MACKAY
Corporate Insurance Brokers

March 2026

COMMERCIAL
Insurance Profile

The Importance of Annual Insurance Reviews

A 2025 survey from insurance company Hiscox found that 74% of UK small- and medium-sized enterprises (SMEs) are underinsured. While that statistic focuses on smaller firms, underinsurance is not limited to smaller organisations. Any organisation can fall behind as risks evolve.

An annual insurance review is one of the most effective ways to ensure cover remains aligned with operational realities. Over the course of a year, organisations may expand services, purchase new equipment, hire staff, relocate premises or adopt new technologies. Regulatory requirements may also shift. Without a structured review, policies can quickly become outdated, leaving costly gaps or unnecessary overlaps.

Why Annual Reviews Matter

An annual insurance review offers several important advantages for organisations seeking to maintain accurate cover, manage costs and strengthen overall risk resilience:

- **Improved cover accuracy and compliance**—Business operations rarely stand still. New contracts, partnerships, digital tools and regulatory updates—such as changes to data protection or health and safety requirements—can all affect insurance needs. A yearly review helps ensure policies reflect these developments and remain compliant with UK legislation.
- **Cost efficiency and clarity**—An insurance review is not solely about increasing protection. It can also reveal duplicated cover, outdated policies or excessive limits that drive up premiums unnecessarily. At the same time, it helps prevent underinsurance, which could lead to reduced claims settlements. Reviewing policies annually also refreshes decision-makers' understanding of terms, exclusions and conditions.
- **Greater confidence and risk readiness**—When leadership knows appropriate cover is in place, it strengthens stakeholder confidence. Clients, partners and employees benefit from knowing the organisation has taken steps to prepare.

Key Areas to Assess

Although every organisation is unique, there are several core areas that deserve attention during an annual review:

- **Property and equipment values**—Rising replacement costs or new assets may require updated sums insured.
- **Revenue and turnover**—Changes can affect business interruption and liability cover limits.
- **Employee numbers and payroll**—These may influence employers' liability exposure.
- **Vehicles and drivers**—Ensure all are accurately listed under commercial motor policies.
- **Cyber and data protection risks**—Review cyber cover in light of evolving threats.
- **Policy exclusions and endorsements**—Understand what is not covered and consider whether additional protection is needed.
- **Contracts, leases or structural changes**—These may introduce new insurance obligations.

Making the Review Productive

To gain the most value, organisations should review current policies in advance, document operational changes from the past year and analyse claims history for emerging patterns. Working with an experienced broker can provide valuable insight into regulatory updates, new products and potential cost-saving opportunities.

Contact Us Today

Organisations of all types and sizes can benefit from conducting an annual insurance review. These yearly check-ups help ensure cover keeps pace with evolving needs while identifying potential cost savings.

Contact us today to learn how we can support your business.

Getting Employee Buy-in on AI

Organisations across the UK are adopting artificial intelligence (AI) to boost productivity, improve accuracy and streamline workflows. However, technology alone does not guarantee success. Securing genuine employee buy-in remains a key challenge. Without trust, clarity and appropriate safeguards, AI initiatives can stall, create friction, or increase operational and cyber-security risk.

Common Barriers to Adoption

While the benefits of AI are widely discussed, employees often approach new tools with caution. Organisations introducing AI frequently encounter several obstacles. Employees may worry about:

- **Job displacement or role changes**—Concerns that AI could replace or significantly alter existing responsibilities
- **Increased monitoring**—Fears that performance may be judged primarily by automated systems
- **Expanded workloads**—Anxiety that adopting AI will add tasks rather than reduce them

Training and governance gaps can also undermine confidence. Providing AI tools without clear policies, structured learning or data protection guidance increases uncertainty. Limited transparency about how outputs are reviewed may heighten compliance and cyber-security risk.

Strengthening Buy-in Through Risk Mitigation

To build trust and reduce resistance, leaders should take deliberate, structured steps. Before launching or expanding AI tools, organisations should:

- **Develop clear AI governance policies** outlining acceptable use, data handling standards and human oversight requirements.
- **Assess cyber-security implications** to ensure AI platforms do not introduce vulnerabilities or compromise sensitive information.
- **Identify high-value pilot use cases** that demonstrate practical benefits without disrupting core operations.

Training and Communication Matter

Training is one of the most powerful drivers of employee confidence. However, effective training extends beyond a one-off introduction to software. It should provide hands-on learning opportunities, role-specific examples and ongoing support.

Equally important is transparent communication. Leaders can improve buy-in by:

- Explaining how AI will complement human expertise rather than replace it
- Sharing clear examples of time savings or improved accuracy
- Reinforcing that employees remain accountable decision-makers
- Encouraging questions and feedback throughout the rollout process

Linking AI to Professional Growth

Adoption may increase when employees see personal value. Positioning AI as a tool that reduces repetitive tasks and frees time for higher-value work can shift perceptions. Organisations should highlight how AI skills contribute to career development, digital literacy and long-term employability. Involving managers in modelling appropriate AI use can also strengthen alignment. When leadership demonstrates responsible adoption, employees are more likely to follow suit.

Conclusion

Overall, AI implementation is not simply a technology upgrade; it is a workforce and risk management strategy. Organisations that combine governance, cyber-security awareness, structured training and transparent communication will be better equipped to unlock AI's benefits while minimising disruption.

For further risk management guidance, contact us today.

Overcoming resistance takes more than simply introducing new tools; it requires communication, training and trust. Organisations that take a thoughtful approach can turn initial hesitation into genuine enthusiasm.