High-Performance IT

Infrastructure Health Check

russell futcher .com

Infrastructure Health Check

Infrastructure Health Check Scope

A three-step approach is used for all Infrastructure assets under management.

1. Audit

The first step is an Infrastructure Audit of all Infrastructure assets producing an Asset Listing. Against each asset a quick risk assessment is made with each asset rated as either (High, Medium, Low) in terms of its risk of failure (for any reason) during the next 12 months. Added to this the word Replace is used to indicate that the asset needs to be replaced due to some technical fault or high failure rate or it is due or is past due its date for replacement. (i.e.: It has been fully depreciated and/or it no-longer forms part of the current Hardware Architecture plan)

2. Risk Assessment and Mitigation

A Risk Assessment listing is then produced for assets rated as High and a Risk Mitigation plan is then prepared to address each asset. Cost estimates coming out of this plan are fed into next year's Budget and where appropriate next year's Strategic Plan. High risk and Replace assets requiring immediate attention are flagged as Red and are immediately acted upon.

3. Budget impact

The next step is to use the Asset Listing to check on the accuracy and completeness of the IT Budget. This is done by ensuring each asset has an accompanying Maintenance Agreement (which may only apply to high value/critical assets) and a Systems Software Licensing Agreement and that each asset is covered in the Depreciation Schedules. Amendments are noted for input into next year's Budget.

1. Servers.	✓
Audit Listing	
Use a spreadsheet or a Configuration Management system to produce a hardware audit listing consisting of:	

1. Systems servers. Web servers. Applications servers. (Name, Location, Number)	
2. E-mail servers. Back-up servers. Other server types in use.	
3. Add server management software (Name) against each item.	
4. Add a maintenance/support agreement (Y/N) against each item.	
5. Add a systems software licensing agreement (Y/N) against each item.	
6. Add a risk assessment (H, M, L) against each item.	
7. Add 'Replace' against servers that are deemed High Risk and require immediate attention.	
Server Assessment	
Next answer the following questions:	
1. What server recovery processes exist?	
2. What is the average production server's failure rate? (Unplanned shutdown/unusable to users).	
3. How is server resource utilisation managed? (CPU, memory, and disk-space (used and free))	
4. Is there a formal process for server physical and logical installation?	
5. Is there a formal manual or automated process for server recovery?	
6. When was the last test of a restoration from a back-up completed?	
7. How are back-ups confirmed as complete?	
8. How often are full image restores used?	
9. Is the reinstallation of systems and applications software manual or automated?	
10. Is resource utilisation trending in place for critical systems?	
11. Are all servers included in the depreciation schedule?	
12. Are all servers covered by a maintenance agreement?	
13. Is critical infrastructure covered by high priority maintenance agreements?	
14. Do all Servers have a systems software licensing agreement?	
15. Has the infrastructure disaster recovery plan been tested?	

16. Is there a server refresh strategy in place?	
2. Desktops/Laptops/Mobile devices.	
Audit Listing	
Use a spreadsheet or a Configuration Management system to produce a hardware audit listing consisting of:	
1. List all desktops, laptops, and mobile devices (by unit or group by type).	
2. Add a maintenance/support agreement (Y/N) against each item.	
3. Add a systems software licensing agreement (Y/N) against each item.	
4. Add a risk assessment (H, M, L) against each item.	
5. Add 'Replace' against servers that are deemed High Risk and require immediate attention.	
Desktops/Laptops/Mobile devices Assessment	
1. Is there a formal process for server physical and logical installation?	
2. How effective are Desktops/Laptops/Mobile devices service delivery and repair procedures?	
3. Is there a Desktops/Laptops/Mobile devices refresh strategy in place?	
4. Is the reinstallation of systems and applications software manual or automated?	
5. Are all Desktops/Laptops/Mobile devices covered by a maintenance agreement?	
3. Networking.	
Audit Listing	
Use a spreadsheet or a Configuration Management system to produce a hardware audit listing consisting of:	
1. List all routers (by unit or group by type).	
2. List all switches (by unit or group by type).	
3. Maintenance/support agreements. (Y/N)	

