

GRC (governance, risk, and compliance) is an executive strategy for managing governance, risk, and compliance with industry standards and government regulations. GRC also refers to a suite of software for implementing and maintaining an enterprise GRC program.

GRC practices and processes structure management’s approach to aligning IT with organizational objectives. It helps organizations manage IT and security risks while lowering costs and meeting compliance requirements. It improves decision-making and resulting performance with an integrated view of the effectiveness of risk management.

In the current business climate, GRC management is more important than ever before. Many organizations are facing significant challenges in regulatory compliance, enterprise risk management, cybersecurity, and vendor management. With auditors and regulators scrutinizing GRC ever more closely, companies must be prepared.

Governance

Governance provides control over infrastructure and facilities, as well as oversight of corporate conduct at the portfolio level.

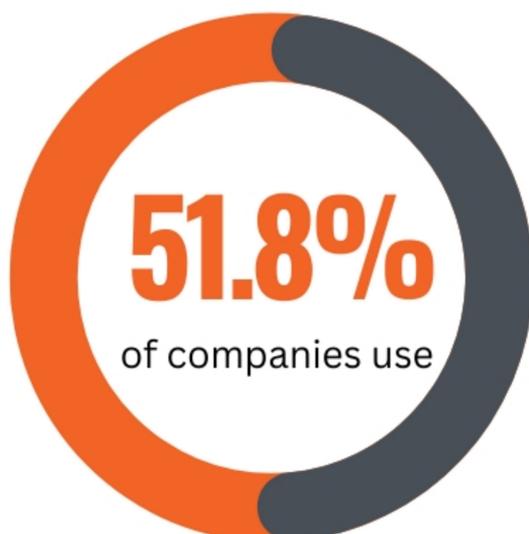
- Only 30% of internal audit departments leverage big data to identify and assess risk.
- Fewer than half, just 48%, of internal audit departments interact with IT services departments to calculate Key Risk Indicators.
- A staggering 60% of internal audit administrators say that their departments never submit documentation of management data to their corporate governing boards.

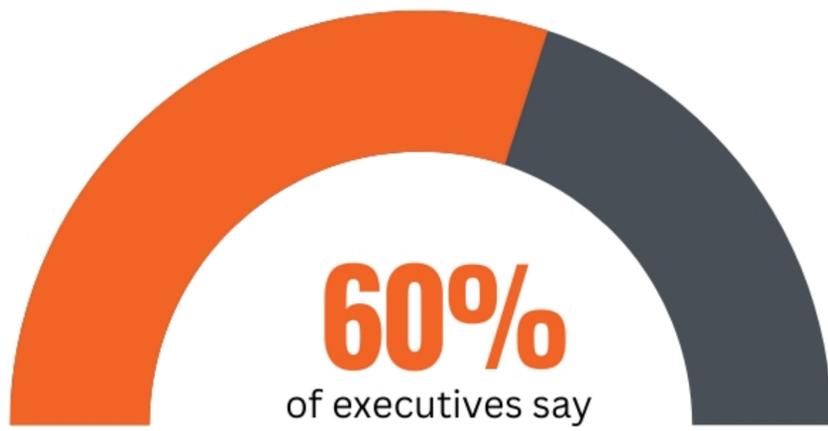


Risk

More than half (51.8%) of companies use ad hoc tools such as spreadsheets and Word documents to manage their business continuity plans. However, an increasing number of IT services departments are using business continuity planning software.

The continuity of business is threatened by natural and manmade disasters and failures of technology. A more prominent source of risk to US corporations, however, is cybersecurity. These statistics indicate how companies are faring with cybersecurity management:





- 130: Average number of cybersecurity breaches per organization per year.
- \$11.7 million: Average annual losses due to cybersecurity breaches across American companies as a whole.
- \$17 million. Average annual spending on damages due to cybercrime in banking and energy industries.
- 32% of organizations experienced a major cyber attack in the last year.
- 60% of executives say that cybersecurity is one of their top priorities.
- 76% of executives say either that their organization has no metrics for cybersecurity risk (49%) or that they do not know if their organization measures cyber risk exposure.

Compliance

Compliance officers rank constant regulatory change as their biggest challenge in meeting compliance rules. In the US, more than 900 regulatory agencies issue over 200 regulatory changes every business day. American corporations, regardless of size, spend an average of \$11,000 per employee per year on regulatory compliance. The Violation Tracker website has compiled a list of 538,000 cases from just 400 regulatory agencies resulting in total fines of over \$850 billion.

- 27% of lead compliance officers strongly agree that their company's compliance department has a management process in place to identify and incorporate legal and regulatory changes so they can be integrated into policies and procedures.
- 53% of lead compliance officers report that compliance is siloed rather than integrated across their organization.

A benchmark compliance study by the Ponemon Institute found that implementing best practices resulted in significant savings in compliance expenses.

- Annual compliance audits resulted in an average \$2.86 million in annual compliance savings.
- Integrating regulatory compliance with security and privacy functions resulted in an average of \$2.02 million in annual compliance savings.
- Standardizing incident response processes resulted in average annual compliance savings of \$1.89 million.
- Enabling compliance technology resulted in an average of \$1.43 million in savings annually.
- Enhanced regulatory monitoring resulted in an average of \$1.02 million in savings annually.



900 regulatory agencies issue over 200 regulatory changes every business day



Intertec International for GRC

Preparing for new and emerging threats in an environment of constantly changing regulatory requirements requires a strong framework for strategic GRC. By partnering with Intertec International, you can ensure security, compliance, and regulatory adherence.