Cesar Mora

(512) 426-1091 • Location • cesarmora809@live.com • www.linkedin.com/in/cesarmmora/ • www.cesarmora.work

Cybersecurity GRC Analyst Profile

Certified CompTIA Security+ professional with ongoing CISA certification and hands-on experience managing complex projects covering cybersecurity assessments, risk management, data protection, information security, and incident response planning.

Well-prepared to leverage GRC skills and foster a culture of proactive risk mitigation. Highly capable of assessing and prioritizing organization-wide risks associated with information security and cybersecurity by reviewing and ensuring compliance with regulatory obligations and security policies. Experienced in carrying out risk assessment, threat analysis, malware detection, and incident response planning along with vulnerability management and security measures deployment to protect organization networks and data. Demonstrated ability to learn new skills, tools, and technologies as well as adapt to new environments.

Areas of Expertise

- Information Security & Cybersecurity
- Cloud Computing & Security
- Identity & Access Management (IAM)
- Data Loss Protection (DLP)
- Security Governance, Risk, & Compliance
- Cyber Security & Compliance Audits
- Third-Party Risk Management
- Team Leadership & Training
- Security Education & Awareness

Technical Proficiencies

Tools & Software:	Salesforce CRM, Perplexity (Advanced AI Platform), *do we have more tools/software to mention here?*
Frameworks & Regulations:	ISO, CIS Controls v8, NIST Cybersecurity Framework (CSF), GDPR, CCPA, HIPAA, PCI DSS

Education & Qualifications

ISACA CISA (Certified Information Security Auditor) | Issuer, Date – Progress

Advance Diploma | Pontificia Universidad Católica Madrey Maestra, Location, Date

CompTIA Security+ (AKYLADE Certified Cyber Resilience Fundamentals – A/CCRF) (Focuses on Concepts for NIST CSF 2.0 Implementation) **|** AKYLADE, 6/2024

AZ-900 (Azure Fundamentals) | Udemy, 7/2024

SC-900 (Azure Security & Compliance) | Issuer, Date

Training & Courses: Simply Cyber – GRC Analyst Master Class, Cybersecurity 101 / XM Cyber-Exposure Management Expert / Level Effect: Cybersecurity Foundation / Cybersecurity Foundations: Cybersecurity Fundamentals / Engaging Stakeholder for Success / Cybrary Certified Information Systems Auditor (CISA) / Fundamentals of PCI-DSS / IT Auditing & GRC / Incident Response Summit – Certificate of Attendance / Master the NIST Cybersecurity Framework

Key Projects

CompTIA Security+ 701 E-Book Month/Date to Month/Date

Developed a detailed CompTIA Security+ Certification Study Guide by utilizing AI Technology to optimize the beginners' learning experience, equipping learners with the skills and knowledge necessary for a certification journey and successful career in the field. Addressed every topic outlined in the official exam blueprint from risk management and incident response to cryptography and access control. Broke down intricate cybersecurity concepts into digestible terms using AI, supplemented with real-world examples and applications. Organized and presented the information using Perplexity, an advanced AI platform, which streamlined the learning journey.

Key Accomplishments:

- Contributed towards democratizing cybersecurity education with the AI-powered study guide, and provided a solid foundation for individuals seeking to make a positive impact in the industry.
- Managed the actual release of the guide, reaching thousands of users in less than a week.
- Ensured the resource availability without any cost, removing financial barriers to empower aspiring professionals with the tools and knowledge that build a more inclusive and capable workforce.

Case Study: Ascension Health Ransomware Attack (2024) – A NIST CSF 2.0 Analysis Month/Date to Month/Date

Demonstrated the effective application of NIST CSF 2.0 to enhance organizations' cybersecurity posture while using the Ascension Health ransomware attack as a case study. Identified gaps/improvement areas in Ascension's cybersecurity defenses and response mechanisms. Highlighted the flexibility and scalability of the NIST CSF 2.0 to address complex cybersecurity challenges and facilitate organizations with protecting sensitive data, mitigating risks, and ensuring operational continuity during evolving cyber threats.

Key Accomplishments:

- Completed the assessment focused on critical controls and categories, identified lessons learned, and recommended improvement areas to optimize future incident response and prevention efforts (RC.IM).
- Defined improvement actions for identity management, authentication, and access control measures (PR.AC).
- Recommend steps to reduce ransomware impacts (PR.DS) by evaluating data security protocols and backup/recovery capabilities.

