DIRECTOR OF INFORMATION SECURITY DIRECTOR OF INFORMATION SECURITY DIRECTOR OF INFORMATION SECURITY - EDUCAUSE Longmont, CO Work Experience DIRECTOR OF INFORMATION SECURITY EDUCAUSE 2018 to Present Key leader in the Enterprise Governance Risk and Compliance Committee (GRC) Developed the Cyber Security program from the ground up using a quantitative risk model for Operational risks.   Served as the designated Information Security Officer for regulatory compliance requirements such as GDPR, GLBA, HIPAA and PCI.   Managed cross-functional project teams in the development and implementation of technology initiatives including multifactor authentication, security awareness training and identity and access management.   Worked with leadership and operations to implement a comprehensive Data Privacy initiative and ensure defensible processes to protect customer identify and personal data.   Built an incident response and business continuity program to ensure consistent system and service delivery based on business impact and dynamic operational requirements. DIRECTOR OF IT EDUCAUSE 2017 to 2018 Championed the implementation of ITIL best practices throughout the IT department. Recruited, trained, and develop eight direct reports. Cultivate trust-based relationships with key stakeholders.   Decreased organizational risk by eliminating 20 legacy systems running unsupported operating systems and applications.   Reduced IT capital costs by replacing legacy on premise systems to the cloud, decreasing the number of vendor contracts, and encouraging staff to seek other cost-saving measures. CYBER SECURITY MANAGER EDUCAUSE 2016 to 2017 Built the first comprehensive cyber security program resulting in a significant reduction in risk and protection of the organization's highly regarded reputation in the Higher Education vertical.   Diminished risk by developing and implementing 28% of the CIS top 20 critical security controls.   Resolved a significant security weakness that affected the .EDU domain space by identifying and securing cross- functional organizational support from cyber security, executive management, application development, and network engineering. PROGRAM CHIEF INFORMATION SECURITY OFFICER DAKOTA CONSULTING, INC - Lakewood, CO 2015 to 2016 CONTRACTED TO THE DEPARTMENT OF THE INTERIOR (DOI)) Liaised, as the company's information systems security officer, between

federal customers and DOI-approved service providers to ensure the full compliance of security controls and responsibilities with the NIST's Risk Management Framework and the DOI's Cloud Implementation Program. Delivered status reports to key members of the DOI's Office of the Chief Information Officer (OCIO).

Won the DOI-OCIO's approval to utilize FEDRAMP-approved cloud service providers for their 18 bureaus and offices. Participated as a subject matter expert with bureau cloud migration and transition plans. Developed a standardized template that facilitated thorough and consistent delivery of risk assessment reports.

CHIEF INFORMATION SECURITY OFFICER / PROJECT MANAGER / FISMA ASSESSOR CHEROKEE SERVICES GROUP - Boulder, CO 2009 to 2015 CONTRACTED TO NOAA) Fulfilled multiple roles on behalf of NOAA that featured distinct responsibilities. As information systems security officer, headed up maintenance and risk management of the Earth System Research Lab (ESRL)'s IT security framework in collaboration with an 10-member team of IT security analysts. - Provided annual IT security training to 600 IT and scientific users to improve awareness. Appointed project manager to oversee the implementation of NOAA's multi-million-dollar, Department of Homeland Security-mandated Trusted Internet Connection project. Led deployment of multi-factor authentication smart cards across the NOAA Line Office and 12 additional locations. - Served as lead project manager for a 5-site, $20 million NOAA security project that was ultimately adopted by the Department of Commerce for all of its agencies. In the role of security assessor, conducted consulting and security assessments at four scientific research labs and delivered security training courses to 600 end users on topics that included the NIST Risk Management Framework, practical use of SANS 20 critical security controls, and ITIL best practices. - Developed creative and appropriate solutions for closing 200 previously documented IT Security audit findings (POA&Ms).

Education MBA in (Master of Business Administration), Management University of Colorado - Denver, CO BA in (Bachelor of Arts), Economics Colorado State University Skills CISSP (10+ years), Information Security (10+ years), It Security (10+ years), FISMA (10+ years), NIST Risk Management Framework (800-53) (8 years), SOX (7 years), Security Awareness (10+ years) Links http://www.linkedin.com/in/Timothy-OBrien-IT-Professional Certifications/Licenses Certified

Information Systems Security Professional (CISSP) 2002 to 2020 Certified Information Systems Auditor (CISA) 1996 to 2020 Project Management Professional (PMP) 2008 to 2020 Certified Bank Auditor (CBA) Certified Fraud Examiner (CFE) Certified Financial Services Auditor (CFSA) GIAC Certified Unix Security Administrator (GCUX) Additional Information CORE COMPETENCIES Ability to collaborate with diverse teams Excellent financial management Ability to deliver timely Strategically minded Project Management Professional Self-motivated Privacy focused Cyber risk mitigation Mission oriented   IT Governance IT Process Frameworks Solid Decision-Making Capacities   Staff Attraction/ Retention / Development NIST/FISMA/ITIL/CIS Excellent Communication Skills

Name: Andrew Mitchell

Email: marissa15@example.com

Phone: 001-851-390-7900