Global Information Assurance Certification Paper

Best Practices: Involving Information Security in Application Development Projects

Tammy Robinson
Version 1.4b
Submission Date: October 11, 2002

Table of Contents:

ABSTRACT

Security is concerned with the protection of assets from threats…[1]Enterprises are usually divided into departments. In manufacturing for example, there will probably be product designers, testers, accounting, payroll, human resources – and the list continues. Because companies are divided into so many smaller entities, large enterprise companies often find themselves in an information security dilemma.

Information security is centralized in many enterprises as a corporate function because there are many enterprise level functions that need to be performed. Enterprise activities might include intrusion detection systems, anti-virus control, and monitoring. All of these activities affect each user in the corporation. However, each department or line of business has special information security needs that are difficult to address on an enterprise level. Activities in the line of business include building specialized applications, creating the company web presence, providing customer support, etc. Most of these activities are projects with a defined beginning and ending point. Corporate information security departments find it difficult to keep up with the changing needs of different lines of business. With this in mind, the role of line of business information security officer (BISO)[2] was created.

BISOs are familiar with the climate, business needs, and security needs of their particular line of business. The BISO is able to handle many of the security needs of the line of business such as application reviews and risk assessments; however, BISOs often find themselves overwhelmed with requests for their services, or they are asked to evaluate a high-risk application using a technology with which they are not familiar. During these circumstances, it is necessary for the BISO to engage corporate information security in the project process.

This document describes the process thorough which the BISO can engage information security on line of business projects. Specifically, this document will target the relationship between the project players on web-based application development projects. In addition, this document will assist line of business information security officers (BISOs), the project managers (PMs), the developers, and corporate information security in determining security requirements and reviewing applications prior to production implementation.

The document is designed to suggest a best practices guide to help the members of an enterprise project team know what responsibilities fall upon them and provides a process to bring corporate information security into the application development project process. A process will be provided that will address concerns on when to contact corporate information security, criteria for ranking the risk of a project, and sample forms

[1] Common Criteria Support Environment. *Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and General Model*. Version 2.1 August 1999, 19. < http://www.commoncriteria.org/docs/PDF/CCPART1V21.PDF>

[2] Mogull, Richard. "*Building a Security-Aware Enterprise."* Gartner G2, January 2002. < http://www.gartnerg2.com/research/rpt-0102-0010.asp>

that can be used in corporate information security department work process flow.

Assumptions

This document will make several assumptions.

- The document is intended for an enterprise company with various lines of business (departments) as well as a corporate function.
- This document assumes that, as part of information security best practices, the corporate information security team employs a program office to coordinate Corporate Information Security workflow.
- The projects submitted to Corporate Information Security are application development projects.

Security Essentials: Should Information Security be Involved?

Lines of business projects often begin with the project manager. A project manager is assigned to a project and sets about finding resources, gathering information, writing documentation, and other project manager duties. This initial phase is the best time for information security to become involved with a project.

As project managers are the first line of contact, they will need a guide to determine if Information Security should be contacted. At a high level, the project manager should answer the following questions:

- Is this an Internet or Extranet project?
- Will the project require access to employee, customer or prospective customer information?
- Will the project result in external customer contact?
- Will the project involve a third party hosting arrangement?
- Will the project require new firewall rules?
- Will the project require new equipment or servers?
- Will the project involve authenticating or authorizing users?

If the answer to any of these questions is "yes," information security will be a concern in the project. At this point, the project manager is required to complete the Security Fundamentals form and contact the Line of Business Information Security Officer to arrange a meeting.

PROJECT MANAGER SECURITY FUNDAMENTALS CHECKLIST

In a large enterprise, there may be hundreds of projects flowing through one line of business. This can cause a heavy strain on the BISO resources. In addition, the BISO is often faced with project managers who have not managed a technology project; therefore, the first meeting between the project manager and the BISO is an informational session in which the BISO is left to explain what kind of information he/she needs to start evaluating the project.

To assist in the planning of the project and to facilitate a production first meeting, the project manager will complete this form before schedule a meeting with the Line of Business Information Security Officer (BISO). The information on the form can easily be obtained from project developers and does not go into great detail. This is the project at a very high level.