Third-Party Risk Assessment: Global Tech Solutions Group (Critical Vendor) Month/Date to Month/Date

Led third-party risk assessment of a vendor, GTSG to identify 12 security vulnerabilities across the network, email, website, and policy domains along with 3 critical and 4 high-severity issues. Highlighted 2 high-risk data leaks, including sensitive health member data and exposed login credentials, API keys, and analytical information.

Key Accomplishments:

- Reduced 75% of risk exposure for the client by providing actionable remediation recommendations.
- Achieved a 90% accuracy rate in risk identification by using a combination of assessment techniques, including ISO 27001 questionnaire reviews, automated web scans, and third-party data leak analysis.

CIS v8 IG1 Data Security Evaluation: Star Sales Solutions Month/Date to Month/Date

Facilitated a tech company with a full security audit to establish security measures while using CIS V8 implementation group 1 Framework. Evaluated 56 controls across the organization in an effort to enhance data security and mitigate breach risks.

Key Accomplishments:

- Devised policies and procedures for the company based on risk assessment while maintaining compliance with applicable regulations such as GDPR/CCPA.
- Ensured cost-effective implementation of security measures for MFA, data privacy, backups, and software updates along with employee training and incident response plan.
- Produced a final assessment report to the stakeholders covering all the steps, findings, and recommendations.
- Formulated and executed remediation strategies for the security gaps in collaboration with the client organization.
- Enhanced clients' trust by implementing authentication best practices and data exposure prevention training.

Case 2: A Construction Company Gets Hammered by a Keylogger Month/Date to Month/Date

Completed a case study on a key topic 'Keylogging, Malware and Bank Fraud', examining the online banking and automated clearing house (ACH) breach incident, $550K worth of unauthorized transfers from company bank accounts in a week. Studied the approach of cyber-attacks used by cyber criminals – use of malware from phishing emails. The company recovered $200K, leaving a loss of $350K, where the bank drew $220K on the business line of credit for covering the fraudulent transfers. Identified the delay in company's response to the fraud – lack of cybersecurity plan and hiring a cybersecurity forensics firm instead of bringing in cybersecurity experts right away.

Key Accomplishments:

- Produced a detailed report detailing the strategy and a better response to the cyber-attack, including implementing a cybersecurity plan, bringing in experts right away, and notifying authorities/impacted parties.
- Emphasized the need for multi-factor authentication, restricted access to sensitive accounts, regular training, and ongoing assessment of specific cybersecurity threats, incident response planning, enhanced email/network security, system updates, and cyber insurance to reduce future risks and breaches.

Career Highlights

Cybersecurity GRC Trainer | StudyGRC – Remote Month/2024 to Present

Oversee a hands-on project to establish a full audit and assessment program from scratch with a focus on CSF 2.0 and PCI compliance while leading a team of 5 students. Engage with mentors to ensure fulfillment of specific needs of the mock company, providing real-life assessment scenarios to the students. Headed the team to plan and conduct risk and security assessments, develop mitigation strategies, evaluate the effectiveness, and produce detailed reports.

Key Accomplishments:

- Optimized incident response and risk mitigation strategies by carrying out a comprehensive NIST CSF 2.0 analysis of ransomware attacks, which enabled the identification of key vulnerabilities and provided actionable recommendations.
- Achieved a 200% increase in program participation by delivering engaging GRC training content on security awareness/compliance.

Additional Experience

Bilingual Regional Sales Manager | LLV Distribution – Austin, TX Month/2021 to Month/2024

- Led the team members to design a set of supply chain KPIs and performance dashboards covering metrics for on-time delivery, supplier quality, inventory turns, and customer satisfaction scores.

Sales Manager | Vivint – Austin, TX Month/2020 to Month/2021

- Initiated security assessment for a diverse clientele to uncover vulnerabilities and develop tailored solutions based on network-connected security devices and cloud-based monitoring platforms to reduce risks of intrusion, theft, and property damage.

Customer Sales Representative | Opcity Realtor – Austin, TX Month/2017 to Month/2020

- Ensured full compliance of customer data handling with the company's data privacy, information security guidelines, and applicable regulations such as GDPR and CCPA.