Optimizing Governance, Risk and Compliance in Microsoft 365

Compliance has become a hot topic in recent years, as regulations govern many aspects of the workplace. To remain competitive, organizations must improve their compliance posture, and Microsoft offers robust tools to support that process. Forward-thinking companies make it a priority to optimize the capabilities around governance, risk and compliance in Microsoft 365.

Compliance and Security

Compliance refers to the laws and industry regulations a company must follow. Regulations such as HIPAA and PCI DSS define the types of data companies must protect. They also mandate processes such as data retention and disclosure of certain security events.

Data security, on the other hand, includes the processes and technologies used to guard sensitive data and protect against breaches. While security is not the same as compliance, many compliance requirements include security components. To truly protect data, organizations will move beyond checkbox compliance to comprehensive information security.

Toolsets to Drive Compliance in Microsoft 365

Microsoft 365 offers a set of integrated tools designed to help organizations achieve and monitor end-to-end compliance. In addition to security controls, these include tools to govern the use, sharing, storing and destruction of data. The chart below outlines key capabilities available for Microsoft 365 customers.

Note: Keep in mind that the compliance capabilities in Microsoft 365 depend on licensing level. Microsoft 365 Business Premium and Enterprise E3 licenses deliver a substantial amount of compliance capabilities. However, to take full advantage of compliance offerings in Microsoft 365, organizations need to purchase an Enterprise E5 plan.

	Available to Business Premium and E3 Customers	**Requires E5 Licensing**
Information Protection	• Data loss prevention • Message encryption • Multi geo (extra) • Sensitivity labels	• Customer key • Data loss prevention for Teams DLP • Hold your own key • Advanced message encryption • Sensitive information types • Sensitivity labels for automated labelling
Information Governance	• Retention labels • Retention policies	• Records management • Retention labels for automated labelling • Retention policies for rules-based policies
Insider Risk Management	NA	• Communications compliance • Customer lock box • Information barriers • Insider risk management • Privacy Management • Privileged access management
eDiscovery and Audit	• Cloud app discovery • Compliance Manager • Litigation hold • Search	• Audit for Advanced Audit • Compliance Manager custom assessments • eDiscovery for Advanced eDiscovery • Microsoft Defender for Cloud Apps (MCAS)

Where Does Your Organization Fit in the Microsoft 365 Maturity Model for Governance, Risk and Compliance?

The Microsoft 365 Maturity Model provides a way for organizations to determine their progress on the path to strategic compliance. Consider the following overview.

- Level 100 (Initial) – Organizations at the Initial level of compliance do not consider compliance as important. Management does not understand the business impact of non-compliance and does not invest in the training or tools that compliance would require. The organization lacks the policies and technical controls to support compliance.

- Level 200 (Managed) – The organization approaches compliance and security from a checkbox philosophy. Consequently, policies exist as mandated, but no one enforces them. Without formal compliance roles and training, the process remains haphazard and localized. Users view compliance as painful, and technical controls see limited use.

  Meanwhile, the organization has not taken steps to identify and secure sensitive data. They either ignore data retention or retain everything. As a result, information clutter leaves the company at risk. Compliance actions happen in response to crisis, rather than as a proactive strategy.

- Level 300 (Defined) – The organization views compliance as essential, and executive sponsorship drives progress toward necessary cultural changes. The company has defined compliance roles and responsibilities, and employees receive annual training.

  While baseline compliance framework exists, and technical controls such as sensitivity labels have been implemented, gaps remain. The organization still needs to address unknown risks and improve information governance to reduce data redundancy and silos.

- Level 400 (Predictable) – The organization has achieved a culture where individuals have a high understanding of compliance risk, and everyone shares accountability. Compliance is more proactive than reactive, with workloads reduced using technology and streamlined policies and automated compliance controls.

- Level 500 (Optimizing) – The organization sees information governance and compliance as a strategy to support business goals rather than a means to reduce risk. Stakeholders balance compliance and risk as they work to continually measure and improve processes and controls.

Take the Next Steps Toward Optimizing Compliance in Microsoft 365

The compliance consultants at Messaging Architects combine a deep understanding Microsoft 365 with records management expertise. We can help your organization take the next step on the path to optimizing Microsoft 365 compliance tools for strategic benefit.