# 

## ACTIONABLE SECURITY CONFIGURATION CHECKLIST

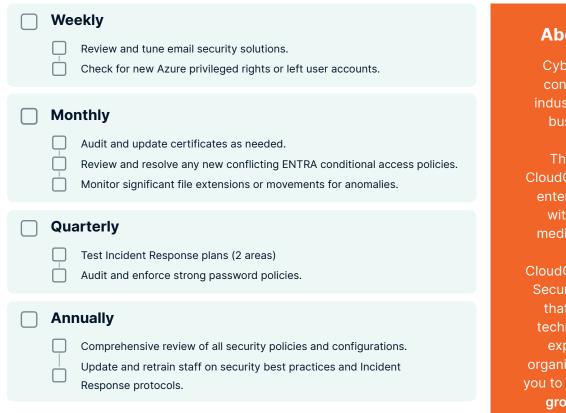
Businesses must continuously improve their cybersecurity posture, regardless of their investment level. Identifying and addressing exploitable gaps between different security products is crucial.

### **Recent Cybersecurity Events**



Even large organisations with significant investments face sophisticated cyber threats.

#### **Regular Maintenance Tasks**



#### About CloudGuard

Cybersecurity isn't just a concern for giants in the industry. It's a necessity for businesses of all sizes.

That's why we created CloudGuard. We want to bring enterprise-level protection within reach of small to medium-sized businesses.

CloudGuard offers a Managed Security Service ecosystem that combines the latest technology with UK-based experts to protect your organisation 24/7. This allows you to focus on what matters growing your business.

### 

Certificate Management
<ul> <li>Avoid using wildcard certificates for key public-facing services.</li> <li>Verify all public-facing services and protocols have correct, non-expired certificates.</li> </ul>
<ul> <li>Email Security</li> <li>Set active DMARC and DKIM policies</li> <li>Regularly tune email security solutions.</li> <li>Implement enhanced analytical rules to detect and prevent malicious content.</li> </ul>
<ul> <li>User Account Management</li> <li>Regularly audit and remove unused Azure privileged rights or left user accounts.</li> <li>Implement strict policies for account creation and deletion to avoid unnecessary privileged accounts.</li> </ul>
Microsoft ENTRA Policies     Review and resolve any conflicting ENTRA conditional access policies.
<ul> <li>File monitoring</li> <li>Implement monitoring for significant file extension changes or unusual file movement.</li> </ul>
<ul> <li>Incident Response</li> <li>Ensure Incident Response plans are updated and tested regularly. Pick 2 to test every 3 months.</li> </ul>
<ul> <li>Password Management</li> <li>Avoid using known weak passwords for any account.</li> <li>Do not use password storage in browser applications.</li> </ul>
<ul> <li>Application Registration</li> <li>Restrict App registration capabilities to authorised users only.</li> <li>Regularly review App registration permissions and adjust as necessary.</li> </ul>
<ul> <li>Multi-Factor Authentication (MFA)</li> <li>Avoid over-reliance on MFA as the sole method of security.</li> <li>Regularly review and update MFA policies to close any gaps.</li> <li>Ensure MFA policies are comprehensive and applied to all users and groups.</li> </ul>
Vulnerability Management Ensure all systems are regularly patched to address known vulnerabilities.
Have security concerns? We're here to help! $\rightarrow$ Contact Us

#### CloudGuard ®

www.cloudguard.ai | hello@cloudguard.ai | +44 (0) 161 504 3313 CloudGuard <sup>®</sup> is a registered trademark of CloudGuard Ltd in the United Kingdom