Peer Assessment Service

Agenda

For Peers, By Peers

How It Works: The Short Story

How It Works: The Long Story

Scope

Pre-Discovery

Report

Assessment Teams

Service Fees

For Peers, By Peers

A fresh perspective from an objective, informed third party

An unbiased analysis of your own internal assessments

A professional report that includes

- National Institute of Standards and Technology (NIST)-oriented, actionable recommendations
- Prioritized steps with a focus on scalability
- Suggestions for continuous process improvement
- Separate executive summary to encourage understanding and buy-in

How It Works: The Short Story

Step 1: You influence scope, topics, dates of the assessment.

Step 2: Assessors research and review institution-specific practices.

Step 3: Assessors perform an in-person analysis including personnel interviews and physical tours

Step 4: Assessors prepare early drafts for review and correction.

Step 5: Final report with executive summary is delivered.

How It Works: The Long Story

- Develop Statement of Work (SOW)
- Perform Pre-Discovery
- Conduct Site Visit – usually 3-4 Days
- Follow-up Questions
- Writing Narrative
- Inserting and prioritizing recommendations with NIST references
- Sharing Draft – CIO
- Finalizing Report
- Report content belongs to the university or college being assessed

Scope

General Assessment

- Broad-based overview of cybersecurity posture

Supplemental Assessments

- Incident Response
- Physical Security
- Policies
- Security Operations
- Standards Gap (compared to NIST Cybersecurity Framework)
- Compliance (i.e. HIPAA, GLBA, FERPA, FISMA)
- Objective Review of External Penetration or Vulnerability Scan Reports

Pre-Discovery

Security Policy

Privacy Policy

Data Management

Asset Inventories & Tracking

Incident Response Procedures

Vulnerability Scanning Procedures

Intrusion Detection & Prevention

Event Log Monitoring

Cloud Services Policy

Change Management Procedures

Employee On-boarding & Orientation

Network Management Procedures

Endpoint Configuration

Encryption

Export controls

Firewall Policy

Organizational Chart

Production Control

Security of Research

Facilities Access Procedures

More…

Report

Asset Management

Business Environment

Human Resources Security

Governance

Security & Privacy Policy

Organization of Security

Compliance

Risk Assessment

Awareness & Training

Identity Management

Access Control

Data Security

Maintenance

Protective Technologies

Physical Security

Security Continuous Monitoring

Detecting Anomalies & Events

Detection Processes

Incident Response

Assessment Teams

- Security professionals from several institutions across the U.S.
- CIOs
- CISOs
- Employed or recently retired

Service Fees

General Assessment

- Broad-based overview of cybersecurity posture $35,000

Supplemental Assessments

- Focused Assessment of Incident Response $2500
- Physical Security Review & Analysis $2500
- Policy Assessment $2500
- In-depth Assessment of Security Operations $2500
- Standards Gap Analysis NIST Cybersecurity Framework $2500
- Compliance (i.e. HIPAA, GLBA, FERPA, FISMA) $4000 per
- Objective Review of External Penetration $2500

  Or Vulnerability Scan Reports

Become a Peer Assessor

Join REN-ISAC and help strengthen cybersecurity throughout the higher education sector.

- Gain real-world experience working within NIST Cybersecurity Framework
- Earn Continuing Professional Experience (CPE) credits
- Stipend
- Paid travel

Contact

peer@ren-isac.net

ren-isac.net/pas

812-856-5049