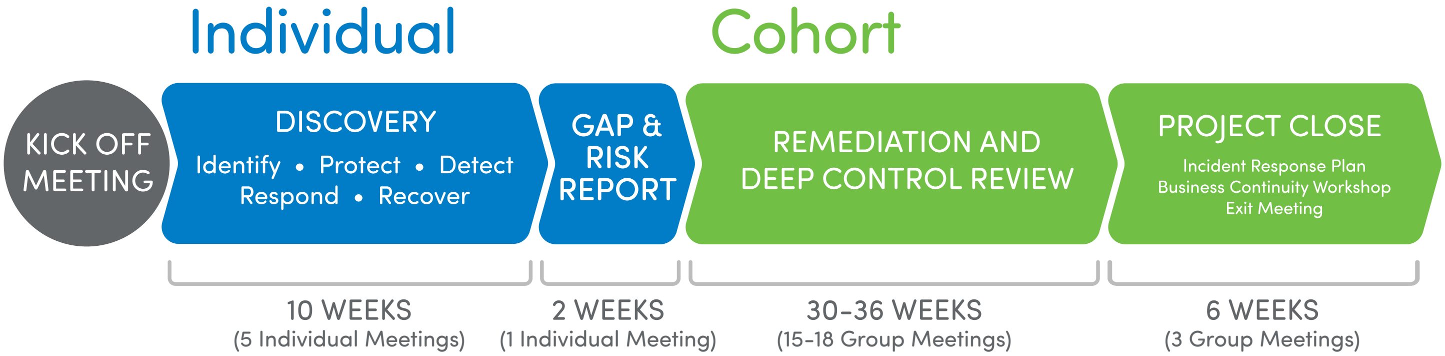
CSF Security Cohort Program

Program Highlights

- **Expert Guidance**: Join a group of your peers to receive bi-weekly expert guidance on data security.
- **Collaborative Learning**: Participate in interactive sessions, sharing experiences and learning from industry experts and your peers.
- **Comprehensive Support**: Benefit from a year-long commitment to enhancing your organization's data security posture.

What You'll Receive

- **Personalized Gap and Risk Assessment**: understand your current data security strengths and areas for improvement through a tailored assessment**.**
- **Deep Dive into Controls**: Gain a thorough understanding of essential data security controls to protect your organization's information.
- **Incident Response and Business Continuity Planning**: Participate in workshops designed to prepare you for potential data breaches and ensure continuity of operations.



Individual

Cohort

KICK OFF MEETING

DISCOVERY
Identify • Protect • Detect
Respond • Recover

10 WEEKS
(5 Individual Meetings)

GAP & RISK REPORT

2 WEEKS
(1 Individual Meeting)

REMEDIATION AND DEEP CONTROL REVIEW

30-36 WEEKS
(15-18 Group Meetings)

PROJECT CLOSE
Incident Response Plan
Business Continuity Workshop
Exit Meeting

6 WEEKS
(3 Group Meetings)

The Management Council
Ohio Education Computer Network

Let's Talk Solutions

Art Provost
CISO
CISSP, CISM, GIAC: GSEC,
GPEN, GWAPT, GSTRT

402.479.6848 - Direct
402.881.6369 - Mobile
art.provost@managementcouncil.org

NIST Cybersecurity Framework (CSF) Control Families

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) provides a set of guidelines to improve an organization's cybersecurity posture. These guidelines, organized into five control families, cover different aspects of cybersecurity management and protection. By adopting the NIST CSF, organizations in Ohio can benefit from the state's Safe Harbor Act, which offers legal protection against data breach claims if they comply with industry-recognized cybersecurity programs.

Identify

We develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data and capabilities.

Controls Addressed

- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy

Protect

We develop and implement appropriate safeguards to ensure delivery of critical services and support the ability to limit or contain the impact of a potential cybersecurity event.

Controls Addressed

- Identity Management and Access Control
- Awareness and Training
- Data Security
- Information Protection Processes and Procedures
- Maintenance
- Protective Technology

Detect

We implement safeguards for the timely discovery of cybersecurity events.

Controls Addressed

- Anomalies and Events
- Security Continuous Monitoring
- Detection Processes

Respond

We develop and implement appropriate activities to take action and contain the impact of a detected cybersecurity incident.

Controls Addressed

- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements

Recover

We ensure timely restoration of capabilities impaired by a cybersecurity incident, that minimizes impact and expedite a return to normal operations.

Controls Addressed

- Recovery Planning
- Improvements
- Communications
- Security Continuous Monitoring
- Detection Processes

The Management Council
Ohio Education Computer Network

07.18.24