

Incident Eradication Checklist

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

<input type="checkbox"/>	Whether the antivirus software is updated with new malware signatures and patterns
<input type="checkbox"/>	Whether the systems and network devices are installed with latest patches
<input type="checkbox"/>	Whether the security personnel is performing independent security audits
<input type="checkbox"/>	Whether there is a policy compliance and updated obsolete policies and procedures
<input type="checkbox"/>	Whether the security personnel have disabled all unnecessary services
<input type="checkbox"/>	Whether the passwords have been changed for all compromised systems, accounts, and network devices
<input type="checkbox"/>	Whether the security personnel have eliminated all access paths and exploits
<input type="checkbox"/>	Whether the operating system, software, and services in compromised systems are installed with an updated version after removing all traces of the attack
<input type="checkbox"/>	Whether the security personnel have rebuilt the compromised systems, servers, databases, and networks
<input type="checkbox"/>	Whether the effectiveness of all countermeasures are validated
<input type="checkbox"/>	Whether there is migration of resources that are unaffected by the incident to the new systems
<input type="checkbox"/>	Whether the organization has improved the monitoring capabilities