cybercert®

https://cybercert.ai

Supplier Cybersecurity Assurance Schedule

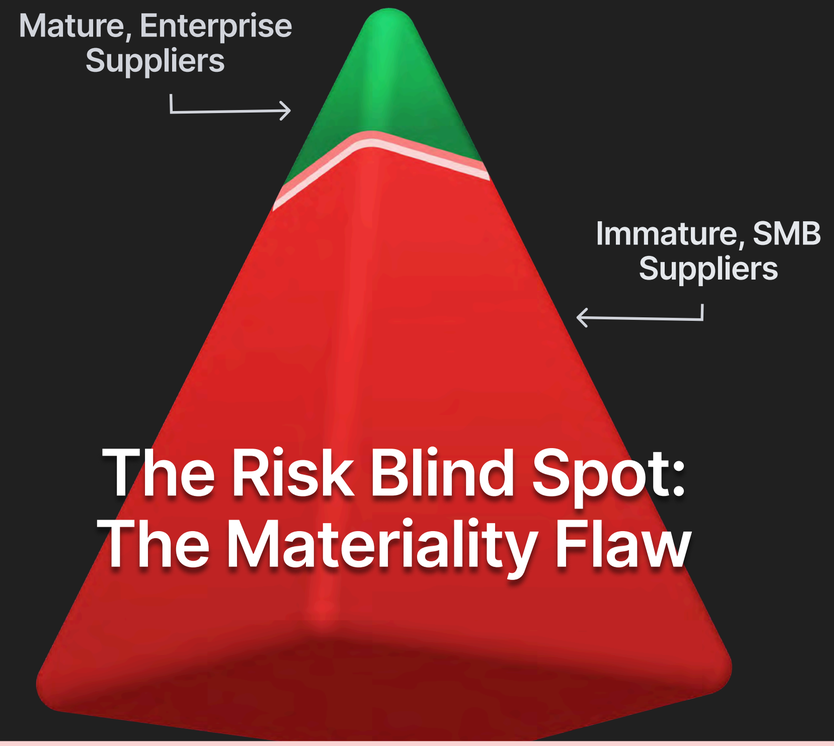
Risk-Based 2-Tier Model

THE PROBLEM:

Traditional TPCRM Fails 95% of the Supply Chain.

Traditional Third-Party Cyber Risk Management (TPCRM) is focused almost exclusively on intensive, manual audits and assessments for a few Tier 1 (Enterprise/High-Risk) vendors.

- This approach ignores the vast majority of suppliers (up to 95% of the supply chain), where critical supplier attacks are actually happening.
- The complex, resource-intensive nature of enterprise-level audits (like ISO/SOC 2) is not fit-for-purpose for the 95% who lack the resources and cyber maturity to comply.

