Active Governance Framework (AGF)
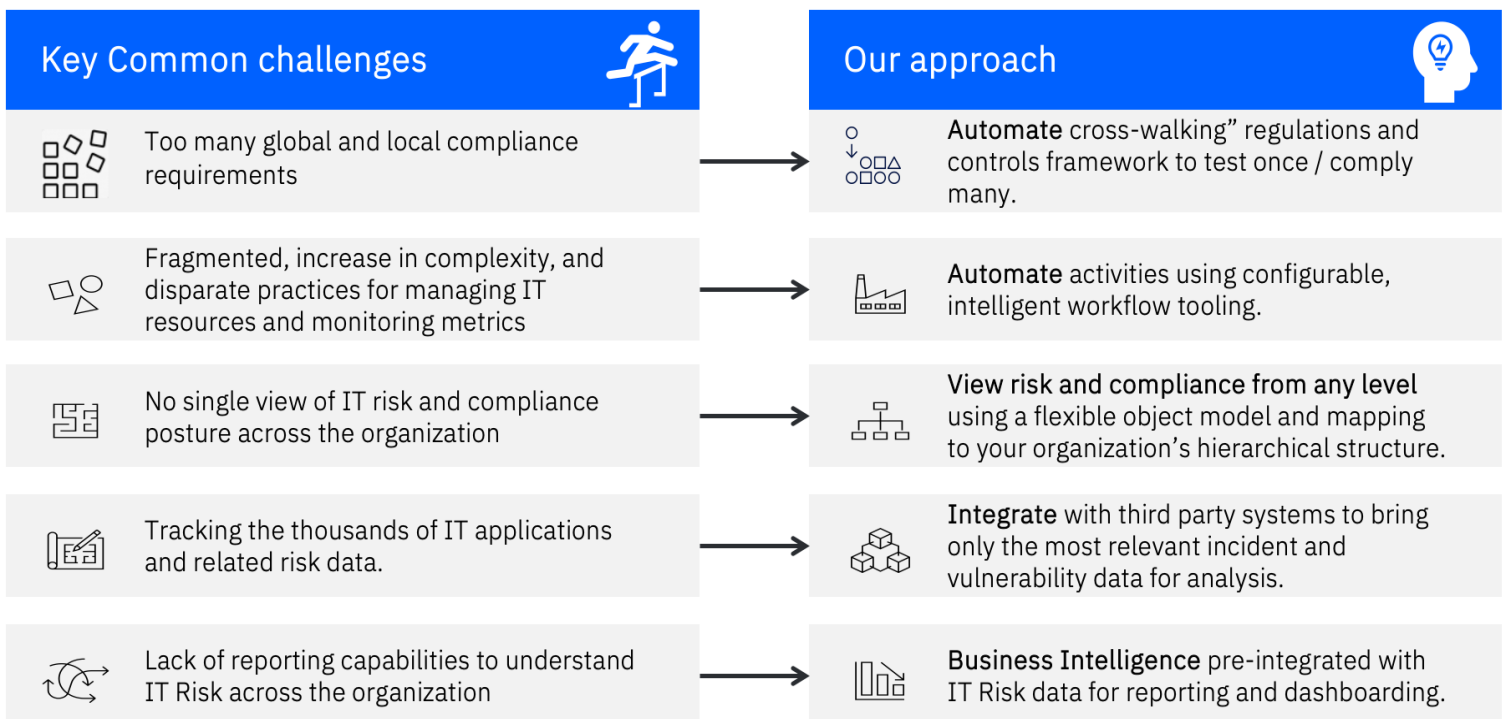
A Proactive Approach to Help Enterprises Manage Increased Cyber Risk Demands

How do you manage the never-ending stream of regulatory mandates, compliance control requirements, audit requests, and cyber threats? Does your organization find it challenging to make sound cybersecurity decisions about risks and resiliency, and aggregate data for visibility and decision making? If you're struggling to gain ground in advancing your enterprise's cybersecurity program, **IBM Active Governance Framework (AGF)** can provide a proactive approach to cybersecurity governance, risk, and compliance across your enterprise.

IBM's AGF solution allows you to:

- Support **Assessments** that drive **Cyber Strategy & Resilience programs** to align to enterprise objectives and **zero trust** methodologies.
- Operationalize **Cyber Risk Management** across the enterprise and deploy real-time visibility into cyber risk exposure and mitigation strategies.
- Embed **Cyber Resilience** within the Three Lines of Defense considering overall ecosystem risks.
- Provide a foundational structure for an automated and multi-layered approach to **Cyber Policy & Compliance Management.**
- Establish a **Metrics, Reporting & Decision-Making** program through key Enterprise Data, Artificial Intelligence & Machine Learning capabilities.

Operationalize cybersecurity risk and compliance with IBM

Key Common challenges	Our approach
Too many global and local compliance requirements	**Automate** cross-walking" regulations and controls framework to test once / comply many.
Fragmented, increase in complexity, and disparate practices for managing IT resources and monitoring metrics	**Automate** activities using configurable, intelligent workflow tooling.
No single view of IT risk and compliance posture across the organization	**View risk and compliance from any level** using a flexible object model and mapping to your organization's hierarchical structure.
Tracking the thousands of IT applications and related risk data.	**Integrate** with third party systems to bring only the most relevant incident and vulnerability data for analysis.
Lack of reporting capabilities to understand IT Risk across the organization	**Business Intelligence** pre-integrated with IT Risk data for reporting and dashboarding.

IBM

The IBM AGF - *Continuous Control Monitoring (CCM)*

Organize & manage the complexities of your enterprise's cybersecurity risk management program

- Drive **risk reduction** and optimize compliance through **automated monitoring** of processes and cyber security controls

- **Modernize** compliance operations through automated **data aggregation** (including regulations, standards, policies, and client data)

- Increase the breadth and depth of controls testing by transitioning from manual sample-based testing to automated **continuous control testing**

- Decrease time to identification and resolution of issues using actionable insights generated from **intelligent workflows** (based on client requirements)

Modernize your risk and compliance initiatives through the power of data driven decisions.

IBM AGF can create a comprehensive, centralized system of governance that will help you reduce your risks, increase your maturity and resiliency, as well as provide continuous monitoring.

IBM can guide you every step of the way. To learn more about IBM Active Governance Framework, please contact your IBM representative.