- The environment where the application will reside
- The application host
- The application author
- Changes to firewalls
- New hardware

Although this knowledge is by no means exhaustive, it is the basic information the BISO needs to get started. An Internet or extranet-facing application will need more security scrutiny than an internal project. Off-site hosting, depending upon the type of enterprise (health care, insurance, financial, government), may entail a lengthy audit of the off-site facility to make sure it complies with industry regulations. Background checks may be essential if contractors are used verses enterprise employees. Firewall changes will need to be investigated and tested for security. New hardware will need to be hardened before the application is loaded. These categories of information have been chosen not only with the BISO in mind. These categories are the ones that are most likely to affect the timeline the project manager has been given. If any of these categories are present, the timeline and perhaps the budget for the project will need to be increased to accommodate in-house or third party penetration testing.

With the form completed and the basic knowledge the form provided, the BISO will be able to assist the project manager in locating the appropriate policies and standards that will apply to the project as well as general information security standards. The BISO will also be able to assist in planning for security compliance related costs such as third-party penetration testing.

A copy of this form follows and can also be found in Appendix A.

Project Manager Security Fundamentals Checklist

Project Manager Contact Information:	
Name	
Email Address	
Phone Number	
Project Information:	
Line of Business	
Project Sponsor	
Project Name	
Project Description	
Current Project Status/Phase	
Project Fundamentals:	
What kind of application is being created?	Web or Client-Server Internet Intranet Extranet Mainframe Other:_____
Where will the application reside? (ie. Will the application server be inside or outside the company?)	In house 3rd Party
Who will build the application?	Employees Contractors (in house) Consulting firm or other third party
Will new firewall rules be needed?	Yes No Unknown
Will the project require new equipment?	Yes No Unknown

RESPONSIBILITY MATRIX

Projects are not built in a vacuum. Projects have multiple team players. There are project managers, developers, stakeholders, and sponsors. In this mix of people, it is easy for security to get lost or be pushed aside in favor of keeping the project on schedule or on budget. To make sure security is a part of every application build, a responsibility matrix has been created. Each team member has responsibilities to the project and to security. The list below is an overview of the responsibilities of each player.

Project Manager

The project manager is the driving force of the project. It is his/her responsibility to oversee and coordinate the different efforts on the project into one unified whole. The main responsibilities of the project manager are listed below:

- Fills in Project Manager Security Fundamentals Checklist
- Sets up meetings with line of business Information Security Officer (BISO)
- If applicable, contact IT Risk Supplier Technology Risk for vendor approval
- Responsible for project and security documentation
- Coordinates with BISO and developer to request security waivers
- If required, coordinates setting up security testing
- Assembles all needed project documentation for Information Security Final Review

BISO

The BISO is the first line of defense for security in a project. The BISO has the role of making sure that the project manager and the developers understand the security risks in their project and work to mitigate those risks before production. The BISO role is hugely important as a good relationship between the BISO and the project team will lead to a more secure product. The BISO…

- Works with project manager and developer on security documentation
- Indicates which security standards apply to project
- Determines if the project is low, medium, high security risk
- Checks and signs off on security diagrams
- Reviews security checklists
- Completes security risk analysis matrix
- Reviews security testing data
- Attends Information Security Final Review

Developer

Developers are the workhorses of the project. They are responsible, not only for the coding, but in many cases, they will also serve as the system administrator while the application is being built. This dual role can be frustrating, as many developers do not like the planning stages. They simply want to develop and worry about the documentation and planning later. Therefore, it is of great importance to clearly state what documentation and what processes the developer will be responsible to provide.