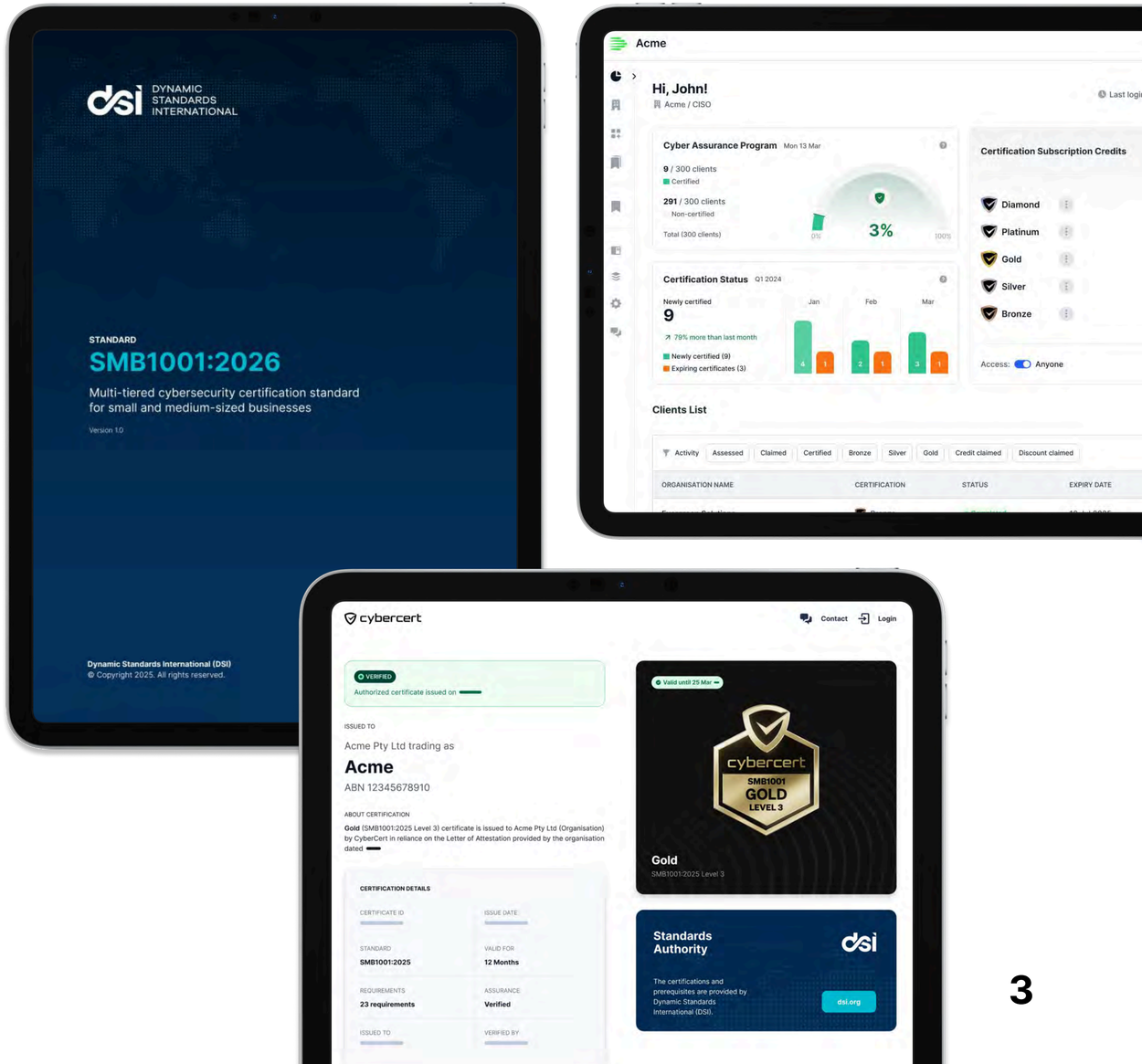


This creates a dangerous "Materiality" assumption, which rationalizes ignoring smaller vendors. The strategy is fundamentally flawed because the aggregate risk across thousands of seemingly "immaterial" SMB suppliers poses a massive, unaddressed threat to the entire supply chain.

THE SOLUTION:

Certification for Every Supplier.

A predictable, scalable, 2-Tiered approach that provides the right level of assurance for every supplier segment:



1 **Tier 1: Enterprise Suppliers**

High-assurance certifications and audits, enhanced by automation and data validation.

2 **Tier 2: SMB Suppliers**

A standardized, proportionate certification (DSI SMB1001).

Why Ignoring the SMB Supplier Segment is a Flawed Strategy.

While the enterprise solution addresses direct, high-risk exposure, the entire system breaks down without the SMB supplier solution. Traditional risk models fail the modern threat landscape in key ways:

The result is a gap where the most exploitable links are left unsecured.

Aggregate Risk

The massive, cumulative exposure introduced by thousands of unaddressed smaller vendors.

Shadow Risk

The failure to gain visibility into the most vulnerable part of the chain—the fourth or fifth-party SMB suppliers that an enterprise may not even know exist.

Proportionality Failure

Critical Nth-party SMB suppliers, which are often the initial point of failure, cannot realistically achieve or answer complex enterprise-grade assessments.

