jumpcloud for MSPs™

# The MSP Compliance Checklist - UK Cyber Security & Resilience Bill

Are you ready to transition from "Service Provider" to "Critical Infrastructure"?

The new Cyber Security and Resilience Bill explicitly designates Managed Service Providers (MSPs) as critical nodes in the UK's digital supply chain. Use this checklist to benchmark your current security posture against the upcoming statutory requirements.

## The New Statutory Duties

The Bill introduces legal obligations that move beyond "best practice."

### ☐ Incident Reporting (The 24-Hour Rule)

**Requirement:** You must report significant incidents to the regulator (likely the Information Commissioner or NCSC) within **24 hours** of discovery, with a full report within **72 hours**.

***Gap Analysis:*** *Can you currently assess the scope and impact of a breach across all client tenants within 24 hours?*

### ☐ Risk Management Mandate

**Requirement:** MSPs must take "appropriate and proportionate measures" to manage risks to the network and information systems they rely on.

***Gap Analysis:*** *Do you have a consolidated view of risk (e.g., unpatched devices, shadow IT, disabled MFA) across your entire managed estate?*

### ☐ Supply Chain Transparency

**Requirement:** Regulators can now designate your own vendors as "Critical Suppliers," subjecting them to direct oversight.

***Gap Analysis:*** *Can you quickly audit and report on the security posture of the third-party tools (RMMs, PSAs) you use to manage clients?*

## Technical Readiness (The "Compliance Stack")

How to map your technology to the regulation using a unified approach (e.g., JumpCloud).

### 1. Identity & Access Control

☐ **Universal MFA Enforcement:** MFA must be enforced for all users, not just privileged admins.

***Solution:*** *Enforce phishing-resistant MFA/passwordless access across all endpoints and applications.*

☐ **Conditional Access Policies:** Access should be granted based on context (device trust, location), not just credentials.

***Solution:*** *Block access attempts from untrusted devices or high-risk geolocations automatically.*

### 2. Device Hygiene & Hardening

☐ **Automated Patching:** Unpatched vulnerabilities are a primary vector for supply chain attacks.

***Solution:*** *Automate OS and browser patching across Windows, macOS, and Linux fleets.*

☐ **Fleet-Wide Encryption:** Data on lost or stolen devices must be rendered inaccessible.

***Solution:*** *Enforce and report on BitLocker/FileVault encryption status for every managed device.*

### 3. Visibility & Forensics

☐ **Centralised Logging:** To meet the 24-hour reporting window, you cannot waste time scraping logs from disparate tools.

***Solution:*** *Consolidate authentication logs (Directory Insights) to immediately trace who accessed what, when, and from where.*

## Executive Accountability

### ☐ Board-Level Awareness:

Ensure your leadership (and your clients' leadership) understands that non-compliance can result in fines up to £17M or 4% of global turnover.

### ☐ Client Communication:

Proactively inform clients that you are aligning with the new "Critical Infrastructure" standards—this is a value-add, not just a cost center.

JumpCloud® is the AI-powered unified IT management platform designed to secure the modern workforce. By consolidating identity, device, and access management, JumpCloud provides intelligent, secure IT that scales from human users to autonomous AI agents. We help organizations around the globe eliminate complexity and turn AI risk into an optimized advantage, ensuring the right people and agents have secure access to the right resources at all times.



jumpcloud for MSPs™

Get Started