- Works with project manager and BISO on security documentation
- Completes security diagrams
- Completes security checklists

- Works with Project Manager on arranging security testing and testing plan
- Attends Information Security Final Review

Corporate Information Security

Corporate Information Security plays many roles in the project. For low or medium risk projects, Corporate Information Security will have little involvement. For complicated projects, members of the Corporate Information Security team may be called upon to lend technical expertise or mitigation skills to the project team. Corporate Information Security is responsible to make sure there is security documentation for the project. The role of reviewer is often overlooked in the security organization; however, the reviewer is the backup person for the BISO. The reviewer may be able to catch and prevent problems that the BISO overlooked. It is essential that Corporate Information Security present themselves in a professional, helpful manner to the project team and the BISO. The main responsibilities of Corporate Information Security follow:

- Reviews project and security documentation
- Provides BISO with estimate of work from Information Security Program Office
- Decides if 3rd party penetration testing is necessary for high-risk projects
- Replies to waivers and firewall change requests
- Provides access to security testing tools
- Signs off at Information Security Final Review

Detail

There are some elements that all projects must follow. Some of these activities are security-related. Some of these activities, such as a delivery process, are enterprise mandates. For all projects:

- All projects must follow the corporate delivery process of initiation, manufacturing, and deployment
- Activities on this chart are broken down by project phase.
- Security coverage is the responsibility of the BISO and Project Manager.
- All projects should be initiated through the BISO who will coordinate with Corporate Information Security.
- High-risk projects such as those facing the Internet or dealing with confidential information will need the approval of Corporate Information Security. The BISO will be responsible for coordinating this activity.
- All lines of business must follow this standard.
- Involvement of Corporate information security personnel, when required, will be coordinated by the BISO.

Responsibility Matrix Detail

Note: Due to spacing constraints, the font on the table has been reduced.

Task	Project Manager	BISO	Developer	Corporate Information Security
To be completed in Initiation Phase				
Project Manager Security Fundamentals Checklist (Appendix A)	Completes with as much detail as possible.	- Checks, signs off, and indicates which security checklists will be needed. - Determines if project is low, medium, high risk using the Project Risk Evaluation Matrix. - For projects deemed high risk, the BISO forwards the following to Corporate Information Security: • Fundamentals Checklist (Appendix A), • any project documentation, • and a Request for Information Security Project Involvement (Appendix C)..	N/A	Information Security Program office receives and processes the Request for Information Security Project Involvement.
Estimate of Work (Appendix D)	N/A	When the estimate of work is received, the BISO schedules a meeting with the security contact to discuss coverage needs.	N/A	The Program Office will begin to track Corporate Information Security work and return an Estimate of Work (Appendix D) and a corporate security contact to BISO within 5 business days.
To be completed in Manufacturing Phase				
Complete application diagrams: Application Data Flow Diagram Network/Firewall Connectivity Diagram Architecture Diagram	Files copies of the diagrams with project documentation.	Checks and signs off on diagrams. Forwards to Corporate IS for high-risk projects.	Completes the diagram. Forwards to BISO and Project Manager.	Reviews documentation for high risk projects
Security Checklists	N/A	Reviews the checklists. Forwards to Corp IS if high-risk. Low and Medium risk projects can hold documentation until final security review.	Completes security checklists as determined by the BISO/Corp IS	Reviews documentation for high risk projects

Task	Project Manager	BISO	Developer	Corporate Information Security
Security Test Plan	Works with BISO to create testing plan for the application	Works with Project Manager to create a testing plan for the application	Submits change management documentation for testing.	Reviews testing plans for high risk projects
Firewall changes	Sets up meeting with BISO and developer to draft request	Meets with Project Manager and developer. Forwards request to Corporate IS	Meets with Project Manager and BISO	Reviews and replies to firewall changes
Security Testing	Sets up meeting with BISO and developer to go over testing results	Reviews testing data; determines if testing is complete. Reviews recommendations from penetration tests	Runs or arranges for test according to change management specifications; supplies BISO/Project Manager with test results.	Provides access to Information Security testing tools such as network testing tools and application testing products. Reviews application testing and penetration tests.
Before deployment	Assembles all needed project documentation. (See Appendix E: Final Security Review). Sends to BISO for review	Reviews documentation. Sets up meeting with Corporate IS for final project review.	Attends final review	Reviews documentation for Corporate Information Security Final Review (Appendix E) and provides sign-off.

TOOLSETS

Several tools are mentioned throughout the responsibility matrix. Each tool is designed to assist the project team, the BISO, the developer, and Corporate Information Security to plan, build, and execute a secure application. A description of each tool will help the BISO and Project Manager in using the tools effectively. There are six tools to assist in security project planning. Each tool will be explained and a copy of the tool inserted directly after the explanation.