The Holistic Solution: 2-Tiered Certification.

To secure the entire chain, both tiers require a focus on certification and verifiable controls:

Enterprise Supplier Tier

Requires a robust, certifiable baseline like ISO/SOC 2, which can be paired with automation to check what's under the hood (data/evidence validation).

Long Tail SMB Supplier Tier

Requires a prescriptive, proportionate certification that validates the controls themselves, not the paperwork around them.

The successful modern TPCRM strategy is defined by proportionality, ensuring the assurance method aligns with the supplier's capacity and risk level.

	TIER 1: Enterprise Supplier Solution	TIER 2: SMB Supplier Solution
Primary Standard	**ISO/IEC 27001, SOC 2** (The baseline certification/audit language)	**DSI SMB1001** (A proportionate, tiered, certifiable standard)
Assurance Method	Automated TPCRM + Bespoke Audit/Evidence Review Required for complex, high-impact vendors	Verifiable Certification. Standardized tiers are accepted by policy, eliminating manual review for 95% of the chain
Outcome	High assurance, high cost, necessary for High-Risk/Tier 1 vendors Can semi-automate lower risk enterprise suppliers	Scalable, affordable assurance covering the majority of the supply chain
Scalability	**Low.** Relies on dedicated security teams and custom reviews for assurance validation	**High.** Standardized controls are verified through a digital platform and partner ecosystem, and accepted via procurement policy

The focus for Tier 1 suppliers is on maximizing the efficiency and trust of high-assurance standards like ISO 27001 and SOC 2.

OUTCOME:

Enterprise supplier assurance is still required, but it is now far more efficient and verifiable through technology, making it scalable for the higher risk Tier 1 vendors.

1. ISO 27001/SOC 2: The Baseline & Common Language

What it is:

The necessary, high-assurance standards used by large, complex, and high-risk vendors (Tier 1).

Key Challenge:

Traditional audits rely heavily on documentation (Statements of Applicability, audit reports), which are time-consuming to review and non-standardized.

2. The Modern Enhancement: Automation and Data Validation

What it is:

Modern TPCRM platforms automate the collection, correlation, and validation of evidence for these large vendors.

Key Characteristics:

- **Automated Evidence Packs:** The platform consumes and standardizes the evidence from the vendor's internal systems, reducing the need for manual review.
- **Risk Alignment:** The platform keeps the risk aligned by ensuring the self-assessment and the final audit align with the enterprise's acceptable controls.
- **Audit Confirmation:** The platform provides a digital layer for enterprises to confirm the controls under the hood are attested to via static documentation.

The focus for Tier 2 suppliers is on achieving verifiable scale for the thousands of long tail SMB suppliers.

OUTCOME:

SMB supplier assurance is democratized, but it is now proportionate and prescriptive through a tiered certification model, making verifiable security scalable for the vast ecosystem of Tier 2 vendors.

1. DSI SMB1001: The “Fit-For-Purpose” Standard

What it is:

Created by Dynamic Standards International (DSI), SMB1001 is an international, proportionate, multi-tiered, and certifiable set of cybersecurity controls specifically designed for the operational realities of SMB suppliers.

Key Characteristics:

- **Consistent & Non-Subjective:** Focuses on verifiably implemented controls (e.g., MFA, backups, incident response, supply chain).
- **Tiered Maturity Model:** Translates to Bronze, Silver, Gold, Platinum, and Diamond CyberCert tiers to scale requirements based on the SMB supplier’s risk profile.
- **Prescriptive:** Tells the SMB supplier exactly what to do, eliminating the complexity and documentation burden of enterprise standards.

