# Project: Access Control Proposal

## Purpose

This course project is intended to assess your ability to comprehend and apply the basic concepts related to information security management, such as the following:

- The ability to discern when a risk assessment should be performed and carrying out the task
- Understanding user or customer access requirements, whether remote or local
- Using a layered security approach to establish and maintain access controls
- Working with other departments, such as the human resources department, to identify and implement methods to prevent unwarranted exposure to information by inappropriate personnel

Your ability to execute the tasks within these information security domains and others will be evaluated against the learning objectives as identified and described in previous lessons of instruction for this course.

## Required Source Information and Tools

The following tools and resources will be needed to complete this project:

- Course textbook
- Access to the Internet
- Access to the library
- IDI Project.pdf

## Learning Objectives and Outcomes

Successful completion of this project will ensure that you are capable of supporting the implementation and management of an information systems security framework. To be able to do so, you need to be able to do the following:

- Relate how an access control policy framework is used to define authorization and access to an information technology (IT) infrastructure for compliance.
- Mitigate risks to an IT infrastructure's confidentiality, integrity, and availability with sound access controls.
- Relate how a data classification standard influences an IT infrastructure's access control requirements and implementation.
- Develop an access control policy framework consisting of best practices for policies, standards, procedures, and guidelines to mitigate unauthorized access.
- Define proper security controls within the User Domain to mitigate risks and threats caused by human nature and behavior.

- Implement appropriate access controls for information systems within IT infrastructures.
- Mitigate risks from unauthorized access to IT systems through proper testing and reporting.

## Project Checkpoints

The course project has a checkpoint strategy. Checkpoint deliverables allow you to receive valuable feedback on your interim work. In this project, you have four ungraded checkpoint deliverables. (See the syllabus for the schedule.) You may discuss project questions with the instructor, and you should receive feedback from the instructor on previously submitted work. The checkpoint deliverable ensures refinement of the final deliverables, if incorporated effectively. The final deliverable for this project is a professional report and a PowerPoint presentation.

| Checkpoint | Purpose of the Checkpoint | Expected Deliverables |
|---|---|---|
| 1 | ▪ Understanding requirements<br>▪ Clarification on project deliverables<br>▪ Discussion on project concerns and progress up to this checkpoint<br>▪ A review of the course project's outline and schedule for completion | Prepare an initial outline of issues and potential solutions and discuss with your instructor, the chief information officer (CIO). |
| 2 | ▪ Clarification on project deliverables<br>▪ Discussion on project concerns and progress up to this checkpoint<br>▪ A review of the course project's outline and schedule for completion | Prepare an extended outline of issues and potential solutions and discuss with your instructor, the CIO. |
| 3 | ▪ Clarification on project deliverables<br>▪ Discussion on project concerns and progress up to this checkpoint<br>▪ A review of the course project's outline and schedule for completion | Draft the report and the PowerPoint presentation to discuss with your instructor, the CIO. |
| 4 | ▪ Clarification on project deliverables<br>▪ Discussion on project concerns and progress up to this checkpoint<br>▪ A review of the course project's outline and schedule for completion | Modify the report and the PowerPoint presentation based on feedback from your instructor, the CIO. |

## Deliverables

### Introduction

User identification, authentication, and authorization are essential in developing, implementing, and maintaining a framework for information system security. The basic function of an information system security framework is to ensure the confidentiality and the integrity, as well as the availability of systems, applications, and data. Certain information security implementation and management knowledge is required of network administrators, IT service personnel, management, and IT security practitioners, such as information security officers, security analysts, and domain administrators.

### Scenario

You are provided with the document, Scenario.pdf, needed to complete this project. You play the dual role of an IT architect and IT security specialist working for Integrated Distributors Incorporated (IDI), a multi-national organization with offices in several countries. Your instructor for this course plays the role of the chief information officer (CIO). Your peers play the role of selected technology staff. Each of the organization's locations is operating with different information technologies and infrastructure—IT systems, applications, and databases. Various levels of IT security and access management have been implemented and embedded within their respective locations.

### Tasks

Your goals as the IT architect and IT security specialist are to:

- Develop solutions to the issues that the specified location of IDI is facing.
- Develop plans to implement corporate-wide information access methods to ensure confidentiality, integrity, and availability.
- Assess risks and vulnerabilities with operating IT facilities in the disparate locations where IDI now functions and develop mitigation plans and implementation methods.
- Analyze the strengths and weaknesses in the current systems of IDI.
- Address remote user and Web site user's secure access requirements.
- Develop a proposed budget for the project—consider hardware, software, upgrades/replacements, and consulting services.
- Prepare detailed network and configuration diagrams outlining the proposed change to be able to present it to the management.
- Develop and submit a comprehensive report addressing the learning objectives and your solutions to the issues within the scenario.

- Prepare a 10- to 15-slide PowerPoint presentation that addresses important access control, infrastructure, and management aspects from each location.

**Self-Assessment Checklist**

- I have considered an access control policy framework to define authorization and access to an IT infrastructure for compliance within the course project.
- I have considered the influence of the data classification standard in an IT infrastructure's access control requirements and implementation.
- I have defined proper security controls within the User Domain to mitigate risk and threats caused by human nature and behavior.
- I have developed and implemented an effective plan to mitigate risks to an IT infrastructure's confidentiality, integrity, and availability with sound access controls.
- I have developed an access control policy framework consisting of best practices for policies, standards, procedures, and guidelines to mitigate unauthorized access.
- I have implemented appropriate access controls for information systems within IT infrastructures.
- I have followed the submission requirements and necessary details for writing the report.