- Security Fundamentals Checklist (Appendix A)
- BISO/Information Security Project Risk Evaluation (Appendix B)
- Request for Corporate Information Security Involvement (Appendix C)
- Corporate Information Security Estimate of Work (Appendix D)
- Corporate Information Security Final Security Review (Appendix E)
- Process Workflow Diagram (Appendix F)

APPENDIX A: PROJECT MANAGER SECURITY FUNDAMENTALS CHECKLIST

This checklist is used by the Project Manager to get the basic information the BISO will need upon an initial meeting to discuss the project. A full description is provided in the Project Manager Security Fundamentals Checklist section of this document.

Security Fundamentals Checklist

Instructions: Project Manager should complete and email to BISO. BISO will review and contact Project Manager on next steps.

Project Manager Contact Information:	
Name	
Email Address	
Phone Number	
Project Information:	
Line of Business	
Project Sponsor	
Project Name	
Project Description	
Current Project Status/Phase	
Project Fundamentals:	
What kind of application is being created?	Web or Client-Server Internet Intranet Extranet Mainframe Other: _____
Where will the application reside? (ie. Will the application server be inside or outside the company?)	In house 3rd Party
Who will build the application?	Employees Contractors (in house) Consulting firm or other third party
Will new firewall rules be needed?	Yes No Unknown
Will the project require new equipment?	Yes No Unknown

APPENDIX B: BISO/INFORMATION SECURITY PROJECT RISK EVALUATION

The risk evaluation chart will help to determine the data security risk of the project and the priority that the project will be assigned in Corporate Information Security.

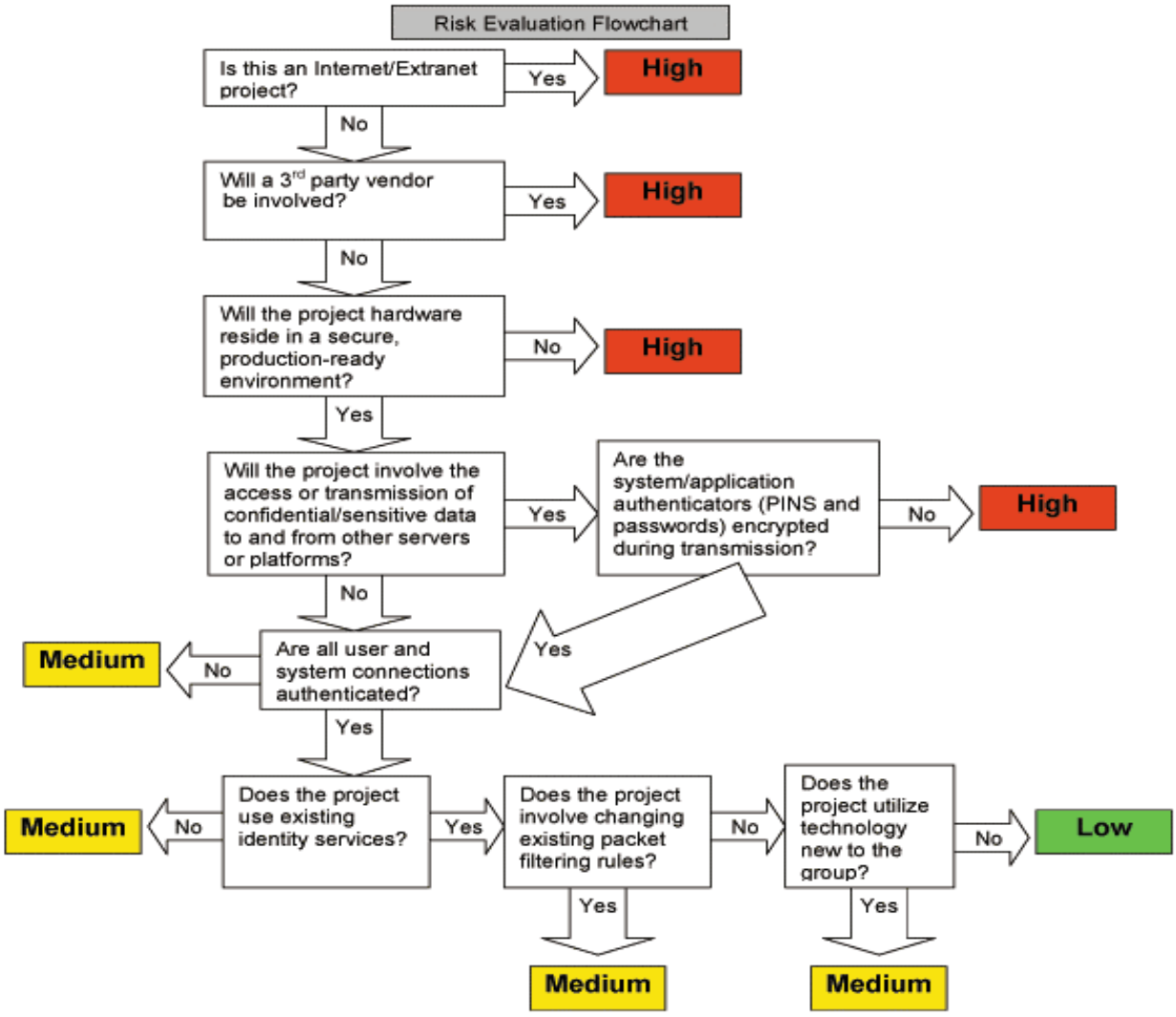
This tool has been designed with simplicity in mind. The chart is a visual representation of security risk in a project. As the BISO moves from one question to the next, he/she gets a visual picture of the risk factors in the project that is being surveyed. In addition, the tool provides an easy assessment of risk from Corporate Information Security. For example, if a high-risk project is presented to Corporate Information Security, using the chart, the project has one of these elements:

- it is an Internet or extranet project
- it has involvement from a 3rd party in hosting or coding
- the hardware is not housed in a production-ready environment
- or there are encryption issues in the project

By the same token, if a medium risk project is presented, Corporate Information Security will automatically know that the project does not have the above-listed elements. As the Security Fundamentals Checklist will give the BISO a quick overview of the project, so the Project Risk Evaluation will give Corporate Information Security a quick overview of project elements.

To use the matrix, answer each question. When the answer to the question terminates in high, medium, or low, this is the data risk evaluation for your project. High-risk project must be reported to Corporate Information Security. Corporate involvement at the medium or low risk range is determined by the BISO. Projects in Corporate Information Security will be prioritized using this matrix.

An example of a Risk Assessment Matrix follows.



APPENDIX C: REQUEST FOR INFORMATION SECURITY PROJECT INVOLVEMENT

This form is used by the BISO to request services from Corporate Information Security. This form is equivalent to the security fundamentals worksheet for the project manager. It gives Corporate Information Security the basic information needed to start the process of evaluating a project. No detailed information is required, as some projects will not have fleshed out the requirements; however, enough information is given to give Corporate Information Security a good idea of what security measures the project will need to plan to accommodate.

A service level agreement is included on the worksheet. The service level agreement holds Corporate Information Security accountable for the project requests it receives. Within five business days, Corporate Information Security will look over the material provided and assign a security contact. The security contact is essential to the process as it validates the service-oriented relationship Corporate Information Security seeks to portray to the lines of business. Far from being a stagnant corporate entity, viable Corporate Information Security departments will seek to be as customer-oriented as external service providers.

Request for Corporate Information Security Involvement

Project Name:	
Project Number:	
Project Manager:	
BISO/Line of Business:	
Project Description and Goal:	
Attachments:	Project Manager Security Fundamentals Checklist List of Applicable Security Standards Project Risk Evaluation

Service Level Agreement: You will be contacted within 5 business days with a preliminary estimate of work (see Appendix D)** and a security contact.

APPENDIX D: ESTIMATE OF WORK

Corporate Information Security will send the BISO a copy of this form indicating the estimated level of work and commitment that will be needed on the project. As indicated on the Request for Project Involvement, an estimate of work will be returned to the BISO according to the SLA within 5 working days. The BISO will also be provided a Corporate Information Security contact for the project.

