

## **EXECUTIVE SUMMARY:**

Mr. Schweyer is an accomplished Information Security Architect/Specialist that is highly motivated and experienced with expert proficiency in Information Security, development and execution of comprehensive IT security programs, and strategies to govern enterprise risk with a focus on safeguarding mission-critical systems and information. He has a comprehensive understanding of the skills needed to coordinate communications between colleagues, clients, and management and executives and he is skilled in establishing strategies that encourage the consistent achievement of project, service, and program milestones on-time and well within budget.

## **SKILLS OVERVIEW**

### **Areas of Expertise:**

Information Protection, Relationship Building, IT Architecture Analysis/Design, Project Management, Threat Assessment, Business Continuity, Cybersecurity, Application Security, IT Process Improvement, Strategic/Tactical Planning, Risk Management, Vendor Product Assessment, IT Security Policy, ISO 27001 Compliance, NIST RMF Compliance, Agile Software Development, Geospatial Information Systems

## **Education & Certifications**

ALGONQUIN COLLEGE - Information Systems Security Graduate Certificate

ACADIA UNIVERSITY – Undergraduate Studies in International Relations

UNIVERSITY of Toronto– Graduate Studies in International Relations

Certified Information Systems Security Professional (CISSP) ISC2 82271

Certified Authorization Professional (CAP) ISC2 82271

Certified Secure Software Development Lifecycle Professional (CSSLP) ISC2 82271

Certified Business Continuity Professional (CBCP) DRII 63776

Associate Member Business Continuity Institute (BCI) 008274

Open Web Application Security Project (OWASP) Conference, *San Francisco, 2015*

Certificate Clouding Security Knowledge (CCSK) Course, *Intrinsec, Ottawa, 2010*

Cyber Security Masters Course, *ECBG, Vienna, Austria 2010*

Vulnerability Assessment Course, *MIW/IntrinSec, Ottawa November 2010*

Gartner IT Security Summit, *London, UK, September 2009*

ISO 27001 Lead Auditor Course, *Veridion, Montreal PQ August 2008*

SANS Security Essentials Boot Camp (GSEC) - *SANS Institute, USA May 2008*

DoD Architecture Framework Course- *System Proposal Engineering Co, Vienna, Virginia 2005*

Senior Intelligence Officers Course - *Defense Intelligence Agency, Washington, D.C. 1998*

Exercise Agents Course - *National Reconnaissance Office, Dulles VA 1998*

## Professional History

### Dramstar Enterprises

*Owner and Chief Information System Security Consultant*

2005 - 2020

- Established this information technology security firm, achieving a demonstrated record of success with over 26 projects delivering Certifying and Accrediting (C&A)/Security Assessment and Authorization(SAA) using a variety of methodologies including NIST RMF, ISSIP, ISO 27000, and DIACAP; produced various IT security gap analysis; development of security strategies, system security architecture; security requirements traceability matrix; security test and evaluation; risk assessments; threat assessments; system security plans; security awareness training; policy and procedure development; and business continuity and disaster recovery planning. Business Continuity, Disaster Recovery and Contingency Planning work based on DRII, BCI and NIST 800-34 frameworks. Reported to the executive, senior management and technical levels with oral and written briefings and reports. Clients include the Department of Defense (DND), Elections Canada (EC), Correction Service Canada (CSC), Health Canada, Environment Canada, Public Works and Government Services Canada (PWGSC), Environment Canada, Canada Revenue Agency (CRA) and Shared Services Canada (SSC). Projects often included system interface with US systems with DoD, USAF, NGA and NRO.
- A selection of client projects include:

*TRA C&A Specialist with iFinex*

2020

- Led the preliminary ISO 27001 and SOC2 compliance audit and Threat and Risk Assessment (TRA) for iFinex Bitfinex cryptocurrency exchange. Bitfinex is a leading-edge cryptocurrency transaction application resident on the Tether Blockchain infrastructure. The purpose of assessment is to identify threats, associated vulnerabilities, evaluate existing ISO 27002 controls and safeguards against Open Web Application Security Project (OWASP) Top 10 software vulnerabilities of the Bitfinex suite of applications and SaaS, IaaS and PaaS cloud service providers.

