SURERIGHT
Growth through compliance

Whitepaper:

The Hidden Risks Your Business Can’t Afford to Ignore (And How to Fix Them)

Scan me to book a discovery call.

The Cost of Inaction: Why SMEs Must Prioritise Risk Management

Small and medium-sized enterprises (SMEs) are particularly vulnerable to business risks due to their limited resources and often informal approach to risk management. Research shows that approximately 60% of small businesses cease operations within six months of experiencing a cyberattack, illustrating the devastating impact of inadequate preparation for operational risks (Small Business Trends, 2023). Furthermore, a study by the European Central Bank found that during the COVID-19 pandemic, SME failure rates increased by 9.1 percentage points, equating to 4.6% of private sector employment, due to their inability to withstand financial shocks (ECB, 2021).

These statistics highlight the critical need for SMEs to adopt proactive risk management strategies to protect their operations, maintain customer trust, and ensure long-term sustainability.

References
European Central Bank (2021). More than 900,000 UK small businesses ‘at risk’ of failing by early April. [online] Available at: https://www.ecb.europa.eu [Accessed 5 Dec. 2024].
Small Business Trends (2023). 60 Percent of Small Businesses Fail After a Cyber Attack. [online] Available at: https://smallbiztrends.com [Accessed 5 Dec. 2024].

Operational Blind Spots

Understanding the Risk

Operational blind spots are hidden vulnerabilities in your processes or supply chains that can lead to unexpected disruptions. These could be anything from an over-reliance on a single supplier to a lack of documented procedures for key roles. An easy way to analyse this for your business is to get to grips with single points of failures (SPOF).

Common Examples of Operational Blind Spots:

- Solely relying on one supplier for critical materials.
- No succession planning for essential staff roles.
- Lack of redundancy for IT systems or key equipment.

Operational blind spots can cause:

- **Customer Dissatisfaction:** Delayed deliveries or services.
- **Financial Strain:** Emergency costs to address sudden failures.
- **Reputation Damage:** Losing customer trust over repeated disruptions.

How to Mitigate This Risk

Conduct a Comprehensive Risk Assessment

1. Map out your key business processes and dependencies.
2. Identify single points of failure (e.g., critical suppliers or systems).
3. Develop Contingency Plans
4. Build redundancy into your supply chain.
5. Create handover guides for key roles to ensure continuity.
6. Implement ISO 22301 (Business Continuity)

This standard provides a framework for identifying operational risks and creating resilience strategies.

Quick Win: Supplier Audit

Audit your suppliers for financial stability, delivery reliability, and contingency plans. Diversify suppliers where possible to reduce reliance on any single source.

These statistics highlight the critical need for SMEs to adopt proactive risk management strategies to protect their operations, maintain customer trust, and ensure long-term sustainability.

Compliance Shortcuts (not a good thing)

Understanding the Risk

Compliance can often feel like a bureaucratic burden, but failing to adhere to regulations is far more costly. Many SMEs unintentionally cut corners, especially when they don’t have a dedicated compliance officer.

Common Compliance Risks:

- Outdated health and safety protocols.
- Ignorance of evolving data protection laws like GDPR.
- Poor documentation for quality management systems.

The Consequences

Compliance shortcuts lead to:

- **Fines and Legal Action:** Regulatory breaches can result in heavy financial penalties.
- **Operational Shutdowns**: Non-compliance may force temporary closures during investigations.
- **Reputational Loss:** Customers and partners may lose confidence in your business.

How to Mitigate This Risk

Adopt a Compliance Framework

- Implement standards such as ISO 45001 for safety or ISO 9001 for quality to maintain compliance systematically.

Schedule Regular Audits

- Internal and external audits help identify gaps and ensure continual improvement.
- Invest in Employee Training
- Ensure your team understands compliance requirements relevant to their roles.

Quick Win: Build a Compliance Calendar

Create a compliance calendar with key deadlines, audits, and policy reviews. Assign ownership for each task to ensure accountability.

Cybersecurity Gaps

Understanding the Risk

Many business owners mistakenly believe their company is too small to attract cyberattacks. In reality, SMEs are prime targets because attackers know they often lack robust defences. According to the UK Government 50% of businesses within 2024 experienced Cyber Security Breaches.

Common Cybersecurity Vulnerabilities:

- Weak passwords and lack of multi-factor authentication.
- Unpatched software vulnerabilities.
- Employees untrained in recognising phishing scams.

The Consequences

A cybersecurity breach can result in:

- **Data Breaches:** Compromising customer or employee information.
- **Financial Loss:** Paying ransoms or losing funds to fraud.
- **Regulatory Penalties:** Non-compliance with data protection laws like GDPR.

