The MSSP Switching **Checklist**

12 areas to assess before choosing your next provider

Red Helix

Changing provider is an opportunity to reassess your technology estate, security controls and service model. Use this checklist to understand where your current arrangement stands, what has changed since the provider was appointed and what you should expect from the next one.

01 | Business and service fit

- [ ] Has your technology estate changed significantly since the current provider was appointed?
- [ ] Is the provider proactive, or predominantly reactive?
- [ ] Are you receiving strategic advice as well as operational support?
- [ ] Can the service scale with your organisation?

Consider: What do you need from your next provider that you are not getting today?

02 | Security capability

- [ ] Can the provider demonstrate how security controls operate in practice?
- [ ] How is security performance measured?
- [ ] Does the provider have a documented incident response capability?
- [ ] How are vulnerabilities identified and prioritised?

Look for: Evidence of capability, not simply a list of certifications or technologies.

03 | Security monitoring & detection

- [ ] Which endpoints, networks, cloud services and identities are covered?
- [ ] Are alerts investigated or simply forwarded?
- [ ] What happens outside normal working hours?
- [ ] Are critical alerts escalated within defined timeframes?

Ask: If a serious alert is generated at 2am, what happens next?

04 | Vulnerability & patch management

- [ ] How are critical vulnerabilities prioritised?
- [ ] Are unsupported and end-of-life systems identified?
- [ ] Is there a named owner for outstanding vulnerabilities?
- [ ] Are remediation timeframes defined?

During transition: Agree responsibility for every outstanding vulnerability before the handover.

05 | Identity and privileged access

- [ ] Have all current provider accounts been identified?
- [ ] Is least privilege applied?
- [ ] Can access be revoked promptly?
- [ ] Are privileged accounts documented?

During transition: Establish what access the new provider needs rather than replicating the incumbent's permissions.

Red Helix

06 | Security monitoring & detection

- [ ] Are restores tested?
- [ ] When was the last successful restore of a critical system?
- [ ] Are recovery time objectives defined?
- [ ] Are recovery point objectives defined?

Ask: Can the provider demonstrate that the recovery process works, rather than simply confirming that backups are running?

07 | Infrastructure & documentation

Before the transition, obtain and validate:

- [ ] Asset inventory
- [ ] Network diagrams
- [ ] Cloud environments and subscriptions
- [ ] Firewall configuration
- [ ] Known vulnerabilities
- [ ] Technical runbooks
- [ ] Licensing information
- [ ] End-of-life systems

Validate: Does the documentation reflect the live environment?

08 | Incident response

- [ ] Is there a documented incident response process?
- [ ] Has it been tested?
- [ ] Are escalation routes defined?
- [ ] Who decides when an event becomes an incident?

During transition: Agree who owns incidents discovered during or shortly after the handover.

09 | Reporting & governance

- [ ] Is security performance reported?
- [ ] Are vulnerabilities and remediation tracked?
- [ ] Are outstanding actions assigned to named owners?
- [ ] Are recurring issues identified?

Ask: Does the reporting help leadership understand exposure and make decisions, or does it mainly report activity?

10 | Technology lifecycle

- [ ] Are unsupported systems identified?
- [ ] Does the provider proactively identify technology that creates unnecessary risk?
- [ ] Is there a roadmap for addressing technical debt?
- [ ] Are legacy systems documented?

11 | Provider and supply chain risk

- [ ] Are critical subcontractors disclosed?
- [ ] Are disaster recovery arrangements tested?
- [ ] Are responsibilities clear if a critical third party fails?
- [ ] Does the provider assess its own suppliers?

Your provider becomes part of your supply chain. Understand the dependencies sitting behind the service you are buying.

12 | Contract and exit

- [ ] Are SLAs clearly defined?
- [ ] Is there a documented exit process?
- [ ] Are data, logs and documentation covered?
- [ ] Are renewal and termination provisions clear?

Red Helix

Compare your current provider with what you need next

Area	Current position	What needs to improve?	Requirement for next provider
Security monitoring			
Vulnerability management			
Patch management			
Privileged access			
Backup and recovery			
Incident response			
Reporting			
Service delivery			
Technology strategy			
Security governance			

The final test

> Before appointing your next provider, ask what will be measurably better after we switch? If the answer is clearer visibility, stronger security operations, better resilience, faster remediation, tighter access controls or more useful reporting, make those improvements explicit in the transition plan and contract.

A successful provider change should not simply transfer responsibility. It should raise the standard of the service you receive.

+44 (0)1296 397711

info@redhelix.co.uk

Phoenix House
Smeaton Close
Aylesbury
Buckinghamshire
HP19 8UW

redhelix.com