Digility
Secure Technology, Simplified

Acme Widgets Cyber & Information Risk Appetite

Illustrative example for a notional physical product vendor that designs its own products, has them made by contract manufacturers, and sells direct to customers online and through a small estate of own-brand stores. Turnover c.£60m; lean operation with limited working-capital headroom. All figures are illustrative and would be set by the Acme Widgets board.

Risk Appetite Scenarios

Risk Category	Description	Appetite
Financial Distress	Risks that could cause Acme Widgets to lose significant money, whether through direct financial loss, indirect loss such as consequential lost revenue, or increased exposure such as loss of insurance cover. Given limited working-capital headroom, a sudden cash shock is more dangerous than an equivalent loss spread over a year. Examples might be: • Subversion of payment or supplier-onboarding processes leading to irrecoverable transfer of funds to an unauthorised account (e.g. invoice redirection fraud on a contract manufacturer payment); • Compromise and ransom of data, systems or resources that would be intolerable, and therefore where the ransom is likely to be paid; • The indirect financial impact of business disruption that leads to lost orders, cancelled peak-season stock and lost revenue; • Poor security that breaches the terms of cyber insurance, leading to a claim being denied or reduced.	Above £2m: Near to Zero Between £250k and £2m: Averse Below £250k: Moderate
Operational Disruption	Disruption to the Minimum Viable Business (MVB) where its impact on sales and cash flow is sufficient to threaten the viability of the business. Core MVB scope is: • ERP system required for all stock management, order fulfilment and financial management (including supplier payments); • Warehouse management system required for warehouse stock control, picking, packing and dispatch; • E-commerce platform (website, checkout and payment gateway) required for all online sales, c.70% of revenue; • Point-of-sale and store systems required for in-person sales across the store estate; • Carrier and courier integration required to dispatch online orders. Disruption to other systems that would not present an immediate existential crisis but, if enduring, would start to have very significant impacts on business health within 2–4 weeks. Examples include: • Product lifecycle management (PLM) system holding product designs, specifications and bills of materials; • Supply chain planning and contract manufacturer portals used to place and track production orders; • Customer service and returns platform.	MVB halted for >2 weeks: Near to Zero >25% impact to sales for >1 week: Averse Else: Moderate

Acme Widgets is a notional company. Illustrative strawman prepared by Digility. All content Copyright © 2026 Digility Ltd

Risk Category	Description	Appetite
Product Integrity & Safety	Risks that the physical products Acme Widgets puts into customers' hands are unsafe, defective or counterfeit as a result of a cyber or information compromise. Examples might be: • Undetected modification of specifications, materials or tolerances in PLM, leading to defective or unsafe product being manufactured and shipped; • Compromise of a contract manufacturer leading to unauthorised production runs and grey-market or counterfeit Acme Widgets products; • A product safety issue requiring a public recall, with associated cost, regulatory scrutiny and reputational damage.	Safety-affecting product shipped to customers: Near to Zero Defective (non-safety) product reaching customers: Averse Else: Moderate
Brand / Reputational	Risks that could do long-term and/or widespread damage to the Acme Widgets brand and reputation. Examples might be: • Very public loss of a significant quantity (thousands) of customer personal details; • Systemic failure of the ordering or fulfilment system that could not be recovered and restored within 24–48 hours, particularly during peak trading; • Offensive content or malware deployed onto our website by malicious parties that distresses or damages our customers and is widely reported; • Believable non-Acme websites or marketplace listings passing off as genuine to defraud our customers, sell counterfeit products or otherwise do them harm; • Hijacking of Acme Widgets social media accounts used to post damaging content or scams.	Above threshold: Averse Below threshold: Moderate
Regulatory & Legislative Sanctions	Our regulatory exposure is light compared with sectors such as Financial Services and Utilities. The core exposures are UK GDPR (and international equivalents) regarding all personally identifiable information, PCI DSS for card payments, and product safety legislation. If we are unable to show that we had 'appropriate technical and organisational measures' to protect personal data, we could be subject to fines with consequential publicity, reputational damage and potential legal damages.	Employee and customer PII at scale (e.g. >10,000 records, or >500 if including special category data or payment card data): Averse Otherwise: Moderate
Intellectual Property	Risks to the designs, know-how and customer insight that differentiate Acme Widgets from lower-cost competitors. Examples might be: • The irrecoverable loss of current and future designs in PLM, delaying our ability to get product to market; • Theft of designs and launch to market by a competitor or rogue manufacturer, followed by accusations of copying when Acme Widgets launch; • The theft, deletion or modification of customer purchasing history and insight data.	Irrecoverable loss of designs: Averse Theft of designs: Moderate Customer insight data: Moderate

