Incident Management Maturity Assessment

1. The incident management team should have senior management support and appointed authorities.
2. Incident management tabletop exercises are performed periodically.
3. IS policies must include formal incident management and response policy separately.
4. A public relations communication plan must be developed, and a relevant designated person must be appointed.
5. A team must be established to handle all types of security events.
6. Incidents are regularly communicated to higher management with data analytics to make them aware of incident tracking and monitoring stats.
7. The incident response process is documented with necessary steps and information.
8. Future improvement areas must be considered upon solving every incident. The response process must be updated based on a knowledge base. Lesson-learned meetings should be conducted by senior management after every major incident.
9. Entire incident management team members must know their roles and responsibilities.
10. A proper escalation matrix must be created and must be made aware to all team members.
11. Technical and physical controls must be in place to identify and detect all sorts of incidents (ATP, Zero days, Malware, Virus, Ransomware, etc.) that cover entire IT capabilities of an organization (OS, networking devices, server. Etc.).
12. Evidence of every incident must be securely preserved and documented.
13. Knowledge sharing exercises or meetings between cross-functional teams must be taken place periodically.
14. Every incident must be classified.
15. Post-incident recovery effectiveness must be analyzed and confirmed after solving every incident. It is essential to make sure the business is retrieved back to its original state and running smoothly.
16. Controls must be in place to contain incidents' artifacts to do further analysis and post-mortem (Sandboxing).