Digital Forensic Readiness Checklist

Reserve Banks Information Technology Private Limited

Version: 1.0

Dated: 06th Jan, 2018

Author: ReBIT & PWC

Checklist

☐	Identify the business scenarios and various threats both external and internal.
☐	Identify potential sources and types of data – devices, applications, data bases
☐	Map the sources of data with threat.
☐	Identify the collection and retention requirement – Legal, Regulatory compliance
☐	Test and improve the forensic preservation, collection and chain of custody capability
☐	Awareness of SoC and IR team forensic capability
☐	Document evidence-based cases, describing the incident and its impact.
☐	Ensure legal review to facilitate appropriate action in response to an incident
☐	Test the sufficiency at regular intervals.

Applicable Standards

ISO 27037	ISO 27041	ISO 27042	ISO 27043
Guidelines for identification, collection, acquisition and preservation of digital evidence	Guidelines on assuring suitability and adequacy of incident investigation method	Guidelines for analysis and interpretation of digital evidence	Guidelines for incident investigation principles and processes