GRC Analyst/Manager Job Description Template

Last reviewed: September 2017

Recommendations if you are developing a job announcement or description for your institution:

1. Review the *sample* GRC Analyst/Manager job description (below).
2. Review the National Cybersecurity Workforce Framework published by NIST, which includes *sample job titles* and *key tasks*.
3. Review the 2016 IT Workforce in Higher Education research hub for the most recent EDUCAUSE research on the evolving IT workforce needed to support contemporary models of IT service delivery.

The following job description template is provided to help you get started on drafting a similar job description at your institution. It is intended to be illustrative and serve as a representative sample of the tasks that might be required for a particular role. It may not be inclusive of all job functions or knowledge, skills, and abilities that your institution requires in a particular role, or it may be overbroad for the position that you are designing. The template was designed so that you can add the example job functions, and knowledge, skills, and abilities statements into your own institutional job description template, and then augment the general items included in this template with your own specific institutional, role, and/or task needs.

GRC Analyst/Manager Job Description Template

Institution Name

Title (e.g., Governance, Risk, and Compliance Analyst or Manager)

Institution's Job or Reference #

Summary: The Governance, Risk, and Compliance [Analyst|Manager] is responsible for the assessing and documenting of the [institution]'s compliance and risk posture as they relate to the its information assets.

The purpose of this position is to provide highly skilled technical and information security expertise for development and implementation of the information security risk management program. Responsibilities require leadership and project management experience, as well as expertise to ensure effective system-wide security analysis; intrusion detection; standards and testing; risk assessment; awareness and education; and development of policies, standards and guidelines.

Reporting position: The GRC [Analyst|Manager] reports to the [Chief Information Security/Compliance Officer or Director of Information Security/Risk].

For more information: For complete details and to apply, please visit: <<Institution's URL>>

Duties and Responsibilities

Leadership

- Perform other duties as assigned to ensure the smooth functioning of the department and maintain the reputation of the organization as a viable business partner.
- Recommend programmatic and technical directions and operate with a high degree of independence in matters relating to the investigation, impact, and analysis of security incidents, decisions regarding risk, and measures for computer and network security.
- Operate with a high degree of independence with regard to project management activities, including development of project plans and budget /resource estimates.

Risk

- Lead the development and implementation of the system-wide risk management function of the information security program to ensure information security risks are identified and monitored.
- Internally assess, evaluate and make recommendations to management regarding the adequacy of the security controls for the University's information and technology systems.

Policy/Compliance

- Lead the system-wide information security compliance program, ensuring IT activities, processes, and procedures meet defined requirements, policies and regulations.
- Develop and implement effective and reasonable policies and practices to secure protected and sensitive data and ensure information security and compliance with relevant legislation and legal interpretation.
- Execute strategy for dealing with increasing number of audits, compliance checks and external assessment processes for internal/external auditors, PCI DSS, ITAR, HIPAA, NIST 800-171 and FISMA

Outreach/Awareness

- Interacts in both oral and written communications with all levels of System staff including; Computer center staff, developers and other ITS staff, campus technical staff, general counsel, auditors, and all System staff and students and technology vendors and contractors, in matters related to information security and security awareness materials.

Audit

- Work with Internal Audit, State Board of Regents, Auditor General's Office and outside consultants as appropriate on required security assessments and audits
- Coordinate and track all information technology and security related audits including scope of audits, colleges/units involved, timelines, auditing agencies and outcomes. Work with auditors as appropriate to keep audit focus in scope, maintain excellent relationships with audit entities and provide a consistent perspective that continually puts the institution in its best light. Provide guidance, evaluation and advocacy on audit responses.

Problem-Solving Skills

- Must be able to assess computer hardware, software, and systems for security risks or violations and work with ITS and campus staff and technology vendors to recommend solutions. Develop strategies to address awareness and training for all stakeholders as well as technical solutions. Must be able to assess the status of complex multi-location projects as well as identify and implement appropriate corrective measures to resolve issues as they arise. Must have a strong customer service orientation and the ability to project that attitude to customers in remote locations.

Contingency planning (IR, BC, DR)

- <<If applicable, duties and responsibilities statement for this section goes here.>>

Knowledge, Skills, and Abilities

Minimum Qualifications

- <<x>> years of advanced IT skills with high level of information security experience and expertise
- Knowledge of information security risk management frameworks and compliance practices.
- Knowledge of securing network technologies, client, and server operating systems.
- Ability to develop security standards and guidelines based on best practices and industry standards
- Experience responding to, analyzing, and communicating information security incidents
- <<x>> years of planning and managing security projects
- Excellent interpersonal, communication, and presentation skills, including formal report writing experience
- Understanding of common security standards and regulations relating to a higher education environment (e.g., PCI DSS, FERPA, ISO2700x, etc.)
- Must be well versed with laws affecting the higher education environment in the following areas:
    - Student Privacy
    - Health Care
    - Finance
    - Research Compliance
    - State Regulations

Preferred Qualifications

- Bachelor’s degree in information technology or other related field
- Information security experience in higher education or state/local government
- Skills in documenting risk and compliance activities
- Information security related training or certifications such as CISSP or CRISC
- Experience performing information security audits or risk assessments
- Familiarity with security auditing processes
- Must be familiar with dashboard creation
- Must have an understanding of campus policy development and dissemination

*PLEASE NOTE: In order to receive proper consideration, applications must be submitted directly via the **Institution's** career site. Applications submitted via any other source will not be considered.*

The **Institution** is an EEO/AA: M/W/D/V (Equal Opportunity/Affirmative Action Employer: Male/Female/Disabled/Veteran) Employer.