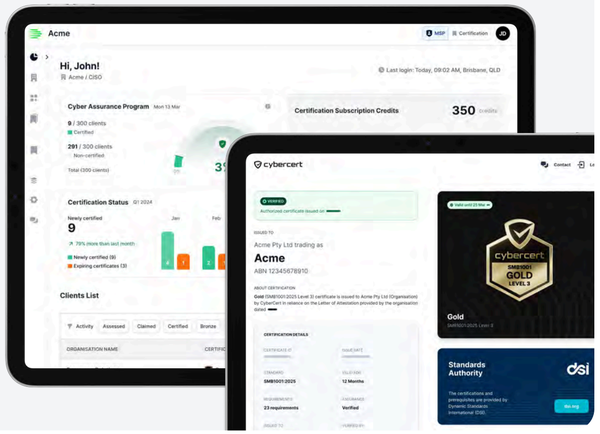
2. CyberCert: The Platform & Assurance Body

What it is:

The digital platform that manages the SMB supplier certification process, verifies controls, and delivers the assurance status.

Key Characteristics:

- **Key Function:** Provides the verifiable, legally effective evidence to the Enterprise/Government, confirming the SMB supplier has met the required SMB1001 tier.
- **The Go-To:** The singular certification body where the ecosystem converges to enable and validate compliance for the vast SMB segment.



This model ensures the assurance method is proportional, enabling reliance on certification instead of bespoke assessments for the majority of the supply chain.

TIER 1: Enterprise Supplier Risk Level		TIER 2: SMB Supplier Risk Level
ISO/IEC 27001, SOC 2 mandated Mandatory evidence validation; automated where possible	**High Cyber Risk**	SMB1001 (Platinum/Diamond Tiers) Highest assurance, independently verified
ISO/IEC 27001, SOC 2 preferred, with automated TPCRM Questionnaire alternative. Discretionary validation; automated where possible	**Medium Cyber Risk**	SMB1001 (Gold Tier) Covers the most common cyber compliance criteria for SMB suppliers
Light-touch self-assessment	**Low Cyber Risk**	SMB1001 (Bronze/Silver Tiers) Base hygiene at Bronze, Cyber Insurable at Silver

The 2-Tiered Model

The only way to achieve true Whole-of-Supply-Chain Cyber Assurance.

TIER 1:
Enterprise Supplier Solution

Features

Efficiency & Deep Validation: Automate the assessment of complex enterprises to confirm control alignment.

Delivery: TPCRM platform integration with audit/evidence systems.

Assurance: Customized audit reports/SoAs reviewed by TPRM platform for verification.

TIER 2:
SMB Supplier Solution

Features

Scale & Consistency: Provide a predictable, certifiable solution for thousands of vendors.

Delivery: Assurance delivered via the existing Technical Support Specialist (TSS) ecosystem.

› https://partners.cybercert.ai

Assurance:
Fixed, non-subjective controls Director attestation (all levels) with independent assurance (Tier 4 & 5).

Win-Win

Eliminating Friction for the Largest Attack Surface.

OUTCOME:

Crucially, this mechanism removes even more friction: SMB suppliers can also pay directly, which is still incredibly cheap and proportionate to their size and maturity, ensuring universal adoption options.

Enterprise/Government Cost Reduction

The operational cost of gaining assurance from thousands of SMB suppliers is virtually eliminated. This is achieved by simply accepting the SMB1001 certification into procurement policies.

Ecosystem-Powered Funding & Flexible Pathways

The certification cost for the SMB supplier is commonly funded by Technology Vendors or Cyber Insurance Brokers/Carriers, providing $0 certification pathways to SMBs.

Sponsors

Sponsors remove the certification paywall, lead with outcomes, and gain line-of-sight ROI.

Sponsored pathways to get you and your SMBs cyber certified.

MSPs

MSPs grow by acting as the implementers for the required standardized controls.

cybercert®

Accept the 2-Tiered TPCRM Model to achieve genuine, whole-of-supply-chain risk reduction.

Follow next steps below for Enterprise & Government Procurement.
Or visit our website for more information: cybercert.ai

Formal Recognition:

Formally accept the CyberCert x SMB1001 standard as sufficient assurance for the entire SMB (Tier 2) segment of your supply chain.

