Adjunct Faculty Adjunct Faculty Governance, Risk, and Compliance Professional Shelby Charter Township, MI Certified Information Assurance Professional with 5+ years managing and implementing regulatory compliance, information technology audit, risk, IT governance, and security programs across a variety of industries, including government, automotive, healthcare, and finance. Project manager effective in leading, directing, and controlling technical, organizational change, security, and risk/audit engagement projects with success in implementation and time/financial targets. More than 13 years of progressive IT and Information security experience across areas of application development, risk assessment and audit, vulnerability management, regulatory and industry standards compliance (HIPAA, SOX, CJIS, FERPA Security Standards, IRS FTI, ISO 27000 series, NIST 800 series, PCI-DSS), disaster recovery and business continuity, cybersecurity policy and procedure development, identity and access management, and infrastructure administration (server, network, database). Work Experience Adjunct Faculty Capella University - Minneapolis, MN January 2019 to Present Highlights and Achievements: Business and Technology School instructor - Teach undergraduate information technology, health information management, and information security concepts. Classroom management - Provided coaching and mentoring to students to manage coursework. Graded using outcome-based recommendations to achieve capabilities for course and overall program. Management Consultant DPM Consulting Services - Troy, MI October 2016 to Present Highlights & Accomplishments: Security Control Assessor - Performed risk analysis using NIST 800-30 methodology of IT systems (web and Windows applications, network, transaction integrity, firewalls, IDS-IPS, SIEM, DR/BCP) and business process controls to assess HIPAA Privacy, Security, Breach Notification Rules, PCI-DSS, OWASP top ten, IRS 1075 Federal Taxpayer Information Safeguards, Michigan Office of Child Support Security, and FBI Criminal Justice Information Security Rule compliance. Managed documentation, work papers, and other audit support artifacts. Trained junior staff to perform security audits, validate control evidence, and document system security plans (SSPs). Created and presented final assessment report to stakeholders. Worked with system owners and business unit leaders to document risk mitigation decisions and plans of action and milestones (PoA&Ms).

Compliance Program Management - Developed and implemented the county's HIPAA and PCI-DSS compliance program strategy and implementation roadmap. Developed countywide policy and procedures. Obtained buy-in across county divisions to form compliance committee and working groups (cross-functional group of leaders from various county business and internal service functions). Facilitated committee and working group meetings, documenting decisions and actions. Managed risk mitigation activities and validated completed corrective action plans. Created and implemented program sustainability plans. Executed targeted privacy and security training for department-level, data custodians, privacy officers, and IT system administrators. Managed HIPAA privacy and security events from reporting to closure.   Vendor Risk Management - Worked with Purchasing to implement periodic vendor risk management audits, including policies, procedures, and communication templates. Drafted request for proposals (RFP), viewed RFP responses, vendor system security plans, and assessed vendor data security. Drafted scope of services in contracts, service level agreements (SLA), and master service agreements (MSAs).   Executive Reporting - Created audit and reporting dashboards using Microsoft (MS) SharePoint for stakeholders. Developed a HIPAA Compliance Maturity model to measure progress against compliance benchmarks.   Project Manager - Created compliance program business case and provided input to the countywide HIPAA policy and procedures, county resolution for Board of Commissioner approval. Managed compliance program budget to implement process improvements, technology enhancements, and develop a sustainability process. Created and managed compliance program and related projects using Clarity Workbench.   Security and Compliance Subject Matter Expert (SME) - Provided security expertise on IT projects to create cloud security design, update applications and technology infrastructure, and make revisions to enterprise architecture processes. Environment: Office 365, Amazon Web Services, Microsoft Azure, Window Server, Linux, Unix, Mainframe, SharePoint, Clarity PPM, Clarity Service Center, Nessus Security Suite, AD Audit Plus Adjunct Faculty Wayne County Community College - Detroit, MI January 2018 to April 2018 Highlights and Achievements: Instructional Designer - Developed and implemented course curriculum for the NIST Risk Management Framework (RMF) to prepare for the Certified

Authorization Professional (CAP) exam. Identified competencies needed to achieve understanding of material. Cybersecurity instructor - Taught project, risk, vulnerability management, and application development lifecycle concepts to students in applying the RMF. Classroom management - Provided coaching and mentoring to students to manage coursework. Graded using outcome-based recommendations to achieve capabilities for course and overall program. IT Governance Analyst Comerica Bank - Auburn Hills, MI April 2016 to October 2016 Assistant Vice President/Business Unit Risk Analyst II - IT Risk Assurance Services - Comerica Inc. Auburn Hills, MI IT Business Unit Risk Analyst - W3R Consulting (assigned to Comerica Inc.) Southfield, MI - Assessed technology and organizational readiness to implement COBIT 5 and FFIEC frameworks. Developed roadmap, policies, procedures, and work instructions to improve enterprise architecture maturity. Implemented Risk Assurance function within IT. IT Risk Analyst - Performed assurance monitoring testing of Windows/Unix/Linux server environment, Security hardware and auditing tools, web application, business continuity and disaster recovery, information backup, and security management controls. Performed SOX and PCI-DSS testing and monitoring. Documented and managed control design and operating effectiveness control deficiencies. Worked with system and process owners to develop corrective action plans and milestones. Provided coaching and mentoring to junior staff on assurance monitoring processes. IT Governance Program Metrics - Developed automated reporting dashboard using SharePoint to present executive and IT area reporting to stakeholders. IT Audit Tools - Developed SharePoint tool to implement risk control self-assessments to assist IT system and process owners in reporting self-identified audit issues. Monitored and tracked SIA issues to closure. Environment: Office 2013-2016, Windows, Linux, Unix, Mainframe, SharePoint 2013-2016, Changepoint, ServiceNow, Archer Information Security Governance, Risk, and Performance Lead Blue Cross Blue Shield of Michigan - Bingham Farms, MI July 2014 to September 2015 Bingham Farms, MI Jul 2014 to Sept 2015 Highlights & Accomplishments: Information Security Governance Lead -Facilitated Information Security Committee Board meetings. Developed and managed security governance and technical policies, standards, procedures, and work instructions. Mentored junior staff on department processes.

