ASCENT
Security Compliance Portal

7 TIPS FOR IMPLEMENTING AN ORGANIZATIONAL RISK MANAGEMENT STRATEGY

Implement and maintain a strong risk management strategy with these best practices.

A risk management strategy is necessary for organizations to implement and maintain an effective risk management program. Subsequently, an effective risk management program is necessary to help ensure that organizations can effectively manage risks to information assets, data, and overall business operations. Lacking a risk management strategy and accompanying program may lead to a false sense of protection regarding risks that could potentially impact the daily operations of an organization, or the recovery of operational capabilities.

To help you implement and maintain a strong risk management strategy for your organization, consider the following tips. They will help you align your risk management program with your overall security program so that you can minimize overall risk with ease.

1. **Develop and implement a program**. A risk management program is critical to achieving the intended goals of an organization's risk management strategy. Program implementation should align with other defined security program goals. The lack of a risk management program may lead to ineffective implementation of an organization's risk management strategy. Risk management control assignment, accountability, and continuous management are key to maintaining an effective program.

2. **Frequently review and update.** The risk management strategy should be reviewed and updated at least annually. More frequent reviews may be required to address changes to information systems, security control requirements or changes to the overall organization.

3. **Solicit feedback and approval**. Risk management processes should be established, managed, and agreed upon by appropriate stakeholders and individual control owners. Solicit feedback and approval for the risk management strategy from all appropriate stakeholders within your organization. This is not an IT-only exercise but should be an organization-wide exercise.

> Lacking a risk management strategy and program may lead to a false sense of risk protection that could impact daily operations or recovery of operational capabilities.

4. **Perform risk assessments.** Once organizations have developed a risk management strategy and program, regular risk assessments should be performed to identify, or update, a list of risk scenarios to which the organization may be susceptible. This process should result in the potential impact for each risk scenario being assessed. Annual risk assessments are not only a best practice, but they are also required by most regulatory control frameworks to validate that an organization routinely monitors applicable risks and applies appropriate risk treatment or mitigation.

5. **Partner up.** If it makes sense for your organization, you can partner with a reputable security provider that provides an effective way to manage and maintain risk assessments. This should include the management and tracking of remediation activities.

6. **Treat and mitigate risk as needed.** Organizations need to have defined processes in place for completing risk treatment and mitigation activities once a risk assessment has been completed. Without these processes, risks may be identified during risk assessments but never properly addressed or managed. Treatment and mitigation requirements need to be assigned to clearly defined owners to ensure that appropriate personnel are held accountable for addressing identified risks. If not, organizations may fall victim to one of the worst types of risk – one of which they are aware but do nothing to resolve.

7. **Categorize security and frame risk.** Security categories for an organization’s information systems need to be defined to enable appropriate risk decisions to be made. Without this, organizations could potentially expend resources to pro-

Effective Risk Management Programs Require...

CONTROL ASSIGNMENT

ACCOUNTABILITY

CONTINUOUS MANAGEMENT

tect a lower-impact, lower-risk system instead of focusing attention on a higher-impact or higher-risk system. It's important to protect all systems, but protection levels should be based on the level of risk defined for information systems.

Risk Management Comes by Design

Your organization should ensure that a comprehensive risk management strategy is developed and implemented consistently across the organization. This is necessary to manage security risks to operations, information assets, individuals, and other organizations associated with the operation or use of your internal information systems.

If applicable, the risk management strategy should also address privacy risks to individuals resulting from the collection, sharing, storing, transmission, use, and disposal of personally identifiable information. By developing a risk management strategy and building a comprehensive risk management program, supported by all organizational stakeholders, you'll ensure that your organization can avoid key risk pitfalls for effective overall security.

READ MORE > 100 Security Program Pitfalls and Prescriptions to Avoid Them. PDF

ASCENT Portal - A Single Source of Security and Compliance Truth

Automate, Manage and Track All Your Compliance Processes Across More than 40 Industry Frameworks

The ASCENT Portal is a comprehensive SaaS-based platform that delivers fingertip access to everything you need to comply with more than 40 industry frameworks. From customizable assessments and calendar-driven control task reminders to governance templates and compliant vendor management, the ASCENT Portal automates your compliance process, end-to-end, while delivering real-time status views and reports all from a single source.

Schedule a demo today.

SCHEDULE A DEMO

ASCENT
Security Compliance Portal

ASCENT Portal
Capital View Center , 1301 S. Capital of Texas Highway, Suite A-130, Austin, TX 78746

Phone: 866.300.0795 **Email:** sales@ascent-portal.com **Web**: www.ascent-portal.com