The main goal of the estimate of work is not to pinpoint the number of hours that will be needed on a project. Instead, the goal of the estimate of work is to give the project team and the BISO the assurance that their project is in the Corporate Information Security queue. Additionally, the estimate of work is a broad overview of Corporate Information Security's involvement. For example, projects that rate low risk will need no other involvement from the Corporate Information Security other than coordinating and reviewing the material for the final review.

This does not mean, however, that Corporate Information Security services will not be needed in the project. Network scanners, application scans, and authentication and encryption services may very well be needed in the project. A medium or low rating simply gives the BISO the leeway to coordinate those activities with the line of business project manger without the overhead of an additional Corporate Information Security project manager.

To avoid frustration and possible misunderstanding on the part of the project team, the team needs to be aware that a preliminary estimate of work is not a guarantee. It is an estimate of the effort needed by Information Security personnel to complete the project evaluation. Additional information may be needed to complete an accurate estimate or changes in the project scope or additional challenges to the project may increase Corporate Information Security's involvement.

A sample Estimate of Work follows.

Estimate of Work

Project Name:	
Project Number:	
Project Manager:	
BISO/Line of Business:	
Project Description and Goal:	
Work Estimate:	Based on the information given, Corporate Information Security's involvement will be: ____ low • Conducts final security review ____ medium • Reviews security milestones • Conducts final security review ____ high • Actively involved with development team • Reviews security milestones • Conducts final security review
Information Security Program Office Internal Prioritization:	
Your security contact is:	Name Contact information

APPENDIX E: INFORMATION SECURITY FINAL SECURITY REVIEW

The final review process is a final assurance that all security measures have been fully documented and implemented. If the process has been followed, the final review should go smoothly as the documentation has been reviewed at various points throughout the project. The final review should include Corporate Information Security, the line of business Project Manager, the BISO, the lead System Administrator, and the lead Developer.

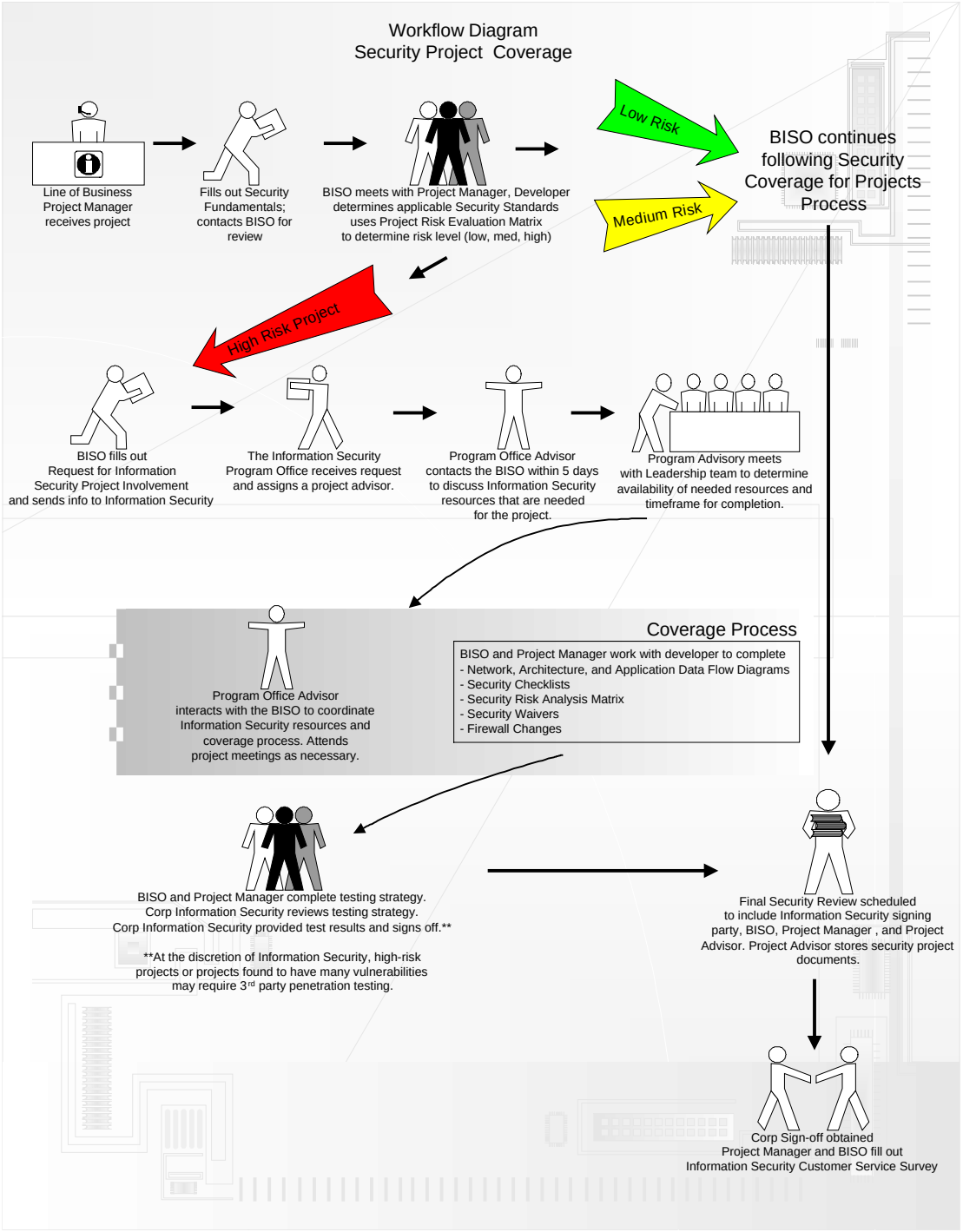
Corporate Information Security Final Review