Processed third party security questionnaires and supporting documentation for corporate customers. Managed compliance and policies using Archer and MetricStream. Drafted, reviewed RFP process for new security tool vendors.   Risk Assessor - Assessed internal controls (network, application, process, transaction integrity) and vendor systems against controls framework to ensure privacy, security, and compliance. Performed assessments to vendor risk management, perimeter, and information security governance program to assess process capability and organizational maturity to implement HITRUST.   Security Training and Awareness - Executed security training and awareness activities for the organization through planned and ad hoc efforts. Topics included data classification, phishing and social engineering, secure application development, mobile and workstation security, online and social media behaviors, and password management. Performed assessments of workstation areas to ensure security of protected health (PHI) and non-public data in work areas and adherence to clean desk policy.   Security Program Metrics - Developed and managed key risk and performance indicators for information security program. Presented executive dashboards to stakeholders and the board of directors. Environment: Office 2013-2016, Windows, Linux, Unix, Mainframe, SharePoint 2013-2016, Project Server, BMC Remedy, Archer, MetricStream Audit, Risk, and Compliance Lead for Technology Infrastructure/Sr. IT Business Analyst Ally Financial - Detroit, MI July 2013 to March 2014 Highlights & Accomplishments: Audit Remediation - Lead, directed, and monitored internal and external audit findings for technology infrastructure. Coordinated internal and external audits. Selected external security assessors for PCI-DSS compliance. Managed security exceptions and risk acceptances. Coordinated risk control self-assessments and self-identified audit issues in OpenPages GRC and Archer.   Data Privacy Officer - Managed, maintained, and revised policies, standards, procedures, work instructions, and guidelines for the Data Protection & Privacy Program and its related activities. Implemented and monitored potential privacy events in Symantec Data Loss Prevention (DLP) tool. Manage data classification labeling, security standards, and processing objectives for new/existing technology and physical records. Performed privacy impact assessments for technology projects and onboarding vendors.   Compliance Program Management - Managed SOX quarterly access audits for

department. Documented security attestations for SOX compliance reporting. Coordinated GBLA privacy assessments for technology and business process. Worked with federal and state regulators in regulatory examinations. Managed and executed business continuity and disaster recovery plans/testing in SunGard Business Continuity software. Environment: Office 2013, Clarity PPM, Service Now, BMC Remedy, SunGard, Symantec DLP, Qualys SIEM, Archer, Windows Server, Linux, Unix, Mainframe, SharePoint 2013, OpenPages Other Work Experience MULTIPLE EMPLOYERS 2001 to 2013 assigned to FCA - Mopar Parts Division   Compliance Analyst, Saras Americas (assigned to Comerica Inc.)   Vendor MSP Implementation Business Systems Analyst, Tek Systems (assigned to Allegis Group)   Program Management Analyst, Indotronix International (assigned to ATOS Solutions)   Identity and Access Management Compliance Analyst, Ivantage Group (assigned to Flagstar Bank)   Business Systems Analyst, Millennium Software (assigned to Ford Credit)   Project Manager/Supply Chain Analyst, Snelling Personnel (Assigned to Nitto Denko Automotive)   Project Manager, Computer Merchant (assigned to Hewlett-Packard/General Motors Project)   System Administrator, Upper Room Ministries Education Master of Science in Information Technology in Cybersecurity specialization Walsh College June 2018 Bachelor of Business Administration in Business Management in Business Management Cleary University April 2013 Skills Linux (5 years), Microsoft sharepoint (5 years), Security (5 years), Sharepoint (5 years), Unix (5 years) Certifications/Licenses Certified Information Systems Security Professional (CISSP) September 2018 to September 2021 System Security Certified Practitioner (SSCP) May 2018 to May 2021 Healthcare Information Security and Privacy Practitioner (HCISPP) July 2018 to July 2021 Certified Information Security Manager (CISM) February 2018 to February 2021 Certified Authorization Professional (CAP) February 2018 to February 2021 COBIT 5 Foundation June 2016 to Present COBIT 5 Implementation July 2016 to Present

Name: Destiny Baker

Email: andreagilmore@example.net

Phone: +1-501-537-1720x20872