

## Purpose

The purpose of this document is to provide sample questions for discussion during a “Lessons Learned” session as part of an incident root cause analysis. Meeting participants are encouraged to share their opinion freely and to the benefit of continuous learning.

## Incident Summary

<Provide a short incident summary, highlighting start time, end time, impact, and resolution. Do not provide details so the discussion can focus on learning and not on technicalities.>

## Questions

1. Technology
  - a. Was adequate technology in place to detect the incident?
  - b. Did the team have access to tools to efficiently and effectively resolve the incident?
  - c. Are there any tools missing to more efficiently detect similar incidents in the future?
  - d. What additional tools or technologies would be helpful to more effectively resolve similar incidents in the future?
2. Team Members
  - a. Were the correct team members involved?
  - b. Did the team members have adequate training to resolve the incident?
  - c. Did each team member know their assigned tasks?
  - d. Were the correct departments involved?
  - e. Were team members relieved by backup team members at the appropriate time?
3. Partners / Vendors
  - a. Did the partners/vendors respond in an appropriate timeframe?
  - b. Were the right vendors involved?
  - c. Did the partner / vendor team members contribute positively to the incident resolution?
  - d. Did the partner / vendor team members have adequate training to assist with the resolution of the incident?
4. Communication & Process
  - a. Was the Incident Response Plan followed?
  - b. Were the incident response team members notified in a timely manner?
  - c. Did the team have access to the correct communication tools?
  - d. Was the end-user communication clear and concise?
  - e. Did management provide adequate support during the incident?
  - f. Was the communication to external entities, such as law enforcement, regulatory entities, legal counsel, etc., adequate and timely?