Adams12 Five Star Schools

Job Description
Prepared/Revised: **May 2026**

Job Title:	**InfoSecurity GRC Architect**	Job Code:	**060608**
Job Family:	**IT Administrative**	FLSA Status:	**Ex- C**
Pay Program:	**Administrative**	Pay Range:	**L14**
Typical Work Year:	**12 months**		

SUMMARY: The InfoSecurity GRC (Governance, Risk, Compliance) Architect serves as the premier subject matter expert and strategic lead for enterprise risk, compliance, and governance operations across the District. This executive-level engineering role drives the overarching information governance strategy, directly advising IT and District leadership on risk posture and regulatory alignment. They act as the primary architect for overarching security policies, driving cultural change, and providing high-level mentorship to the InfoSecurity GRC Engineering team. This position is Level V on InfoSecurity GRC Engineer career ladder.

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. **Strategic Governance Leadership:** Lead the development and execution of the District's overarching information governance strategy and recommend strategic directions to leadership.	D	30%
2. **Mentorship & Leadership (Expertise):** Provide guidance, mentorship, and subject matter expertise to junior team members on complex assessments, auditing, and privacy issues.	D	20%
3. **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%
4. **Infrastructure Architecture & Secure Frameworks:** Architect and engineer robust and secure frameworks for technology infrastructure and data classification systems.	D	10%
5. **Technology Risk Assessment:** Evaluate technology requests (software, hardware, and Chrome extensions) for security risks and privacy compliance.	D	5%
6. **DLP Policy, Data Classification & Technical Controls:** Collaborate with stakeholders to design DLP policies, execute data classification tasks, and implement technical security controls.	D	5%
7. **Technical Auditing & Compliance:** Conduct technical compliance audits of District systems and monitor for security policy or privacy violations.	D	5%
8. **Reporting & Governance Documentation:** Generate technical reports on system vulnerabilities, threat landscapes, and technology risk profiles to maintain transparency in governance operations.	D	5%
TOTAL		100%

EDUCATION AND RELATED WORK EXPERIENCE:

- Bachelor's degree in Computer Science, Information Systems, Cybersecurity, Law/Policy, or a related field (Master's degree highly preferred).
- Ten to twelve years of progressive experience in IT operations and enterprise architecture, including a minimum of six years functioning as a strategic partner in IT Governance, Risk Management, Compliance (GRC), or Data Privacy.

LICENSES, REGISTRATIONS or CERTIFICATIONS:

- Criminal background check required for hire.
- Advanced, executive-level industry certifications in enterprise risk and governance strongly preferred. Strong preference for advanced GRC and data privacy certifications such as CRISC, CISA, ISACA CISM, CIPT, CIPP/US, CISSP, etc.

TECHNICAL SKILLS, KNOWLEDGE & ABILITIES:

Technology Risk Assessment and Third-Party Risk

- Direct the overarching enterprise framework architecture, aligning District technology infrastructure to stringent federal frameworks (e.g., NIST CSF, ISO 27001).
- Oversee high-level risk assessments for strategic, district-wide technology initiatives and deployments.
- Serve as the primary technical authority in negotiations with high-level vendors regarding security capabilities and enterprise risk sharing.
- Architect and engineer robust and secure frameworks for technology infrastructure and data classification systems.

Data Loss Prevention (DLP) and Monitoring

- Direct the enterprise-wide data security strategy, ensuring advanced threat intelligence and DLP orchestration operate effectively at scale.
- Serve as the ultimate escalation point for severe data breaches, directing high-level incident response and recovery efforts.
- Collaborate with stakeholders to design DLP policies, execute data classification tasks, and implement technical security controls.

Governance, Compliance, and Awareness

- Serve as the premier subject matter expert and strategic lead for enterprise risk, compliance, and governance operations across the District.
- Act as the definitive authority and advocate for legal and regulatory adherence, ensuring robust enforcement of FERPA, COPPA, CIPA, and evolving state data privacy laws across all platforms.
- Translate highly technical risk metrics into actionable business intelligence and present strategic directions to District leadership and the Board of Education.
- Lead the development and execution of the District's overarching information governance strategy and recommend strategic directions to leadership.
- Assist in or lead the development of District information security strategy and policies to ensure overall regulatory compliance.
- Act as the primary architect for overarching security policies, driving cultural change, and providing high-level mentorship to the governance engineering team.
- Lead complex, cross-departmental initiatives while serving as a dedicated mentor and driving cultural change regarding data security across the entire organization.
- Provide guidance, mentorship, and subject matter expertise to junior team members on complex assessments, auditing, and privacy issues.
- Conduct technical compliance audits of District systems and monitor for security policy or privacy violations.
- Generate reports on system vulnerabilities and technology risk profiles to maintain transparency in governance operations.

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			

WORK ENVIRONMENT:	Amount of Time			
	None	Under 1/3	1/3 to 2/3	Over 2/3
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	