CREATED BY ADEOSUN PETER

1. Are Roles and Responsibility Being Defined in the Organisation?

. This gives the foundation to Foster partnership and Identify opportunities. And in Cyber recovery frame work in speeds up recovery process and stakeholders are trained in their role.

IF yes is Controls such as RCAI matrix is being used to define roles and responsibilities using a chat and this chat is defined by Accountability, Responsibility, Consulted and Informed.

1. Is there Reliable source of information for Organisation Assets.

The main goal of this control is creating a database of organisation assets. This will Give the recovery team a clear view of assets that are affected by attacks

If yes Are Controls of Reliable source of Information Assets implemented through various software like (SolarWinds N-Central by Solaris winds. Fresh Service by Fresh works, DEVICE42)

1. Are assets being Prioritised?

The rating of assets with consideration of their reliability, impact of failure. Categorising this asset will help in the recovery process, as the recovery plan will give importance to the most prioritized assets

If Yes Is Assets analysis carried out with the following

* Mission and customer impact
* Safety and environmental impact
* Ability to isolate single-point-failures
* Preventive maintenance (PM) history
* Corrective maintenance (CM) history
* Mean time between failures (MTBF) or “reliability”

Probability of failure

Spares lead time

* Asset replacement value
* Planned utilization rate

4. Is There a map of Organisation Dependencies?

The goal of organisation dependence is to define relationships between capacities required by roles and Organisations on the one hand, and services that realize them on the other hand

If yes

* Are Internal and External dependencies Identified.
* Does the analysis reflect the Information system (data dependency) and end point systems?

Are The following Method used in Defining Dependencies analysis?

* business impact analysis
* service/operational level agreements
* dependency maps

5. Are Service Level Agreement being mapped out for third parities

Organisation are increasing reliant on third party information technology service which includes: cloud Computing, Data backup, operating partners.  It is a drawn agreement between the service provider and its external and internal consumers Its entails documents that specifies what services the provider is compelled to meet. This can assist the organisation Recovery team in the event of a major cyber security attack.

IF yes

The following controls should be put in place when mapping out an SLA;

* Documenting specific security Objectives in agreements with third parties
* Measurement of cyber Security performance in third party agreements.
* Monitoring of Compliance with security objectives in agreements with third parties
* Cybersecurity Performance when selecting third parties

6. IS there a backup level Agreement? --

The aim in mapping out SLA for internal backup and recovery environment will entail all elements of infrastructure that can have precaution in the outstanding backup of recovery of critical business data

If yes does it include

1. San Network (fibber Channel, Iscsi)
2. Backup severs (masters or Media Severs)
3. Backup reporting Severs
4. Client Backup Software
5. Backup Client Priorities (Business Critical Nature of the Application Sever)
6. San Network (fibber Channel, Iscsi)
7. Ethernet Network (connections to Clients and Backup Severs)
8. Offsite /Internal Media (Storage Locations: How fast can you retrieve tapes)
9. Backup Libraries (Disk-based or Tape based)
10. Backup Operators
11. Data (Centre Environmental E.g  power supply’s , cabling and environment
12. control stations)
13. Offsite /Internal Media (Storage Locations: How fast can you retrieve tapes)

7 Do you have a recovery Metrics

: To ensure Delivering of all agreements in the SLA the metrics determines the responsibilities of infrastructures and IT teams Operation in the Level Agreements

If yes does it include

Groups that needs to be supported as part of the overall back and recovery Environment e.g. (Windows and Unix team, Operations and Implementation Teams, Application and Database Teams, Facilities Team and Outside Vendors were applicable)

8 **Is the Personnel to carry out recovery plan Identified**

To be able to carry out effectively a recovery plan, criteria and associated plan need to be identified by the appropriate recovery personnel. theses personnel must understand their roles and responsibility

If yes Recovery plan personnel roles must categorise as follows

Management

**Recovery Coordinator:**

**Business Analysist**:

**Infrastructure Team**:

* **Servers/Storage/Databases**
* **Networks/Telecom**
* **IT Applications**

**9. Are Specific recovery details and procedures mapped out?**

Specific recovery Details should account for both technical and Nod technical procedures

**If yes**

**Technical Recovery Procedures should** include

I.Restoring system from clean backups

II.Replacing Compromised files with clean Versions

III.Installing patches

IV.Remediating software misconfiguration

Non-Technical Recovery Procedures should include

Business Process

IT Polices.

10. Is there **Out of band communications implemented**

Identifying out band communication in communicating with critical business including internal and external IT security stakeholder. during recovery process without using the existing system which can be compromised

**If yes**

**Are protocols such as FTP and TCP being used in such communications**

**11. Is there** Continuous Improvement implemented after the recovery Process

The plans policies and Procedures Created for recovery should be continually improved by Incorporating lesson Learned during recovery efforts

If yes The Security team should follow

Discovery: In this phase the recovery team disuses things that can be in proved through the recovery process such as communication or any technical or non-technical process. It is very important to obtain many viewpoints form team. This allows the team to see an issue more holistically

Validation Phase: This allows the test the suggestion from the Discovery phase and see if it can be implemented

Integration Phase: A lesson can be adapted or applied to the organisation during this phase.

Assessment Phase: phase the team determines whether the lesson was successfully integrated into the work. If the new lesson was only partially successful, there’s an opportunity to send it back to the prior step and revise it, before moving it to get revaluated. If the lesson is successfully implemented, the team considers it “learned” and it gets recorded in a repository that everyone has access to so others can refer to it when they face a similar experience.

12 Is there Requirments to Validating Recovery Capabilities.

If yes

The Requirements must include the following controls

Are backups Encrypted at rest as well as in transit?

Is there an established Recovery time objective and a Recovery point objective?

How long will it take to recovery from an attack?

Doe backup performance comply with any compliance need, client driven compliance or service requirements.

Where us data being hosted

Verifying data been backed is free form vulnerability and corruption

Aware of data replication, duplication and Redundancy

Backup strategy documented

Testing strategy on a regular basis

13 IS there Defined Effective Cyberattack playbook

It’s a compilation of effective information and process that can be played out to create a recovery plan and be prepared for different cybersecurity incidents.

If yes