PiSYS.net

# Vendor Risk and MSP Scrutiny Pack

We make IT easy

# Vendor Risk and MSP Scrutiny Pack

## How to Use This Pack

- Use **Part 1** to quickly score your suppliers on core cyber and governance risks.
- Use **Part 2** as a due diligence form to gather detailed information from suppliers.
- Use **Part 3** for MSPs, who require extra scrutiny and ongoing quarterly review.

This pack is designed to help your board, procurement team, and IT leads spot risks early and build resilience into your 2025 supply chain strategy.

# Part 1: Supplier Risk Scorecard

## Quick-check tool for any supplier

| Question | Response (Yes/No/Unsure) | Notes & Actions |
|---|---|---|
| Do they hold independent certification (ISO 27001, Cyber Essentials Plus)? | | |
| Do they provide an up-to-date security policy on request? | | |
| Is Multi-Factor Authentication (MFA) enforced across their systems? | | |
| Have they had a penetration test or vulnerability scan in the last 12 months? | | |
| Do they have a documented incident response plan? | | |
| Do they comply with GDPR and disclose how data is stored and processed? | | |
| Are data transfers encrypted end-to-end? | | |
| Do they have a tested disaster recovery or business continuity plan? | | |
| Do they agree to regular audits or reviews? | | |
| Are subcontractors disclosed and held to the same standards? | | |

**Scoring:**

- 8–10 Yes = Low risk
- 4–7 Yes = Medium risk — review actions required
- 0–3 Yes = High risk — urgent intervention needed

# Part 2: Example Supplier Due Diligence Form

**Content to request detailed information from suppliers**

## A. Company Information

- Legal entity name
- Company registration number
- Registered address
- Contact details

## B. Certification & Quality

- ISO 9001 / 14001 / 27001 held? (Attach certificates)
- Cyber Essentials Plus held? (Attach certificate)
- Other relevant accreditations

## C. Insurance

- Employers' Liability
- Public Liability
- Professional Indemnity
- (include insurer, policy number, expiry dates)

## D. Regulatory Compliance

- GDPR / Data Protection compliance
- WEEE, REACH, CE/UKCA (if applicable)
- Modern Slavery Act statement

## E. Data Protection & Security

- Where will client data be stored (country, provider)?
- Encryption methods in place
- Incident notification procedure
- Incident response plan (attached)

## F. Declaration

- Completed by: [Name / Title / Date / Signature]

# Part 3: MSP Scrutiny

## Apply additional due diligence to your MSP — they manage your data and systems directly.

### MSP Scrutiny Questions

| Question | Response (Yes/No/Unsure) | Notes & Actions |
|---|---|---|
| Is the MSP independently certified to ISO 27001? | | |
| Do they also hold Cyber Essentials Plus? | | |
| Do they provide quarterly risk or incident reports? | | |
| Do they run 24/7 monitoring and patch management? | | |
| Have they provided a technology roadmap in the last 12 months? | | |
| Do they evidence continuous improvement (e.g. audit results, new controls)? | | |

# Part 4: Quarterly Business Review Template

**Data required from MSP:**

- Incident reports (last quarter)
- Ticket volumes and resolution times
- Patch compliance rates
- Downtime / availability metrics
- Upcoming risks or emerging threats

**Decision Tree:**

- Risk ↑ = Escalate to board, update roadmap
- Risk steady = Maintain review
- Risk ↓ = Consider expanding engagement

| Quarter | Key Risks | Agreed Actions | Deadline | Owner |
|---|---|---|---|---|
| **Q1** | | | | |
| **Q2** | | | | |
| **Q3** | | | | |
| **Q4** | | | | |

# Get a 2nd Opinion

**Next Steps**

1. Complete the scorecard for all suppliers.
2. Send the due diligence form to high-risk or critical suppliers.
3. Apply additional scrutiny to your MSP using the quarterly review template.

PiSYS is one of the few MSPs in Wales certified to ISO 27001. Our controls are independently audited, so you can benchmark us with confidence.

Book a complimentary Security Assurance Call with PiSYS. We'll review your supplier risk results and help shape your 2025 resilience plan.

BOOK NOW

# Let's talk...

**Contact me directly:**
**Steve** Bain
MD PiSYS.net
steve@pisys.net

**CALL:** 01792 464748
**EMAIL:** hello@pisys.net
**WEBSITE:** www.pisys.net