CYBER CENTER OF EXCELLENCE

Governance, Risk, and Compliance Professional

FOCUSED LEARNING PATH

⏱ self-paced training
🤝 in-person training

Role Description

A Governance, Risk, and Compliance (GRC) professional plays a key role in ensuring that organizational security practices align with established frameworks, policies, and regulatory requirements. This role focuses on interpreting risk, applying structured control frameworks, and supporting the development and assessment of security and privacy controls. Individuals in this space tend to be detail-oriented, process-driven, and comfortable working across technical and non-technical teams to translate requirements into actionable security practices. Their work helps ensure accountability, consistency, and continuous improvement across the cybersecurity program.

For support in accessing hands-on training opportunities or coordinating practical experience related to this development path, individuals or supervisors may reach out to Raymond.Girdler@arkansas.gov.

Building Foundational RMF Knowledge

- RMF Introductory Course (NIST SP 800-37) (3 hours) ⏱

Understanding Security and Privacy Controls

- Security and Privacy Controls Introductory Course (NIST SP 800-53) (1 hour) ⏱
- Control Baselines Introductory Course (NIST SP 800-53B) (45 minutes) ⏱

Assessing Security and Privacy Controls

- Assessing Security and Privacy Controls Introductory Course (NIST SP 800-53A) (1 hour) ⏱
- Certified Cybersecurity Rubric Evaluator (NIST CSF) (3 hours) ⏱

Practical Experience and Skill Application

- Participate in policy, standard, and procedure reviews as part of the annual governance cycle
- Complete an evaluation of internal controls to ensure alignment with regulatory requirements and organizational risk management practices
- Support external audits by assisting with evidence collection and gaining exposure to audit procedures
- Participate in assessing and approving risks related to application development, third-party tools, services, and equipment

Baseline Cybersecurity Knowledge Development

These online certification paths and foundational courses are considerations to support the development of foundational cybersecurity knowledge for individuals new to the field or transitioning into Governance, Risk, and Compliance roles, particularly where skills may need strengthening before entering GRC responsibilities.

- Cisco NetAcad Junior Cybersecurity Analyst (120 hours) ⏱
- Grow with Google: Google Cybersecurity (133 hours) ⏱
- NCPC Comprehensive Cybersecurity Defense (32 hours) 🤝