Institute for Cyber Executive Education

Executive Education for Cybersecurity Governance and Mission System Authorization

Industry Partnership & Sponsored Cohort Programs

Executive Summary

Modern cyber systems operate within complex mission environments involving distributed infrastructure, continuous software delivery pipelines, AI-enabled capabilities, and evolving operational risks.

Organizations responsible for developing and deploying these systems must navigate not only cybersecurity controls, but also governance decisions, authorization pathways, and mission risk leadership.

The Institute for Cyber Executive Education (ICEE) provides executive-level education focused on these decision environments. Institute programs explain how cyber systems are governed, authorized, and deployed within operational missions.

Through industry-sponsored learning cohorts, organizations can support structured education programs that strengthen the broader ecosystem surrounding government and regulated cyber systems.

Industry Partnership Programs

The Institute partners with technology companies, platform providers, and ecosystem leaders to support cybersecurity education programs.

Program Tracks:

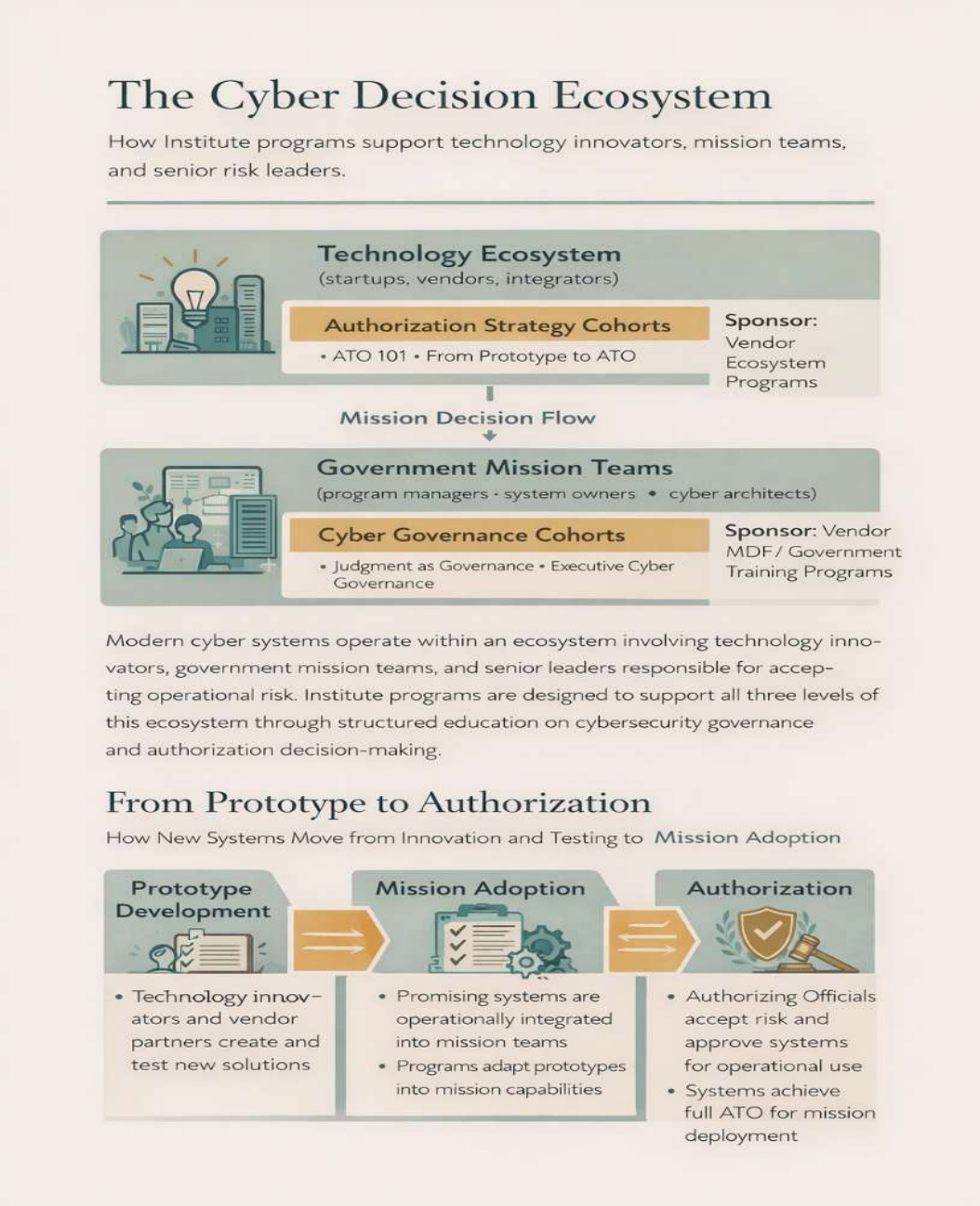
1. **Vendor Ecosystem Cohorts**
   Programs sponsored by technology vendors educate partners, startups, integrators, and solution architects operating within their ecosystem.

