CYBERSECURITY PROGRAM ASSESSMENT

PROFESSIONAL SERVICES. CLOUD.
EdgeDx
CYBERSECURITY. DIGITAL LEARNING.

The Security Program Assessment draws on our collective expertise to deliver tailored, actionable recommendations to improve your security posture, reduce risk, and mitigate the impact of security incidents.

PROCEDURE:

Our vCISO will take the time to interview staff, review policies & procedures, determine risk appetite, identify weaknesses, and provide detailed, actionable recommendations to improve your Security Program.

Security Program Assessment evaluates the maturity of an organization's security program based on industry standards (NIST & NJSISM) and controls to identify gaps and provide an incremental roadmap to improve the overall security posture of the organization.

DELIVERABLES:

Edge will review documentation, perform interviews and facilitate interactive workshops to understand the current security posture of the environment and to ensure roadmaps and recommendations are driven through collaboration. Edge will deliver actionable recommendations and an implementation roadmap specific to the organization's short- and long-term goals. The final report will include an executive summary, vulnerability report, an in-depth gap analysis and recommendations, and a prioritized security program roadmap. Additionally, an Executive presentation will be provided, tailored to the requirements of the organization and audience. Recommendations will include guidance on how to fully utilize existing tools as well as suggestions for new tools and processes that can be implemented to improve security posture and reduce risk.

- Understand the organization's risk expose
- Improve the overall security posture of the organization
- Reduce the risk of breach and data theft
- Reduce the impact of security incidents
- Security Program Roadmap and recommendations
- Executive Presentation

READY TO TAKE PROACTIVE CONTROL OF YOUR CYBERSECURITY NEEDS? CONTACT INFO@NJEDGE.NET.

THE CONTROL FAMILIES THAT WE WILL COVER ARE:

- Access Control
- Audit and Accountability
- Awareness and Training
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Personnel Security
- Physical and Environmental Protection
- Planning
- Program Management
- Risk Assessment
- Security Assessment and Authorization
- System and Communications Protection
- System and Information Integrity
- System and Services Acquisition

* All facets of the Cybersecurity Assessment Program comply with the NIST Cybersecurity Framework (CSF) which categorically creates five concurrent and continuous reference functions - Identify, Protect, Detect, Respond and Recover. Each category maintains a strategic view of the life cycle within an organization's cybersecurity program. The operation, prioritization, measuring and monitoring are implemented using the Center for Internet Security - Critical Security Controls (CSC) to map directly to the CSF core requirements. Collectively these methods formulate the strategy to meet many standards such as: NIST SP 800-53, ISO/IEC 27001:2013, CIS CSC, HIPPA, PCI DSS 3.0, COBIT 5, ITIL.