

Job Title: **InfoSecurity GRC Engineer III**
Job Family: **IT Administrative**
Pay Program: **Administrative**
Typical Work Year: **12 months**

Job Code: **260606**
FLSA Status: **Ex- C**
Pay Range: **L09**

SUMMARY: The InfoSecurity GRC (Governance, Risk, Compliance) Engineer III is a key contributor to the District's GRC and data governance efforts, bringing advanced experience in technical auditing, DLP administration, and framework alignment. This position collaborates closely with internal departments and external vendors to evaluate and mitigate complex technical risks. By actively contributing to the design of security policies and performing thorough risk assessments, they ensure IT leadership receives timely, actionable information to safeguard District digital assets.

ESSENTIAL DUTIES AND RESPONSIBILITIES: *To perform this job successfully, an individual must be able to perform each essential duty satisfactorily. The requirements listed below are representative of the knowledge, skill and/or ability required. Reasonable accommodation may be made to enable individuals with disabilities to perform the essential functions.*

Job Tasks Descriptions	Frequency	% of Time
1. Strategy, Policy Design & Regulatory Assurance: Assist in or lead the development of District information security strategy and policies to ensure overall regulatory compliance.	D	15%
2. Technology Risk Assessment: Evaluate technology requests (software, hardware, and Chrome extensions) for security risks and privacy compliance.	D	15%
3. Remediation Management & Vendor Coordination: Manage technology risk remediation efforts, working with vendors and IT teams to ensure requested systems meet District security standards.	D	15%
4. Reporting & Governance Documentation: Generate technical reports on system vulnerabilities, threat landscapes, and technology risk profiles to maintain transparency in governance operations.	D	10%
5. DLP Policy, Data Classification & Technical Controls: Collaborate with stakeholders to design DLP policies, execute data classification tasks, and implement technical security controls.	D	10%
6. Technical Auditing & Compliance: Conduct technical compliance audits of District systems and monitor for security policy or privacy violations.	D	10%
7. User Awareness Implementation: Assist or lead in the development and implementation of awareness programs to educate staff and students on data security, privacy, and District policies.	D	5%
8. Daily Alarm Monitoring & Alert Triage: Monitor daily security alarms, review system dashboards, and triage incoming automated alerts to identify potential risks or incidents for immediate resolution or escalation.	D	5%
9. Ticket Management & Support Resolution: Manage, resolve, or escalate routine technical support tickets related to information governance, risk assessments, privacy inquiries, and basic access controls.	D	5%
10. Infrastructure Architecture & Secure Frameworks: Architect and engineer robust and secure frameworks for technology infrastructure and data classification systems.	D	5%
11. Perform other duties as assigned.	D	5%
TOTAL		100%

EDUCATION AND RELATED WORK EXPERIENCE:

- Bachelor's degree in Computer Science, Information Systems, Cybersecurity, or a related field (Four years of similar experience may substitute).
- Strong knowledge in developing cybersecurity policies, governing compliance frameworks, and third-party risk management.
- Four to six years of progressive experience in IT operations, including a minimum of two years' experience in GRC programs, IT auditing, or risk management.

LICENSES, REGISTRATIONS or CERTIFICATIONS:

- Criminal background check required for hire.
- Preference for intermediate governance, risk, or data privacy certifications such as CISA, CGRC, CIPP/US, etc.

TECHNICAL SKILLS, KNOWLEDGE & ABILITIES:***Technology Risk Assessment and Third-Party Risk***

- Conduct technical compliance audits across District systems and framework alignment (NIST/ISO).
- Help architect and design technical security controls and GRC frameworks.
- Execute data classification projects and identify sensitive student and staff information.
- Perform comprehensive risk analysis and help with system hardening.

Data Loss Prevention (DLP) and Monitoring

- Help with the design and implementation of Data Loss Prevention (DLP) policies and alert orchestration.
- Utilize key technologies such as SIEM and endpoint protection to identify policy violations.

Governance, Compliance, and Awareness

- Help lead the adherence to regulatory standards including FERPA, COPPA, and CIPA.
- Help lead the development of user awareness programs.
- Uphold strict confidentiality when dealing with sensitive information.
- Help lead in the creation of Standards and Policies across the District.

General Administrative and Technical Skills and Abilities:

- Participate in on-call rotation responding to urgent issues during off hours.
- Communicate effectively with both technical and non-technical personnel to coordinate activities and deliver clear technical solutions.
- Work collaboratively with diverse groups, fostering an inclusive environment that respects differences in culture and background.
- Uphold confidentiality across all job functions, particularly when dealing with sensitive information.
- Stay informed of District policies, standards, and training related to data quality, privacy, and cybersecurity, ensuring compliance with relevant guidelines for student and staff data.
- Adhere to Board of Education and Superintendent Policies, as well as department and building procedures.
- Recognize workplace safety as a priority, following safety protocols, using appropriate safety equipment, and reporting unsafe conditions to supervisors.

REPORTING RELATIONSHIPS & DIRECTION/GUIDANCE:

	POSITION TITLE	JOB CODE
Reports to:	Information Security Manager	130903

	POSITION TITLE	# of EMPLOYEES	JOB CODE
Direct reports:	This job has no direct supervisory responsibilities.		

BUDGET AND/OR RESOURCE RESPONSIBILITY:

- None

PHYSICAL REQUIREMENTS & WORKING CONDITIONS: *The physical demands, work environmental factors and mental functions described below are representative of those that must be met by an employee to successfully perform the essential functions of this job. Reasonable accommodation may be made to enable individuals with disabilities to perform the essential functions.*

PHYSICAL ACTIVITIES:	Amount of Time			
	None	Under 1/3	1/3 to 2/3	Over 2/3
Stand		X		
Walk		X		
Sit				X
Use hands and fingers to handle or feel				X
Reach with hands and arms		X		
Climb or balance		X		
Stoop, kneel, crouch, or crawl		X		
Talk			X	
Hear			X	
Taste	X			
Smell	X			

WEIGHT and FORCE DEMANDS:	Amount of Time			
	None	Under 1/3	1/3 to 2/3	Over 2/3
Up to 10 pounds			X	
Up to 25 pounds			X	
Up to 50 pounds	X			
51 to 100 pounds	X			
More than 100 pounds	X			

MENTAL FUNCTIONS:	Amount of Time			
	None	Under 1/3	1/3 to 2/3	Over 2/3
Compare				X
Analyze				X
Communicate				X
Copy		X		
Coordinate			X	
Instruct		X		
Compute				X
Synthesize		X		
Evaluate				X
Interpersonal Skills			X	
Compile				X
Negotiate			X	

WORK ENVIRONMENT:	Amount of Time			
	None	Under 1/3	1/3 to 2/3	Over 2/3
Wet or humid conditions (non-weather)	X			
Work near moving mechanical parts	X			
Work in high, precarious places	X			
Fumes or airborne particles	X			
Toxic or caustic chemicals	X			
Outdoor weather conditions	X			
Extreme cold (non-weather)	X			
Extreme heat (non-weather)	X			
Risk of electrical shock		X		
Work with explosives	X			
Risk of radiation	X			
Vibration	X			

VISION DEMANDS:	Required
No special vision requirements.	
Close vision (clear vision at 20 inches or less)	X
Distance vision (clear vision at 20 feet or more)	X
Color vision (ability to identify and distinguish colors)	X
Peripheral vision	X
Depth perception	X
Ability to adjust focus	X

NOISE LEVEL:	Exposure Level
Very quiet	
Quiet	
Moderate	X
Loud	
Very Loud	