# Case Study #2: Integrating Disaster Recovery / IT Service Continuity with Information Technology Governance Frameworks

## Case Scenario:

You have been assigned to a large, cross-functional team which is investigating adopting a new governance framework for your company’s Information Technology governance program. Your first assignment as a member of this team is to research and write a 2 to 3 page white paper which discusses one of the Chief Information Security Officer (CISO) functional areas. The purpose of this white paper is to “fill in the gaps” for team members from other areas of the company who are not familiar with the functions and responsibilities of the Office of the Chief Information Security Officer.

**Your assigned CISO functional area is:** **Disaster Recovery / IT Service Continuity** (*IT Service Continuity* is a subset of *Business Continuity*). Your white paper must address the *planning, implementation,* and *execution* aspects of this CISO functional area. Your audience will be familiar with the general requirements for business continuity planning (BCP), business impact analysis (BIA), and continuity/recovery strategies for business operations (e.g. restore in place, alternate worksite, etc.). Your readers will NOT have in-depth knowledge of the requirements / implementation strategies which are specific to restoring IT services which support the critical functions of the business (as identified in a BIA).

**Note:** in your *Critical Analyses and Discussion* for this case study you will address specific aspects of a governance framework, e.g. COBIT®, ITIL®, or ISO/IEC 27002, which apply to planning and implementation of disaster recovery / IT Service Continuity.

## Research:

1. Read / Review the Week 3 readings:
2. Find three or more additional sources which provide information about best practices for IT Service Continuity / Disaster Recovery planning, implementation, and execution. (Hint: begin by exploring <http://www.ready.gov/business> ) For the purposes of this assignment, *implementation* means the advance work necessary to implement recovery plans by acquiring or contracting for products, services, infrastructures, and facilities. Execution means activating the DR/BCP plans and overseeing the recovery operations.

## Write:

Using standard terminology (see case study #1), write a two to three page summary of your research. At a minimum, your summary must include the following:

1. An introduction or overview of disaster recovery / IT Service Continuity which provides definitions and addresses the reasons **why cybersecurity should be specifically addressed** **in the company’s DR/BCP strategies and plans.** This introduction should be suitable for an executive audience.
2. A separate section which addresses disaster recovery / IT Service Continuity planning functions performed by staff members in the Office of the CISO.
3. A separate section which addresses best practices for implementing disaster recovery / IT Service Continuity.

## Submit For Grading & Discussion

Submit your case study in MS Word format (.docx or .doc file) using the Case Study #2 Assignment in your assignment folder. (Attach the file.)

## Formatting Instructions

1. Use standard APA formatting for the MS Word document that you submit to your assignment folder. Formatting requirements and examples are found under Course Resources > APA Resources.

## Additional Information

1. 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. These items are graded under Professionalism and constitute 20% of the assignment grade.
2. You are expected to credit your sources using in-text citations and reference list entries. Both your citations and your reference list entries must comply with APA 6th edition Style requirements. Failure to credit your sources will result in penalties as provided for under the university’s Academic Integrity policy.