	Security Documentation:	Notes:
	Security Fundamentals Checklist	
	List of Application Security Standards	
	Project Risk Evaluation (low, medium, high)	
	Estimate of Work and Security Contact	
	Application Data Flow Diagram	
	Network/Firewall Connectivity Diagram	
	Architecture Diagram	
	Completed Security Checklists	
	Security Risk Analysis Matrix	
	Completed Security Waivers (if applicable)	
	Completed Firewall Change Request (if applicable)	
	Security Testing Plan and Results	

	Print Name	Signature	Date
BISO			
Line of business Project Manager			
Corporate Information Security			

WORKFLOW DIAGRAM

Introducing a new process into the enterprise is never easy. When the Corporate Information Security department develops a program office and a corporate workflow, it is necessary to communicate that change. It is especially important that the BISOs are familiar and comfortable with using the process. To assist in the learning process, it is wise to create a visual workflow that gives a good overall picture of the Corporate Information Security process.



LIST OF REFERENCES

Common Criteria Support Environment. *Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and General Model*. Version 2.1 August 1999, 19. < http://www.commoncriteria.org/docs/PDF/CCPART1V21.PDF>

Harris, Shon. All in One CISSP Certification Exam Guide. New York: McGraw-Hill, 2002.

Hunt, Steve, and Phil Rosch. "*Best Practices in Managing IT Security*." Giga Information Group, Inc., 5 March 2002. < http://www.gigaweb.com/mktg/sarcx/best_practices.pdf>

Kernzer, Harold. Project Management A Systems Approach to Planning, Scheduling, and Controlling. New York: John Wiley & Sons, Inc., 2001.

Light, M., and T. Berg. "*The Project Office: Teams, Processes and Tools*." Gartner Group, Inc., 1 August 2000. <http://www.aisc.com/us/lang_en/library/analyst_information/analyst_reports/GARTNERStrategicAnalysisRep.pdf >

Mogull, Richard. "*Building a Security-Aware Enterprise.***"** Gartner G2, January 2002. < http://www.gartnerg2.com/research/rpt-0102-0010.asp>

Pentasafe Security Technologies. *"Integrated Security Management: Managing Four Critical Security Functions to Improve Protection Across Your Enterprise."* Houston: Pentasafe Security Technologies, 2002. < http://www.pentasafe.com/whitepapers/ISM_whitepaper.pdf>

Pfleeger, Charles. Security in Computing. 2nd Edition. New York: Prentice Hall Professional Technical Reference, 1996.