Contract Integration

Integrate a clear acceptance of the tiered SMB1001 certification within procurement clauses for vendors below relevant size thresholds.

(See attached document: Example Cyber Procurement Clause with SMB1001)

Integrate TPCRM

Utilize existing TPRM solutions to automate the initial discovery and segregation of suppliers, routing Tier 1 vendors to the automated audit process and Tier 2 (SMB suppliers) directly to CyberCert for self-service certification.

Empower, Don't Mandate

Actively promote the CyberCert program as the proven, scalable pathway for SMB suppliers—the segment that makes up the overwhelming majority of suppliers and the largest attack surface.

Example Procurement Clause

(The "Lift and Shift" Mandate)

Disclaimer: this is for informational purposes only and is not a substitute for professional advice.

cybercert®

1. Cybersecurity and Information Security Requirements

This clause establishes the cybersecurity and information security obligations applicable to all Suppliers engaged by the Customer (the “Enterprise”).

It applies proportionally based on the Supplier’s assigned risk category:

- *High Risk*,
- *Medium Risk*, or
- *Low Risk*;

as determined by the Enterprise’s risk assessment framework and supported by the **Dynamic Standard International (DSI) Categorization Matrix** available at https://dsi.org/categorization-matrix.

The purpose of these requirements is to ensure that Suppliers implement and maintain security controls commensurate with the sensitivity of the information handled, the criticality of the services provided, and the potential impact to the Enterprise.

2. 2-Tier Supplier Model

To ensure effective and proportional cyber risk management across the entire supply chain, we adopt a “2-Tier Supplier Model”.

By distinguishing between our complex enterprise suppliers and our Small and Medium Business (SMB) suppliers, this model provides a “whole-of-supply-chain” cyber risk management strategy that aligns assurance requirements with our supplier’s organizational maturity and scale.

The suppliers are categorized as follows:

- **Tier 1 (Enterprise Suppliers)**
  Complex enterprise suppliers requiring ISO/SOC2-level certification, or alignment - depending on risk classification - supported by automated evidence validation to confirm control consistency.
- **Tier 2 (SMB Suppliers)**
  Small and mid-sized suppliers certified to the prescriptive SMB1001 standard, delivering scalable, non-subjective, certifiable proof of proportionate security across the long-tail of the supply chain.

3. General Requirements

All Suppliers, regardless of tier, must:

a) Implement and maintain reasonable and proportionate cybersecurity measures to protect against unauthorised access, disclosure, loss, or compromise of Enterprise data.
b) Promptly notify the Enterprise of any actual or suspected cyber incident, data breach, or security compromise affecting services or data under this Agreement.
c) Cooperate fully with any Enterprise investigation, audit, or remediation activity related to cybersecurity.
d) Ensure subcontractors and affiliates engaged in delivery of the contracted services adhere to equivalent standards.

4. Risk-Based Cybersecurity Requirements by Supplier Tier

4.1 High Risk Suppliers

High Risk Suppliers are defined as those whose products or services:

- Process or store sensitive, regulated, or personal information on behalf of the Enterprise; or
- Provide mission-critical functions that cannot be replaced or substituted within seven (7) days; or\
- Have privileged access to the Enterprise’s internal systems, data, or networks.

4.1.1 Requirements for Tier 1 – High Risk Enterprise Suppliers

a) Must demonstrate compliance with one of the following:
   - ISO/IEC 27001 certification; or
   - SOC 2 Type II report; or
   - Equivalent internationally recognised standard approved by the Enterprise; or
   - Must complete the Enterprise Supplier Cybersecurity Questionnaire on request and maintain updated responses throughout the contract term.

b) May be subject to **audit, remote assessment, or onsite verification** by the Enterprise or its appointed assessor at any time during the contract term and prior to service commencement.
c) Must remediate any deficiencies identified through audit or questionnaire findings within a mutually agreed timeframe.