4. Systems software licensing agreements. (Y/N)	
5. Risk assessment (H, M, L).	
6. Add 'Replace' against assets that are deemed High Risk and require immediate attention.	
Networking Assessment	
1. Is there a formal process for physical and logical installation?	
2. How quickly can a router or a switch be replaced?	
3. What are the router and switch failure rates?	
4. Is critical infrastructure covered by high priority maintenance agreements?	
5. Are patches up to date?	
6. Is the reinstallation of systems software manual or automated?	
7. Are all assets covered by a maintenance agreement?	
4. DBMS.	
DBMS Assessment	
Use a spreadsheet to produce an audit listing consisting of:	
1. How many staff are involved with database administration?	
2. Are there user account and share management procedures in place?	
3. Are Administration services for active RDBMS in use?	
4. How is capacity management, managed?	
5. How is performance analysis/tuning conducted?	
6. Does a systems software upgrade strategy exist?	
7. Who owns and manages software license management?	
8. What vendor support arrangements are in place?	

5. Naming Standards.	
Often hardware does not have a formal naming standard, instead names of planets or mountains or similar are used which is not only unprofessional but can lead to a variety of problems. The Best Practice IT Standard is the use of a server, router and switch naming standard consisting of 'type' (for servers -web, system, print, production, application), 'location code' and an 'incremental number.' A good naming standard makes it easy to deploy, identify and filter through hardware farms, especially when you may have hundreds, or thousands of units deployed. There are important advantages re adopting a formal naming standard, one that scales as the population grows, namely:	
1. It speaks to the professionalism of the IT department.	
2. New staff can quickly learn to identify hardware types.	
3. Mistakes caused by selecting the wrong piece of hardware are far less likely.	
4. Disaster management benefits when staff and third parties need to identify and prioritise the hardware recovery sequence.	
Naming Standard Assessment	
Create a document to record.	
1. What is the current naming standard convention?	
2. How is it applied?	
3. Does the convention cover servers, routers, and switches?	
4. Is the convention professionally based or otherwise?	
6. Tools and Utilities.	
The Best Practice IT Standard is that all software tools and utilities are vendor supported with an OS, systems software and applications upgrade path. This is the only way to have confidence that common and consistent outcomes will be produced. Tools and utilities have a nasty habit of multiplying, especially when they are freely downloadable from the Web. Most technical and engineering staff have their own set of utilities for fixing problems as against a set of approved vendors supported products.	
Audit Listing	
Use a spreadsheet to produce an audit listing consisting of:	
1. List all software tools and utilities in use.	

2. List all scripts in use.	
3. List all SOE's in use.	
4. Flag each item as either (H, M, L) risk based on being vendor or non-vendor supported.	
5. Act on the high-risk items.	
Audit Assessment	
1. What tools/utilities redundancies exist? (Multiple types)	
2. What script redundancies exist? (Multiple versions)	
3. What tools, utilities and scripts can be removed?	
4. Should there be a policy of not downloading products from the Web?	
5. Is software distribution fully automated?	
6. Are production and development SOEs isolated from each other?	
7. Are their redundant SOEs, what can be removed?	

Build an Infrastructure Scope of works.

1. Collate all of the responses together.
2. Prepare a risk analysis for all hardware, software, and DBMS.
3. Act on risk mitigation actions from the risk assessment.
4. Update asset registers.
5. Update budget depreciation amounts and other asset related costs.
6. Review production servers with high failure rates. (Unplanned outages).
7. Establish server resource utilisation management. (CPU, memory, and disk-space (used and free))
8. Create a process for server recovery by type.
9. Create a hardware fleet upgrade strategy.
10. Create a systems software upgrade strategy.
11. Create a desktop refresh strategy.
12. Put in place database monitoring.
13. Breakdown the scope of works to a task level.
14. Fully automate software distribution.

15. Remove redundant, tools, utilities, and scripts.
16. Replace non-vendor supported products with vendor supported products.
17. Train staff on vendor supported products.
18. Standardise engineering toolsets.
19. Introduce a common naming convention for servers, routers, switches and migrate to over six months.
20. Breakdown the scope of works to task level.
21. Create a project schedule based on the tasks.