Exercise planner

Package 3, exercise 2

‘Irregularities in data traffic’

Version 1.0

Table of contents

1 Introduction

1.1 Background and scope

Facilities and installations in the petroleum sector are required to have preparedness plans in place for managing serious incidents. The industry is subject to various scenarios involving ICT incidents, but the Norwegian Ocean Industry Authority (Havtil) has, through audits, noted that little or no training is carried out related ICT security in the industrial control and security systems. Considering this, Havtil has commissioned a set of training and exercise scenarios. These exercises have been prepared by Proactima together with Netsecurity and was adapted by Havtil.

The Activity regulation § 23 stipulates that: «necessary training and necessary drills are conducted, to ensure that the personnel are always able to handle operational disturbances, hazard, and accident situations in an effective manner». The Technical and Operational regulation stipulates the same in § 52. This means that the requirements for training and exercise are the same for onshore and offshore facilities.

Training enhances personal skills and knowledge, while exercises test collaboration and response capabilities during an emergency. In addition, exercises can reveal organisational and structural strengths and weaknesses and prepare management for dealing with various crises.

1.2 Structure of this guide

The exercise planner contains several scenarios. Each scenario includes suggestions on which functions are relevant to the exercise. The scenarios can be used for training, tabletop exercises, or incident response simulation exercises.

Part 3 of the guide contains additional information to aid in preparation and implementation. This includes:

- a possible sequence of events prior to exercise start-up
- a sequential incident flow chart

2 Scenario

Most installations on the Norwegian Continental Shelf (NCS) have communication solutions that enables effective transference of production data to ICT systems for operational support and analysis. A lacking correspondence between the production data from the operation systems and the data that is utilised in the models for support functions is detected.

2.1 Overview of the scenario

Table 1 indicates which functions/departments that are relevant for the different scenarios. It is up to the exercise leader to select which tasks to include in the exercise.

Table 1. Summary of roles/functions that can be trained using the various modules.

Task	Stage	Personnel responsible for SAS/IACS	Local operations managers	Personnel responsible for systems operation	ICT department
2.2	Initial events – irregularities between production data and models	x		x	x
2.3	Further development – changes in the system			x	x

2.2 Initial events – irregularities between production data and models

In the interaction between the control room operator and the personnel responsible for production planning, it is discovered that for the past weeks, data from the production models has deviated from the operational results in the control room. Responsible personnel for production planning contacts personnel responsible for system operation.

2.2.1 Initial questions

Personnel responsible for system operation

- Which systems are involved?
    - Who is responsible for the individual systems?
    - Who are data owners and what is the interface between the owners?
- Does it exist any logs for performed work on the systems? If so, what is logged?

ICT department

- What is the ICT department's responsibility for the involved systems?
- How can the ICT department assist?

Personnel responsible for SAS/IACS

- How can personnel responsible for SAS/IACS assist?
- Has any work been executed on relevant instruments and systems? If so, what work has been done?
- How does collaboration with onshore departments take place?

2.3 Further development – changes to the system

Personnel responsible for system operation contacts personnel responsible for applications and is informed that there recently was made a minor change to follow-up the initiative from management regarding energy optimalisation. Considering this, an application has been implemented to follow up the energy usage as a result of production. The change is implemented in collaboration with the local operations managers and personnel responsible for electronics.

2.3.1 Initial questions

- How to investigate what has happened?
  - Are the changes documented?
  - Are there any backups?
  - How are implementation and changes to such applications verified and approved?

3 Additional information for preparation and implementation

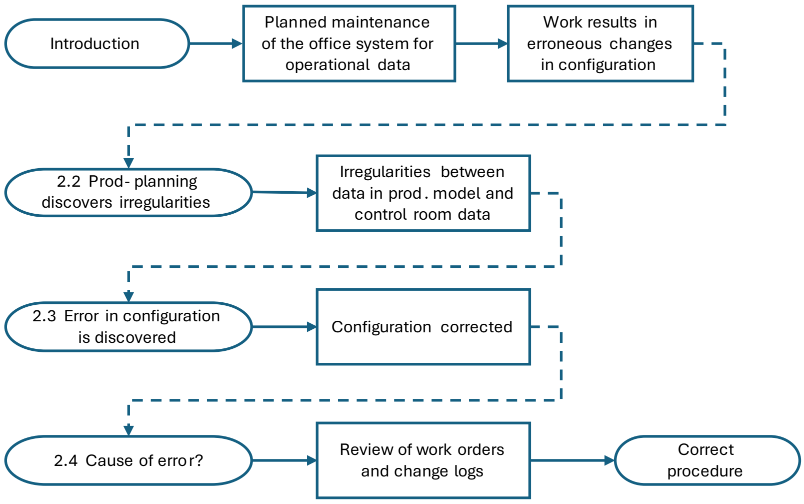
Not all incidents in the ICT systems are a result of cyberattacks. This exercise is connected to a minor modification where the changes affect other parts of the user managed solutions.

The exercise utilises the role “personnel responsible for applications”. This role is thought to be a function in the operational support environment who utilises data from operations made available in the office network. The applications consist partially of long-term solutions, and partially of short-term set ups to examine specific issues. These solutions are not necessarily subject to the same change management regime as the other ICT systems.

3.1 The incident

Management has increased its focus on energy optimalisation. They want data-driven display of energy efficiency. Personnel responsible for applications has, in collaboration with the onshore operations manager and electrical systems supervisor created an application for monitoring of energy consumption as a function of production. The solution is an expansion of the software and data used for displaying data for production optimalisation.

3.2 The incidenta


Introduction
Planned maintenance of the office system for operational data
Work results in erroneous changes in configuration
2.2 Prod- planning discovers irregularities
Irregularities between data in prod. model and control room data
2.3 Error in configuration is discovered
Configuration corrected
2.4 Cause of error?
Review of work orders and change logs
Correct procedure

3.3 Lessons learned

Review of procedures, clarification of roles and responsibilities, and improvement of systems.

3.3.1 Advisory questions

- Are roles and responsibilities adequately described?
- How to ensure that lessons learned from this incident are implemented?
- Who is responsible for the functions data owner and personnel responsible for applications?