4.1.2 Requirements for Tier 2 – High Risk SMB Suppliers

a) Must demonstrate compliance with:
   - **Platinum or Diamond SMB1001 Certification** issued by CyberCert as defined in the DSI Categorization Matrix.

b) May be subject to **audit, remote assessment, or onsite verification** by the Enterprise or its appointed assessor at any time during the contract term and prior to service commencement.
c) Must remediate any deficiencies identified through audit or questionnaire findings within a mutually agreed timeframe.

4.2 Medium Risk Suppliers

Medium Risk Suppliers are defined as those whose products or services:

- Interact with Enterprise systems or information but do not directly manage or store regulated data; or
- Support operations that are important but not business-critical; and
- Can be replaced or substituted within seven (7) to thirty (30) days.

4.2.1 Requirements for Tier 1 – Medium Risk Enterprise Suppliers

a) Must provide evidence of cybersecurity maturity by:
   - Completing the Enterprise Supplier Cybersecurity Questionnaire.

b) May be subject to **random audits or assurance reviews** by the Enterprise or its appointed assessor.
c) Must maintain controls in accordance with an industry standard governance model (e.g. ISO 27001, NIST CSF).

4.2.2 Requirements for Tier 2 – Medium Risk SMB Suppliers

a) Must provide evidence of cybersecurity maturity by:
   - Holding a **CyberCert Gold or higher SMB1001 Certification**, as defined by the DSI Categorization Matrix.

b) May be subject to **random audits or assurance reviews** by the Enterprise or its appointed assessor.

4.3 Low Risk Suppliers

Low Risk Suppliers are defined as those whose products or services:

- Have no access to sensitive, regulated, or personal information;
- Are not critical to business continuity; and
- Can be replaced within thirty (30) days or more without material impact.

4.3.1 Requirements for Tier 1 – Low Risk Enterprise Suppliers

a) Must complete an **annual cybersecurity attestation** confirming implementation of basic safeguards (e.g., strong passwords, patching, antivirus, backups, MFA).
b) May be subject to **spot-check audits** at the Enterprise's discretion.

4.3.2 Requirements for Tier 2 – SMB Suppliers

a) Must hold at minimum a **CyberCert Bronze or Silver SMB1001 Certification** (as per the DSI Categorization Matrix), or alternatively provide a completed reduced set of cyber questions as provided by the Enterprise.
b) May be subject to **spot-check audits** at the Enterprise's discretion.

5. Evidence and Verification

Suppliers must provide current certificates, attestations, or completed questionnaires within ten (10) business days of request.

Failure to maintain compliance with these obligations, or refusal to provide evidence, may constitute a material breach of contract and grounds for suspension or termination.

6. Continuous Improvement

The Enterprise and Supplier acknowledge that cybersecurity standards and threats evolve.

Suppliers shall review and update their security controls and certifications annually or as required to remain aligned with current best practice and the SMB1001:2025 standard or its successors.

7. Definitions

For the purpose of this clause:

CyberCert means the independent certification body authorised to certify organisations against the SMB1001 international cybersecurity standard. https://cybercert.ai

DSI Categorization Matrix defines the criteria by which suppliers are classified by size, risk, and criticality for certification equivalence. https://dsi.org/categorization-matrix

Supplier Cybersecurity Questionnaire means the assessment form provided by the Enterprise to collect and validate supplier control information. May be provided by an enterprise technology solution.

Enterprise is characterized by size, capability needed to manage cyber risk at scale, its complexity, and governance maturity – requiring risk management practices that exceed what is proportionate or feasible for SMBs.

Common core attributes that define an enterprise:

- **Scale:** Typically, 1,000+ employees or equivalent operational footprint.
- **Dedicated Security & GRC Functions:** Full-time roles responsible for governance, risk management, compliance, incident response, and assurance activities.
- **Structured Governance:** Formal committees, policies, and reporting lines, including board-level oversight of cyber and operational risk.
- **Mature Risk Management:** A maintained risk register, ongoing threat assessment, internal audit cycles, and capacity to manage complex control environments.
- **Regulatory Exposure:** Operates across multiple jurisdictions or sectors requiring demonstrable scope-based compliance (e.g., ISO, SOC 2, PCI-DSS, sector-specific law).
- **Budget & Capacity:** Financial resources to sustain continuous governance, monitoring, and improvement at scale.

