



## GRC Analyst

**Job Code:** 8282

**Salary Grade:** S09

**FLSA Status:** Exempt

*The following statements are designed to outline the general functions and typical responsibility levels associated with positions in this classification. They are not intended to serve as an exhaustive list of specific duties or requirements for individual positions assigned to this classification.*

### Duties and Responsibilities

Responsible for ensuring the organization's information systems and processes align with established cybersecurity, privacy, and regulatory standards. This role conducts in-depth security consultations and risk assessments to evaluate the effectiveness of security controls, identify vulnerabilities, and recommend mitigation strategies.

- Conducts security consultations to evaluate the effectiveness of security controls, identify risks, and recommend mitigation strategies.
- Manages the security exception process by documenting, reviewing, and verifying deviations from established security postures.
- Supports organizational compliance with cybersecurity, privacy, and data protection requirements.
- Performs and prepares risk assessments for software, networks, systems, and third-party vendors.
- Coordinates and produces records in response to Open Records requests.
- Evaluates new and existing services for compliance with security, privacy, and regulatory obligations.
- Assess systems and networks for configuration compliance, policy alignment, and potential security gaps.
- Performs independent assessments of management, operational, and technical controls to determine overall effectiveness.
- Collects, preserves, and documents digital evidence in support of investigations and preservation holds.
- Performs other duties as assigned

### Minimum Qualifications

**Education:**

- Bachelor's Degree in Computer Science, Information Technology, or related field.

**Equivalency/Substitution:**

Experience or a combination of education & related experience can be considered in lieu of degree. A one-to-one ratio is used to determine the number of years of experience required in place of a degree.

**Experience:**

- None

**Certifications or Licenses:**

- None

**Verification of education and licensure (if applicable) will be required if selected for hire.**

### Knowledge, Skills, and Abilities

- Ability to perform effectively in high-pressure, fast-paced environments.
- In-depth understanding of cybersecurity frameworks and standards
- Strong verbal and written communication skills, with the ability to convey complex information clearly to both technical and non-technical audiences.
- Excellent interpersonal and mentoring skills, with the ability to teach and guide others.
- Familiarity with regulatory and compliance requirements
- Understanding of network and system architecture, including common security configurations and vulnerabilities
- Strong analytical and problem-solving skills for identifying security risks and evaluating mitigation strategies
- Skilled in using risk assessment and compliance tools, vulnerability scanners, and GRC platforms.
- Ability to effectively interpret and apply security policies, procedures, and technical standards
- Ability to assess technical environments for compliance with security and privacy requirements
- Ability to maintain confidentiality and handle sensitive information with discretion
- Ability to adapt to changing technologies, threats, and regulatory landscapes

### Working Conditions



## JOB DESCRIPTION

# The UNIVERSITY of OKLAHOMA

- Requires extended periods of sitting, working at a computer, and using a phone.
- Requires sound judgment under pressure and the ability to manage multiple competing priorities effectively.
- Office Work Environment.
- Occasional evening, weekend, or on-call availability during critical incidents or high-severity events.

Printed Date: 07/10/2026