How to Mitigate This Risk

- Invest in Cybersecurity Basics
- Implement firewalls, antivirus software, and regular system updates.
- Use multi-factor authentication for all critical accounts.
- Train Your Employees
- implement ISO 27001 (IT and Data Security)
- Implement Cyber Essentials and Cyber Essentials Plus
- Run regular workshops on identifying phishing emails and other common threats.
- Develop an Incident Response Plan such as a Business Continuity or Serious Incident Management Plan (SIMP)
- Outline step-by-step actions to take in the event of a cyberattack.

Quick Win: Back-Up Your Data

Set up automatic daily backups for all critical data and test your restoration process quarterly.

Common Cybersecurity Vulnerabilities

- Weak passwords and lack of multi-factor authentication.
- Unpatched software vulnerabilities.
- Employees untrained in recognising phishing scams.

The Consequences

A cybersecurity breach can result in:

- Data Breaches: Compromising customer or employee information.
- Financial Loss: Paying ransoms or losing funds to fraud.
- Regulatory Penalties: Non-compliance with data protection laws like GDPR.

How to Mitigate This Risk

- Invest in Cybersecurity Basics
- Implement firewalls, antivirus software, and regular system updates.
- Use multi-factor authentication for all critical accounts.
- Train Your Employees
- Run regular workshops on identifying phishing emails and other common threats.
- Develop an Incident Response Plan
- Outline step-by-step actions to take in the event of a cyberattack.

Quick Win: Back-Up Your Data

Set up automatic daily backups for all critical data and test your restoration process quarterly.

Inefficient Processes

Understanding the Risk

Inefficient processes are silent profit killers. Whether it's manual data entry, outdated workflows, or unnecessary meetings, these inefficiencies waste time and money.

Common Inefficiencies in SMEs:

- Relying on manual invoicing or inventory tracking.
- Disorganised communication between departments.
- Redundant or overly complex approval processes.

The Consequences

Higher Costs: Paying for avoidable labour or errors.
Lower Productivity: Time wasted on repetitive tasks.
Employee Frustration: Reduced morale due to inefficient systems.

How to Mitigate This Risk

- Streamline Processes
- Use Lean principles to eliminate waste.
- Automate repetitive tasks with digital tools.
- Adopt ISO 9001

Invest in Technology

Tools like project management software (e.g., Trello or Asana) can improve collaboration and task tracking.

Quick Win: Automate One Process

Identify one manual task (e.g., invoicing) and replace it with an automated solution.

Cultural Disconnects

Understanding the Risk

Your workplace culture directly impacts employee engagement, productivity, and safety. A disconnect between leadership and staff can lead to miscommunication, low morale, and poor performance.

Signs of Cultural Disconnects:

- High turnover rates or absenteeism.
- Resistance to safety protocols or new initiatives.
- Lack of innovation and collaboration.

The Consequences

- Reduced Productivity: Disengaged employees are less efficient.
- Higher Risk of Incidents: Employees who feel undervalued are less likely to follow safety protocols.
- Loss of Talent: High turnover costs both time and money.

How to Mitigate This Risk

- Foster Open Communication
- Regularly seek employee feedback through surveys or meetings.
- Invest in Training and Development
- Celebrate Success

Quick Win: Host a Feedback Session

Organise a 30-minute team meeting to gather input on one area of improvement and implement at least one suggestion.

Case Study: Resilience in Action

Client: XYZ Construction Ltd
Problem: Frequent project delays caused by supplier issues and poor communication.
Solution:

- Conducted a risk assessment to identify operational blind spots.
- Implemented ISO 9001 to improve process efficiency.
- Trained employees to improve workplace culture and engagement.

- Results:
- 35% reduction in project delays.
- Improved team morale and client satisfaction scores.

Taking the First Step

Addressing these hidden risks doesn’t have to be overwhelming. Small changes can yield big results, and we’re here to help you every step of the way.

References

References
European Central Bank (2021). More than 900,000 UK small businesses ‘at risk’ of failing by early April. [online] Available at: https://www.ecb.europa.eu [Accessed 5 Dec. 2024].

Small Business Trends (2023). 60 Percent of Small Businesses Fail After a Cyber Attack. [online] Available at: https://smallbiztrends.com [Accessed 5 Dec. 2024].

UK Government, 2024. *Cyber Security Breaches Survey 2024*. [online] available at: https://www.gov.uk/goverment/cyber-security-breaches-survey-2024/cyber-secuirty-breaches-survey-2024 [Accessed 5 Dec.2024].