application and it's interfaces. ▪ Act as a consultant for integration of existing technical installations. ▪ Identifies project issues. ▪ Identifies project risks. ▪ Provides additional services/skills as needed for project.
Risk Analyst	**The Risk Analysts is responsible for maintaining continuity of all internal and corporate polices.** ▪ Translate workflow processes with internal auditable processes. ▪ Work with technical team to identify process improvements and document as auditable process. ▪ Review all audit questionnaires in the new IT-GRC tool. ▪ Identifies project issues. ▪ Identifies project risks. ▪ Provides additional services/skills as needed for project.
Integration Engineer	**The Integration Engineer is the primary focal point for all integration tasks associated with all data feeds.** ▪ Provide technical expertise on integration of all data feeds. ▪ Provides input to product design and workflow processes. ▪ Provides technical guidance and review of project deliverables. ▪ Work with data feed vendors to provide best practice integration. ▪ Identifies project issues. ▪ Identifies project risks. ▪ Provides additional services/skills as needed for project.

Business Analyst	**The Business Analyst's primary function is to translate business workflow processes into technical requirements.** ▪ Work with extended stakeholders to document existing and improved business processes. ▪ Communicate with extended team. ▪ Provide ▪ Identify and communicate project issues and risks. ▪ Performs project tasks as according to project need and as directed by the project schedule. ▪ Provide technical knowledge to the development of the project output. ▪ Attend project meetings and provide project status reports. ▪ Identifies project issues. ▪ Identifies project risks.

8. Project Conclusions

8.1. Project Observations

As mentioned in the project disclosure sections, this project was ~40% complete when this report was written. Some so the questions regarding project completion still need to be determined and could not be answered. Due to the structure nature of the project, certain closure phases still need to be executed once the project is completed.

The primary motivator for the project team was operational efficiency. Since the project team ran the ISRA program for the entire organization on a daily basis, implementing a COTS IT-GRC tool provided workflow efficiencies.

8.2. Strengths

The team was cohesive and worked well together. Since most of the team members were also part of the same functional team, the team worked well. The functional managers managed team conflicts a well.

8.3. Weaknesses

The project manager was a contracted resource that was not part of the tea during the entire course of the project. The project manger was brought in as contract resource to alleviate resource contention to the existing project manger. The cohesion of the project team hit a roadblock when the project manager was changed out during the course of the project.

9. Appendix

9.1. Terms and Definitions

Term	Definition
Enterprise Risk Management [3]	Enterprise risk management (ERM) is the process of planning, organizing, leading, and controlling the activities of an organization in order to minimize the effects of risk on an organization's capital and earnings. Enterprise risk management expands the process to include not just risks associated with accidental losses, but also financial, strategic, operational, and other risks.
COTS [4]	A COTS (commercial off-the-shelf) product is one that is used "as-is." COTS products are designed to be easily installed and to interoperate with existing system components. Almost all software bought by the average computer user fits into the COTS category: operating systems, office product suites, word processing, and e-mail programs are among the myriad examples. One of the major advantages of COTS software, which is mass-produced, is its relatively low cost.
GRC [2]	GRC (governance, risk management and compliance) software allows publicly held companies to integrate and manage IT operations that are subject to regulation. Such software typically combines applications that manage the core functions of GRC into a single integrated package.

Reference

[1] “How the SEC Protects Investors, Maintains Market Integrity.” [Online]. Available: http://www.sec.gov/about/laws.shtml#sox2002. [Accessed: 07-Mar-2011].

[2] “What is GRC (governance, risk management and compliance) software? - Definition from Whatis.com.” [Online]. Available: http://searchcio.techtarget.com/definition/GRC-governance-risk-management-and-compliance-software. [Accessed: 08-Mar-2011].

[3] “What is enterprise risk management (ERM)? - Definition from Whatis.com.” [Online]. Available: http://searchcio.techtarget.com/definition/enterprise-risk-management. [Accessed: 10-Mar-2011].

[4] “What is COTS, MOTS, GOTS, and NOTS? - Definition from Whatis.com.” [Online]. Available: http://searchenterpriselinux.techtarget.com/definition/COTS-MOTS-GOTS-and-NOTS. [Accessed: 10-Mar-2011].