2. **Government Cohorts (Supported by Vendor MDF)**
   Programs funded through vendor Marketing Development Funds (MDF) provide

executive education programs for government participants responsible for cybersecurity governance and system authorization.

3. Authorizing Official Leadership Programs (Supported by Vendor MDF)

An executive education program designed specifically for Authorizing Officials and senior mission leaders responsible for accepting operational cyber risk.



These programs address different parts of the mission technology ecosystem and strengthen understanding of how cyber systems are governed and deployed in operational environments.

The Institute's programs support different participants within the cybersecurity decision ecosystem surrounding modern mission systems.

Modern cyber systems operate within an ecosystem involving technology innovators, government mission teams, and senior leaders responsible for accepting operational risk. Institute programs are designed to support each level of this ecosystem through structured education on cybersecurity governance and authorization decision-making.

Flagship Sponsored Cohort Programs

The Institute currently offers three (3) flagship cohort program tracks designed specifically for industry sponsorship.

These programs address the two most common educational needs within government technology ecosystems.

Cohort programs may be customized in collaboration with sponsoring organizations to address specific mission environments, technology ecosystems, or stakeholder communities.

1. Authorization Strategy for Technology Ecosystems

Delivered in either a 3 module or 10 module format, this cohort program helps vendor partner communities understand how cybersecurity authorization decisions are made within government mission environments.

Participants learn how systems move from prototype development to operational deployment and how architecture and governance decisions affect authorization outcomes.

This program draws from Institute courses including:

- ATO 101
- From Prototype to ATO
- Authorization as a Leadership Decision

Typical participants include:

- partner solution architects

- startup founders and innovators
- cybersecurity engineers
- integrator technical teams
- federal market technical leaders

Sponsors use this program to strengthen their partner ecosystem and improve partner readiness for government cybersecurity environments.

2. Cyber Governance for Mission Leaders *(Government Cohort Supported by Vendor MDF)*

This cohort program provides executive education for government participants responsible for cybersecurity governance and mission system authorization.

Programs may be funded through vendor Marketing Development Funds (MDF) and delivered exclusively to government audiences.

Participants explore governance frameworks and engineering decision environments that shape modern cyber systems.

This program draws from Institute courses including:

- Judgment as a Governance Act
- Executive Cyber & AI Governance
- AI Governance, Ethics & Judgment in Practice

Typical participants include:

- program managers
- system owners
- cybersecurity architects
- mission technology leaders
- innovation program teams

Vendor-supported government cohorts help mission organizations better understand the governance challenges surrounding emerging technologies.

3. Authorizing Official Leadership Programs
(Government Cohort Supported by Vendor MDF)

The Institute also offers executive education programs designed specifically for Authorizing Officials and senior mission leaders responsible for cybersecurity risk acceptance.

These programs address the leadership responsibilities associated with authorizing complex cyber systems within operational mission environments.

Participants explore topics including:

- the role of the Authorizing Official in mission risk governance
- understanding architectural evidence and system behavior
- decision-making under operational uncertainty
- leadership responsibility for cyber risk acceptance

These programs draw from Institute courses including:

- Stewards of Risk: Authorizing Officials
- Executive Cyber & AI Governance

Typical participants include:

- Authorizing Officials
- senior mission executives
- risk acceptance authorities
- senior cybersecurity leaders

These programs support leaders responsible for balancing cybersecurity risk with operational mission requirements.

Program Structure

Program Delivery

Sponsored cohort programs typically include:

- live executive instruction sessions
- scenario-based discussion exercises
- asynchronous learning modules

- real-world case studies
- certificate of completion

Cohorts typically include 25–40 participants and are delivered over three (3) to ten (10) weeks.

Programs may be tailored to the sponsor's ecosystem or mission community.

Professional Education Credit Alignment

Institute programs are designed to support the continuing professional education needs of cybersecurity and technology professionals. Where appropriate, participants may self-report continuing professional education (CPE) hours for professional certifications. Participants are responsible for reporting applicable credits to their respective certification bodies in accordance with those organizations' reporting requirements.

Benefits for Industry Sponsors

Organizations support Institute cohort programs because they strengthen the broader cybersecurity ecosystem.

Ecosystem Enablement

Partners gain a deeper understanding of cybersecurity authorization environments.

Government Customer Education

Government participants gain structured education on cybersecurity governance and authorization decision-making.

Market Enablement

Stakeholders accelerate the adoption of their technologies within mission environments.

Thought Leadership

Sponsors demonstrate leadership in supporting cybersecurity governance education.

About the Institute

The Institute for Cyber Executive Education provides executive-level education focused on cybersecurity governance, system authorization, and mission risk decision-making.

Institute programs emphasize practical decision frameworks rather than compliance checklists and are designed for professionals responsible for governing and operating complex cyber systems.

Programs draw on decades of experience across government, industry, information systems, and academic environments and reflect the evolving challenges of modern cyber operations.

Partnership Inquiries

Organizations interested in sponsoring cohort programs or exploring partnership opportunities are invited to contact the Institute via the website.

Additional information is available at:

www.instituteforcyberexecutiveeducation.org

