# Project #4: IT Audit Policy and Plans

## Company Background & Operating Environment

Use the assigned case study for information about “the company.”

## Policy Issue & Plan of Action

The corporate board was recently briefed by the Chief Information Officer concerning the company’s IT Security Program and how this program contributes to the company’s risk management strategy. During the briefing, the CIO presented assessment reports and audit findings from IT security audits. These audits focused upon the technical infrastructure and the effectiveness and efficiency of the company’s implementation of security controls. During the discussion period, members of the corporate board asked about audits of policy compliance and assessments as to the degree that employees were (a) aware of IT security policies and (b) complying with these policies. The Chief Information Officer was tasked with providing the following items to the board before its next quarterly meeting:

1. Issue Specific Policy requiring an annual compliance audit for IT security policies as documented in the company’s Policy System
2. Audit Plan for assessing employee awareness of and compliance with IT security policies
   1. Are employees aware of the IT security policies in the Employee Handbook?
   2. Do employees know their responsibilities under those policies?
3. Audit Plan for assessing the IT security policy system
   1. Do required policies exist?
   2. Have they been updated within the past year?
   3. Are the policies being reviewed and approved by the appropriate oversight authorities (managers, IT governance board, etc.)?

**Your Task Assignment**

As a staff member supporting the CISO, you have been asked to research this issue (auditing IT security policy compliance) and then prepare an “approval draft” for a compliance policy. You must also research and draft two separate audit plans (a) employee compliance and (b) policy system audit. The audit policy should not exceed two typed pages in length so you will need to be concise in your writing and only include the most important elements for the policy. Make sure that you include a requirement for an assessment report to be provided to company management and the corporate board of directors.

* For the employee compliance assessment, you must use an interview strategy which includes 10 or more multiple choice questions that can be used to construct a web-based survey of all employees. The questions should be split between (a) awareness of key policies and (b) awareness of personal responsibilities in regards to compliance.
* For the policy system audit, you should use a documentation assessment strategy which reviews the contents of the individual policies to determine when the policy was last updated, who “owns” the policy, who reviewed the policy, and who approved the policy for implementation.

## Research:

1. Review the weekly readings including the example audit assessment report.
2. Review work completed previously in this course which provides background about the IT Policy System and specific policies for the case study company.
3. Find additional resources which discuss IT compliance audits and/or policy system audits.

## Write:

1. Prepare briefing package with approval drafts of the three required documents. Place all three documents in a single MS Word (.doc or .docx) files.
2. Your briefing package must contain the following:

* Executive Summary
* “Approval Drafts” for
  + Issue Specific Policy for IT Security Policy Compliance Audits
  + Audit Plan for IT Security Policy Awareness & Compliance (Employee Survey)
  + Audit Plan for IT Security Policies Audit (Documentation Review)

As you write your policy and audit plans, make sure that you address security issues using standard cybersecurity terminology (e.g. 5 Pillars of IA, 5 Pillars of Information Security). See the resources listed under Course Resources > Cybersecurity Concepts Review for definitions and terminology.

1. Use a professional format for your policy documents and briefing package. Your policy documents should be consistently formatted and easy to read.
2. Common phrases do not require citations. If there is doubt as to whether or not information requires attribution, provide a footnote with publication information or use APA format citations and references.
3. You are expected to write grammatically correct English in every assignment that you submit for grading. Do not turn in any work without (a) using spell check, (b) using grammar check, (c) verifying that your punctuation is correct and (d) reviewing your work for correct word usage and correctly structured sentences and paragraphs.

## Submit For Grading

Submit briefing package in MS Word format (.docx or .doc file) for grading using your assignment folder. (Attach the file.)