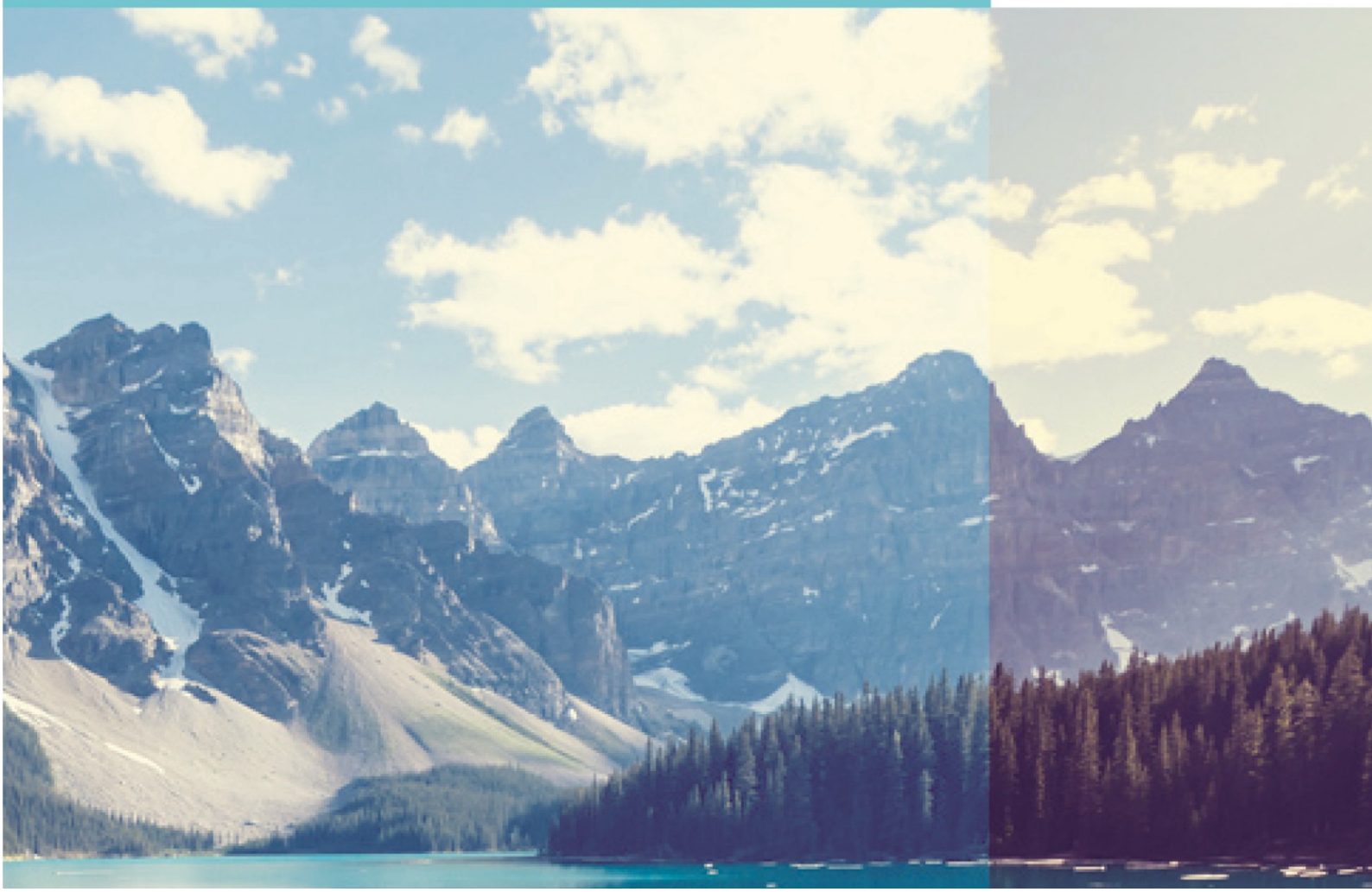
itps

intelligent technology. practical solutions.

Cyber Security Risk Assessment

Service Level Description



Crown Commercial Service Supplier

CYBER ESSENTIALS PLUS

IASME CYBER BASELINE

CYBER ESSENTIALS PLUS

bsi ISO 9001 Quality Management Systems CERTIFIED | ISO/IEC 20000-1 IT Service Management CERTIFIED | ISO/IEC 27001 Information Security Management CERTIFIED

Registered Office:

