Course : DSI, anticipating and managing a crisis

Seminar - 2d - 14h00 - Ref. GCI
Price : 1850 € E.T.

Today, all an organization's activities depend on its information system. To guarantee a safe and reliable system, you need to be able to quickly restart your business and minimize data loss in the event of a problem. In this seminar, you will learn how to identify possible crises, organize their management before they occur, and structure a crisis plan to deal with them.

Teaching objectives

At the end of the training, the participant will be able to:

- ✓ Understanding the different types of crisis in an IS context
- ✓ Define the key elements and different scenarios for managing an IT crisis
- ✓ Structuring a crisis plan
- ✓ Managing the different stages of a crisis
- ✓ Developing an IT continuity plan

Intended audience

Managers, information systems directors, IS managers, engineers, project managers and anyone dealing with crisis situations.

Prerequisites

Basic knowledge of the components and role of an IS department. Experience in IS management required.

Course schedule

1 Introduction

- What is a crisis?
- Exceptional events due to their scale.
- Psychological threshold exceeded. Immediate inability to restore the situation.
- Change, a vector for crisis. The ability to react.
- Typology of IT crises. First mistakes to avoid for IT Departments.

PARTICIPANTS

Managers, information systems directors, IS managers, engineers, project managers and anyone dealing with crisis situations.

PREREQUISITES

Basic knowledge of the components and role of an IS department. Experience in IS management required.

TRAINER QUALIFICATIONS

The experts leading the training are specialists in the covered subjects. They have been approved by our instructional teams for both their professional knowledge and their teaching ability, for each course they teach. They have at least five to ten years of experience in their field and hold (or have held) decision-making positions in companies.

ASSESSMENT TERMS

The trainer evaluates each participant's academic progress throughout the training using multiple choice, scenarios, hands-on work and more.
Participants also complete a placement test before and after the course to measure the skills they've developed.

② Crisis potential and scenarios

- Crises only happen to other people! Anticipate and prepare.
- Assess crisis potential. Identify all stakeholders.
- Objectives of the crisis management organization. Use crisis scenarios.
- Prepare for danger. Reduce the severity of the event if and when it occurs.
- Study and pre-deploy protective measures in advance. Limit impact and collateral damage.
- Formalize trigger levels.

③ Steps in crisis management

- Invariable steps. Diagnosis, action and decision.
- Quickly perceive the seriousness of the situation. Induced priorities and most appropriate decisions.
- Crisis entry. Setting up the crisis unit.
- Duties to be performed.

④ Crisis unit

- Setting up a crisis unit. Crisis entry: detection, first actions.
- Setting up a crisis unit. Functions to be performed.
- Communication. Alert and inform staff, partners and the media.

Case study
Crisis simulation.

⑤ Risk management

- Crisis and risk detection.
- Analyze, assess and prioritize risks.
- Risk management: phases of risk management, legal obligations.
- Standards and methods (brief introduction).
- Organization of the function "risk management".

⑥ IT continuity plan

- Issues and priorities. Recovery options. Input information.
- Vital processes and SLR. Knowledge of IS (CMDB).
- Targets for recovery times and recovery points. Diagnosis of the situation.
- Stages in the implementation of a BCP. Importance of testing and level of maturity.
- Writing the BCP document. A few rules for building an effective BCP.
- Team roles and responsibilities. Recommendations and keys to ICP success.

Dates and locations

REMOTE CLASS
2026 : 16 Apr., 4 June, 17 Sep., 24 Nov.

PARIS LA DÉFENSE
2026 : 4 June, 17 Sep., 24 Nov.