It can be difficult to establish an appropriate and complete enterprise security posture that can also support business growth objectives. The threats to information assets are varied and constantly evolving, as are the available products, tools and methods to help you respond. Moreover, what may be an adequate security level for one IT system or business process may be insufficient for another.

The IBM Information Security Framework is designed to help businesses meet the challenge of creating a security posture that corresponds to the threats, risks and business demands they face—while providing a clear path to improving security levels as situations and conditions evolve.

The IBM Information Security Framework is offered in conjunction with IBM assessment and planning services for security and privacy. It is designed to enable a better understanding of your unique security program, provide an effective roadmap for improvement and allow you to measure the program’s success.

**Simplifying the planning and execution of your enterprise security program**

Our Information Security Framework is an integrated and comprehensive best-practice-driven approach to security. It’s based on our research, extensive portfolio of security offerings, and leadership in performing assessments and developing and supporting security solutions for global clients.

The framework’s best practices address these core security themes:

- **Governance**
- **Privacy**
- **Threat mitigation**
- **Transaction and data integrity**
- **Identity and access management**
- **Application security**
- **Physical security**
- **Personnel security**
Creating security programs in response to business requirements
To help you develop a comprehensive security program that meets your business objectives, the information security capability reference model and assessment tool enable you to determine your current security posture. They measure your level of response to each capability in the core security themes against the layers of the enterprise IT security model: principles, policies, processes, standards, procedures, architecture and products. For each capability, the maturity model provides a scale defining posture: initial, basic, capable, efficient and optimized. This detailed discovery process considers the entire security environment, not just individual components, and helps ensure that you have an accurate baseline evaluation of your security posture.

Enabling self-assessments to help identify shortcomings
The Information Security Framework’s assessment tool helps you determine the potential risks associated with each capability’s current posture. The tool provides a roadmap to remediate and move between maturity levels if the corresponding risk is unacceptable to the business. By providing meaningful evaluation of your enterprise’s security risks and proposing steps to reduce risk and achieve specific security requirements, the framework helps you quickly plan and execute an effective response that matches your business needs and resources.

Leveraging the experience of IBM’s global team
Unlike security vendors that provide point solutions to address a specific threat or process, IBM provides a comprehensive portfolio of proven capabilities, including the Information Security Framework, that offers you an end-to-end, systemic approach to enterprise security. Our expertise and breakthrough thinking can help you manage and mitigate the risk to your information assets, pursue new business initiatives more securely and proactively prevent security problems.

For more information
To learn more about the IBM Information Security Framework, contact your IBM representative or visit:

ibm.com/services/security