Small or Medium Business (SMB) The term ‘SMB’ can have varying definitions across different regions and economies. SMB1001 is a globally applicable standard. To ensure clarity and facilitate adoption by organizations of all sizes, the SMB1001 standard provides guidance using:

1) employee count,
2) revenue/turnover ranges, and
3) as organizational capability and risk profile.

These ranges are intended to help organizations determine an appropriate starting point within the standard and are not intended to be strict categorizations or advice.

Guidance by Employee Count

The following employee count ranges are provided as general guidance for starting points and progression through the certification levels.

Note: These ranges are illustrative and should be considered in conjunction with revenue/turnover and organizational capability and risk profile.

- For organizations with fewer than 20 employees: Level 1 is the recommended starting point. While Level 3 would typically be the highest level most organizations in this range will aim for, depending on other factors, they could and possibly should progress all the way to Level 5.
- For organizations with 20-99 employees: Level 2 or 3 is the recommended starting point. While Level 3 would typically be the highest level most organizations in this range will aim for, depending on other factors, they could and possibly should progress all the way to Level 5.
- For organizations with 100-249 employees: Level 3 is the recommended starting point, and organizations in this range should aim to progress all the way through to Level 5.
- For organizations with 250-499 employees: Level 3 or 4 is the recommended starting point, and organizations in this range should aim to progress all the way through to Level 5.
- For organizations with 500+ employees: Level 3 or 4 is the recommended starting point, and organizations in this range should aim to progress all the way through to Level 5.

Guidance by Revenue / Turnover

The following revenue/turnover ranges are provided as general guidance for starting points and progression through the certification levels.

Note: The revenue/turnover ranges provided are initially framed with U.S. dollar (USD) values for illustrative purposes. However, it’s critical to understand that the economic context and purchasing power of $1 million USD can vary significantly across different countries and regions. A business with $1 million USD in annual turnover might be considered quite large in some economies (e.g., Vanuatu), while it might be truly “small” in others. These ranges are illustrative and should be considered in conjunction with employee count and organizational capability and risk profile.

- For organizations with less than $1 Million annual revenue/turnover: Level 1 is the recommended starting point. While Level 3 would typically be the highest level most organizations in this range will aim for, depending on other factors, they could and possibly should progress all the way to Level 5.
- For organizations with $1 Million - $10 Million annual revenue/turnover: Level 2 or 3 is the recommended starting point. While Level 3 would typically be the highest level most organizations in this range will aim for, depending on other factors, they could and possibly should progress all the way to Level 5.
- For organizations with $10 Million - $50 Million annual revenue/turnover: Level 3 or 4 is the recommended starting point, and organizations in this range should aim to progress all the way through to Level 5.

- For organizations with $50 Million - $250 Million annual revenue/turnover: Level 4 is the recommended starting point, and organizations in this range should aim to progress all the way through to Level 5.
- For organizations with over $250 Million annual revenue/turnover: Level 4 is the recommended starting point, and organizations in this range should aim to progress all the way through to Level 5.

Organizational Capability and Risk Profile

It is crucial to emphasize organizations should consider their specific circumstances, including:

- Industry: Some industries may require higher levels of security regardless of employee count or revenue.
- Data Sensitivity: Organizations handling highly sensitive data may need to achieve higher levels.
- Regulatory and Legislative Requirements: Compliance with specific national or international regulatory and legislative requirements (e.g., data protection laws, industry-specific regulations) may necessitate achieving certain certification levels, implementing specific controls, or require independent external audit.
- Risk Tolerance: Organizations with a low-risk tolerance may choose to pursue higher levels.
- Available Resources: Organizations should consider their financial and technical resources when determining the appropriate level.

