

# Incident Recovery Checklist

## The IH&R team must perform the following activities during the recovery phase:

<input type="checkbox"/>	Whether there are various system recovery strategies implemented according to the incident's impact
<input type="checkbox"/>	Whether there is an appropriate plan after considering the availability of resources, the criticality of affected systems, and the results of a cost-benefit analysis
<input type="checkbox"/>	Whether the IH&R team has monitored and validated affected systems to ensure that the recovered systems do not have any traces of incident
<input type="checkbox"/>	Whether the IH&R team has checked the integrity of restored information from a backup
<input type="checkbox"/>	Whether the IH&R team has verified the system's normal condition after installing the backup
<input type="checkbox"/>	Whether the organization is performing regular vulnerability assessments and penetration testing
<input type="checkbox"/>	Whether the IH&R team is monitoring the system using network loggers and system log files
<input type="checkbox"/>	Whether the impacted systems are rebuilt by installing a new OSes
<input type="checkbox"/>	Whether the team has restored the user data from a trusted backup
<input type="checkbox"/>	Whether the team has replaced the infected files with clean copies
<input type="checkbox"/>	Whether the passwords of all systems and networks have been changed
<input type="checkbox"/>	Whether the team has examined all protection and detection methods
<input type="checkbox"/>	Whether there is an inspection of security patches before installation and enabling system logging