Acme Widgets is a notional company. Illustrative strawman prepared by Digility. All content Copyright © 2026 Digility Ltd

Posture

Appetite	Posture

Near to Zero
Risks that cannot be accepted outright.
All reasonable means should be applied to reduce the likelihood, and deliberate steps must be put in place in advance to mitigate the impact, enable recovery and protect the business in the event that it occurs.
	• Incidents believed to fall into this category will trigger the Acme Widgets Crisis Management Plan.
	• Mitigations will be a "whole business" solution involving reversionary modes of operation, leveraging diversity between store and online sales channels, designed-in graceful degradation of the business (e.g. manual order capture and dispatch from a reduced catalogue), integration of external resources (e.g. insurer incident response, alternative 3PL warehousing), and practised restoration and recovery.
	• In-scope systems must:
	  • Be Secure by Design, considering and documenting risks and building mitigations into the design to minimise the impact;
	  • Be regularly (minimum annually and on major change) tested for resistance to attack and recovery from compromise (e.g. penetration tests, restore and recovery exercises);
	  • Be monitored 24x7 for early indications that a threat is active;
	  • Have contingency plans to pre-emptively disrupt attempts to attack them when indications of heightened threat are present, even at the temporary expense of business efficiency (e.g. isolating MVB systems from non-MVB systems, suspending third-party remote access);
	  • In the event of an attack, apply the best endeavours of the business to minimise the impact (e.g. redeploying head-office and store staff to support reversionary processes, disconnecting all non-critical resources and services, shutting down the affected service);
	  • Have recovery plans supported by immutable backups of data and configuration, enabling them to be restored to a safe and accurate state (no more than 10 minutes' loss of data) within no more than 48 hours.
	• Changes to product specifications and bills of materials released to manufacturers require two-person approval and are integrity-checked against the master record before production.
	• A table-top exercise for a believable high-impact scenario (e.g. ransomware during peak trading) is run at least annually, and lessons learnt are used to refine processes and controls.
	• The wider business should recognise the imperative to protect against this, so that every member of staff considers their part in prevention, business continuity and recovery.
	• Systems are not to be exposed to any AI technologies unless the scope of exposure is minimised and limited to specific use cases, and a full risk assessment has been conducted.
	• Outsourced systems and critical suppliers (including contract manufacturers and 3PL partners) must either have equivalent levels of control assured with evidence annually, or alternative diverse suppliers should provide redundancy.
	The risk management plan describing the actions above, and the consequential residual risk, can only be accepted by the board.

Averse
There will be a balance between mitigating the risk, enabling the business and avoiding disproportionate cost, but that balance should be struck with evidence and
	• In-scope systems must:
	  • Be Secure by Design, considering and documenting key risks and building mitigations into the design to minimise the likelihood and/or impact;
	  • Be periodically (on major change) tested for resistance to attack and recovery from compromise (e.g. penetration tests, restore and recovery exercises);
	  • Be monitored for malicious and suspicious activity;
	  • Have documented procedures to follow for the most likely scenarios;

Acme Widgets is a notional company. Illustrative strawman prepared by Digility. All content Copyright © 2026 Digility Ltd

Appetite	Posture
consideration. Acceptance by the business must recognise that the risk may materialise, and consider what actions would be taken and what consequences felt.	• Have recovery plans supported by immutable backups of data and configuration, enabling them to be restored to a safe and accurate state (no more than 60 minutes' loss of data) within no more than 7 days. • Outsourced systems and suppliers must have their security and resilience assured with evidence every two years. • AI technologies may be used, but the use cases are to be defined, the vendors subject to supplier assurance and control review, and controls applied to ensure the technologies cannot exceed that scope. **The COO has the authority to sign off the risk management plan and residual risk.**
Moderate Standard controls are designed to balance these risks with business flexibility and agility.	• The standard Acme Widgets controls are consistently applied. • A subset of systems is periodically audited and tested (20% annually). • Suppliers of outsourced systems should have been through a standard technology vendor assurance review when onboarded, and at least every 5 years or on change of control. • Approved AI technologies can be employed within the framework specified in the AI policy. **Residual risk is considered in aggregate. The CTO has the authority to approve a system's non-compliance with a standard control.**

Acme Widgets is a notional company. Illustrative strawman prepared by Digility. All content Copyright © 2026 Digility Ltd