*TRA C&A Specialist with Elections Canada*

2018 - 2019

- Led the SAA Project for the Geographic/Geospatial Information System (GIS) at Elections Canada. The GIS at Elections Canada is comprised of 28 applications and an underlying infrastructure of seven servers and three databases. The GIS is used to establish election districts and polling station boundaries. Work included developing a SAA Plan, which covered three years of work, the Statement of Acceptable Risk, Asset Categorization, Security Requirements Traceability Matrix (SRTM) for both the application and infrastructure/network layer and gathering evidence to support the SAA. GIS applications are transitioning from government datacenter to commercial cloud-based service.

*C&A Specialist/Director of Enterprise Application, DND*

2012 - 2018

- Led the application security strategy and program for a group of 18-30 developers who support enterprise applications such as GCCS-J and Modern Integrated Database (MIDB) on classified military systems integrated with US DoD. This project based on complex risk assessment. The SAA was based on NIST RMF standards to ensure US DoD connectivity. The strategy involved standardizing the static testing automation, providing developer focused training on application security threats and vulnerabilities, developing a configuration management program using ITIL frameworks and leading to automation of the configuration management process and developing and validating contingency planning. Assessment involves developing threat models for 15 applications using various vulnerability reports such as OWASP Top 10. Implemented SAA process in Agile software development process.
- Developed and implemented the Configuration Management Plan and process based on ITIL standards.
- Developed the BCP/DRP; conducted annual validation exercise. BCP/DRP based on DRI and BCI framework. COOP and ISCP based on NIST 800-34

- Conducts bi-annual Security Awareness Training tailored for application security based on OWASP Top 10.

*Canada Revenue Agency (CRA)/IT Continuity and Risk Management*

2016 - 2018

- A Senior IT Security Specialist assigned a variety of projects including SAA of the first Windows 10 deployment in Government of Canada (GC), implementing SAA in Agile SDLC, secure API, modernization and transformation of physical security services to network based (SCADA) system for 108 CRA Sites across Canada, and implementation of classified processing domain for the CRA.
- Developed policy paper for integration of GC SAA process for implementation of Agile software development CRA has over 1000 COTS and GOTS applications under development.
- Led the SAA Project for Windows 10 transition using NIST RMF and ISSIP. The first transition to Windows 10 in the Government of Canada
- Responsible for development of policy, test procedures and standards for CRA instance in Government of Canada API Store
- Led application security assessment project for Chubb Director FX and KanTech EntraPass physical security software for integration into CRA network.

*Defense Research and Development Canada*

2010 -2013 / 2014 - 2016

- Led the IT Security Project for the Defense Research and Development Canada (DRDC), responsible for implementing cyber-security strategy and risk mitigation program in response to an event (link below).
- (<https://www.cbc.ca/news/politics/foreign-hackers-attack-canadian-government-1.982618>)
- Achievements included Security Gap Analysis of the Defense Research Establish Network leading to an IT security strategy and implementation of that strategy including the development of Security Architecture and managing all C&A activities.
- Led the SAA project for the Virtual Laboratory (VL), a US government (NRO) led global collaborative research environment. SAA based on NIST Risk Management Framework and NIST 800-53 controls to ensure conformity to US SAA requirements.

*DND/Military Pension Renewal Project*

2013 - 2016

- Led IT Security project to interface the DND Central Computerized Pay System (CCPS) with GC pension system.
- Played leading role in ensuring the Designated Private Key Infrastructure (PKI) was cross certified to the GC Federal Bridge to ensure full functionality of the MPR resulting in SA&A Report and recommendation.

*Mapping and Charting Establishment (MCE)*

2008 - 2014

- IT Security project leader responsible to the senior engineering and military command for implementing an IT security program of three systems, two of which were classified. Work included implementing an IT security strategy and plan leading to Certification and Accreditation of unclassified and classified systems. Those systems support internationally deployed Canadian military forces and operate at high availability. MCE is closely associated with the US National Geospatial Agency (NGA), whose NIST and FIPS requirements were considered for integration and interface purposes.

*AIR FORCE COMMAND AND CONTROL INFORMATION SYSTEM (AFFCIS)*

2006 – 2013

- IT Security Manager responsible for security architecture and C&A activities of Lockheed-Martin Project team implementing \$49MM AFFCIS/Joint Command System (JCS) Air Project. Led project IT security project from conception through development, deployment, production and disposal. Completed risk assessments included AFFCIS Enterprise Network, Secure deployable suite, NORAD Extranet using DIACAP framework, TBMCS (GCCS-N), and Canadian Forces Weather and Oceanographic System Interface. Was also the IT security advisor to the Commander 1 Canadian Air Division ISSO on a variety of IS security matters including incidence response and investigations.

**Department of National Defense**