IT Professional Services Ltd
Angel House
Unit 5
Angel Park
Drum Industrial Estate
Chester-Le-Street
DH2 1AQ

http://www.itps.co.uk

Contents

Document Control

DOCUMENT TYPE:	**SERVICE LEVEL DEFINITION & DESCRIPTION**
DOCUMENT CLASSIFICATION:	**RESTRICTED**
DOCUMENT VERSION:	**V1.2**
DOCUMENT OWNER:	**ANDY LEE**
CREATION DATE:	**27TH JANUARY 2026**
PRODUCT OFFERING	**SECURITY** [OFFERING]
COMPONENT(S)	[COMPONENT]

Revision History

DATE	VERSION NUMBER	AUTHOR / AMENDED BY	DESCRIPTION OF AMENDMENTS
03/01/2024	1.0	Andy Lee	SLD created
28/09/2024	1.1	Simon Hopkin	SLD review
27/01/2026	1.2	Kirsty Porter	SLD Review

Distribution

NAME	ROLE	CONTACT NUMBERS

Document Review

This document will be reviewed and updated, when necessary, as stipulated below:

- ✓ As required to correct or enhance the content.
- ✓ Following changes to the ITIL or ISO quality systems standard as defined by ITPS.
- ✓ Following any organisation changes or restructuring.
- ✓ No longer than 12 months after the previous approval date.

1.0 Service Name & Reference ID

Cyber Security Risk Assessment

2.0 Service Overview

Our Cyber Security Assessment Tool (CSAT) assessments provide a comprehensive evaluation of your organisation's cybersecurity posture, covering both CIS (Centre for Internet Security) and NIS (Network and Information Security) standards. Through automated scans, manual inspections, and in-depth analysis, we assess your IT infrastructure, networks, and systems to identify vulnerabilities, weaknesses, and compliance gaps.

Our assessments utilise industry-leading methodologies and best practices to deliver actionable insights and recommendations tailored to your organisation's specific cybersecurity needs. By leveraging the CSAT assessments, you can strengthen your security defences, mitigate risks, and enhance overall resilience against cyber threats.

3.0 Business Benefit

- **Enhanced Security Posture:** Identify and address cybersecurity vulnerabilities and compliance gaps to strengthen your organisation's security posture.
- **Risk Mitigation:** Proactively identify and mitigate cybersecurity risks, reducing the likelihood and impact of cyberattacks.
- **Compliance Assurance:** Ensure compliance with industry standards and regulations, such as CIS and NIS, reducing the risk of fines and penalties.
- **Cost Savings:** Avoid potential financial losses associated with cybersecurity incidents by investing in proactive risk assessment and mitigation.
- **Enhanced Reputation:** Demonstrate a commitment to cybersecurity best practices and compliance, enhancing trust and confidence among customers, partners, and stakeholders.

4.0 Included Service Components

- **Initial Assessment:** Review of existing cybersecurity policies, procedures, and controls.
- **Automated Scans:** Utilisation of automated scanning tools to identify vulnerabilities and compliance gaps.
- **Manual Inspections:** Manual review of critical systems and configurations to uncover hidden security issues.
- **Risk Analysis:** Assessment of cybersecurity risks based on industry standards and best practices.
- **Compliance Evaluation:** Evaluation of compliance with CIS and NIS standards, as well as other relevant regulations.
- **Report and Recommendations:** Delivery of a comprehensive report outlining findings, recommendations, and remediation steps.

We offer two variations of the CSAT assessment:

Quick Scan

- Target Customer - SMB (Up-to 300 employees)
- Duration - 3 Days
- Purpose of the assessment
    - Do a quick check on the cybersecurity hygiene
    - Propose improvement actions based on actual data
    - Based on the CIS controls Implementation Group 1
    - Quick report and few customizations
- Scan Sources
    - Basic Automated Endpoint Scan
    - Local Active Directory
    - Email DNS check
    - Microsoft 365 environment
    - Limited datasets from the Azure tenant
    - Checked against CIS IG1 (basic security hygiene controls)

Full Scan

- Target Customer - Enterprise, Corporate and Top SMB (300+ employees)
- Duration - 5 Days
- Purpose of the assessment
    - Comprehensive cybersecurity assessment
    - Help to decide on new security initiatives based on facts
    - Align Business and IT management
    - Deployment and implementation plan
    - Based on the CIS controls Implementation Group 1, 2 and 3 – covering the full CIS scope.
- Scan Sources
    - Comprehensive Automated Endpoint Scan, including
    - Google Workspace and AWS are checked against the full CISv8 controls
    - Linux machines and network devices
    - Local Active Directory
    - Email DNS check
    - Microsoft 365 environment
    - Comprehensive scan of the Azure tenant
    - SharePoint on-premises
    - Checked against the full CISv8 controls

5.0 Service Exclusions

- Implementation of recommended security controls or remediation actions.
- Ongoing monitoring or management of cybersecurity controls beyond the assessment period.
- External factors affecting cybersecurity that are beyond the scope of the assessment.