**Resume**

**For**

**Dr. Al Lively**

Monroe, Georgia 30655

Phone: (Cell) (404) 606-7915, Email: [al.lively@comcast.net](mailto:al.lively@comcast.net)

**Summary**: Thirty years of information technology security and audit experience. Equipped with a Ph.D. in Computer and Information Security, coupled with extensive education, training, knowledge, management, and experience in the evaluation and assessment of legislative, regulatory, and international best practices of organizations’ information systems’ security and control practices.

**Work Experience:**

Recall Corporation

Norcross, Ga.

Employed: (01/15 – 01/16)

Duties and Accomplishments - IT Senior Manager – Governance and Compliance

* Developed corporate Governance and Compliance program of international organization.
* Developed and maintained corporate security policies
* Developed and administered security awareness program for over 5000 employees and contractors
* Reviewed and approved all system projects and vendor contractors for compliance with local and international standards
* Coordinated with external auditors and certifiers for effective review SOC, HIPAA, NIST, and PCI-DSS of internal operations compliance and remediation of deficiencies.

**Security Consultant/Contractor/Professor (3/07 – 7/11 and 6/12 – Present)**

Contractors Supported/Partnered:

Clearbridgetech (November 2016 – February 2017)

Enterprise IT Solutions (January 2016 – May 2016)

Apex Systems (July 2014 – January 2015)

University of Maryland University College (Adjunct Professor) (May 2011 – May 2013)

Conscious Security, Inc. (April 2013 – May 2014)

Rapid External Solutions (June 2012 – October 2012)

Northrop Grumman Corporation (August 2010 – July 2011)

Lockheed Martin Corporation (May 2008 – March 2009) & (August 2009 – August 2010)

Computech Resources International (March 2009 – August 2009)

Jefferson Wells International (February 2007 – February 2008)

Contractor Clients Supported:

Banner Healthcare of Arizona

South Carolina Department of Health and Human Services (SCDHHS)

Georgia State Accounting Office (SAO)

Centers for Disease Control and Prevention (CDC)

International Business Machines (IBM)

Department of Defense (DoD) Hq. US Army

Department of Defense (DoD) Marine Corps Systems Command (MARCORSYSCOM)

Centers for Medicare and Medicaid Services (CMS)

Contract Responsibilities/Tasks Supported:

* Developing Security Policies and Procedures for compliance with HIPAA and PCI-DSS.
* Assisted South Carolina Department of Health and Human Services (SCDHHS) Office of Information Assurance (OIA) with identifying, evaluating, and documenting, according to State, NIST, HIPAA, IRS and CMS (MARS-E) standards, the required controls and proper implementations of the State’s Replacement Medicaid Management Information System (RMMIS). Coordinated with CISO, CIO, Enterprise Architect, DBA, programmers, and Program Director to ensure RMMIS achieves sufficient security and privacy objectives.
* Conducted analyses of organization security posture and risk exposure in preparation for designing and developing organization security policies and standards for compliance with Federal Information Security Management Act (FISMA). Designed and developed security policies and standards for statewide PeopleSoft ERP and the enterprise Georgia State Accounting Office.
* Supervised Information Assurance staff tasked with preparing certification and accreditation documentation in support of the Marine Corps’ Logistics Information System (14 applications), evaluating and assuring compliance with FISMA, DoDI 8500.2, Information Assurance Implementation, and DoD Information Assurance Certification and Accreditation Process (DIACAP). Conducted security validation tests of systems and applications using DISA STIG tools and templates. Assisted in transition from DIACAP to NIST RMF.
* Worked with IBM (prime contractor) in completing Audit Readiness testing and evaluating of security controls of Army Headquarters newly implemented General Fund Enterprise Business System (GFEBS), hosted on SAP platforms.
* Reviewed NIST Special Publications to ensure CDC security certification policies and procedures adequately and effectively met FISMA computer and network security requirements, and make recommendations for compliance, when applicable.
* Coordinated with Business, Technical, and Security Stewards and prepared security certification documents of CDC applications, ensuring applications complied with Federal Information Security Management Act (FISMA), US Federal Privacy Act, and CDC Office of Chief Information Security Officer (OCISO) policies and standards requirements.
* Conducted risk assessments and produced reports of results for CDC Designated Approving Authority (DAA).
* Assessed adequacy of CDC applications’ Business Continuity Plans; participated and evaluated tests of plans for sufficiency in meeting recovery objectives.
* Conducted investigations of workstation and/or network security incidents, determined root causes of incidents, took actions to mitigate threats, and counseled CDC employees of risk-prone actions to avoid.
* Trained and lead Contractor staff of Security Analysts in Quality Assurance functions, ensuring application certification packages submitted by Information System Security Officers (ISSOs) met CDC, HHS, and NIST security standards and adequately documented risks, controls, vulnerabilities, and planned actions for mitigating control weaknesses.
* Coordinated with and advised CDC personnel regarding correct methods in preparing certification documents for CDC applications according to Federal Information Security Management Act (FISMA) requirements and provided accreditation advice to Certification Authority (CA).
* Performed annual FISMA IT Audit of U.S. Department of Health and Human Services (HHS) Center for Medicare and Medicaid Services (CMS) infrastructure security and application controls including verification of effective Software Development Life Cycle (SDLC) and Configuration Management (CM) controls according to FISCAM and NIST guidelines, in support of Ernst & Young LLP (prime contractor) audit of HHS financial statements and FISMA compliance.
* Conducted business continuity and disaster recovery assessments of international credit card processing corporation in support and preparation of PCI DSS assessment. Provided assistance in identifying strengths and weaknesses in continuing operations of key business process areas and assisted management in design of effective recovery controls.
* Developed and implemented SOX IS risk assessment program for manufacturing client with plants located throughout the world. Performed SOX application testing at several manufacturing plants.
* As Assistant Professor, instructed online courses in various security subjects for undergraduate and graduate students.

**Centers for Disease Control and Prevention (CDC)**

Atlanta, Georgia

Employed: 7/11 – 6/12

Duties and Accomplishments: Certification and Accreditation (C&A) Security Analyst

* Coordinated with Business and Technical Stewards and prepared security certification documents of CDC applications, ensuring applications comply with Federal Information Security Management Act (FISMA) and CDC Office of Chief Information Security Officer (OCISO) requirements.
* Conducted risk assessments and produced reports for Designated Approving Authority (DAA). Assessed adequacy of Business Continuity Plans and participated in tests of security safeguards.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Georgia Department of Audits**

Atlanta, Georgia

Employed: 9/99-3/07

Duties and Accomplishments: Information Technology Auditor

* Assisted audit management with design of newly created IT Audit function. Developed mission, policies, standards, and audit plans consistent with ISO, COBIT, NIST, GAO, and SANS industry guidance. Assisted in recruitment of IT Audit staff to fill newly created positions.
* Conducted audits and reviews of state agency management identity, authentication, and access controls over computer systems.
* Performed reviews of State Health Clinics for compliance to HIPAA security and privacy rules.
* Advised agency management of appropriate information and computer system security controls, including planning, analysis, design, development, testing, conversion, and operations.
* Wrote audit reports for distribution to agency and other State departments identifying strengths and weaknesses in locally developed or purchased software.
* Planned, organized and reviewed work of other information technology team members, including PeopleSoft implementation teams
* Trained and mentored other IT audit team members in audit strategy, procedures and standards.

----------------------------------------------------------------

**Georgia Institute of Technology**

Atlanta, Georgia

Employed: 10/90-9/99

Duties and Accomplishments: Information Technology Auditor

* Designed newly created IT Audit function for Institute. Developed mission, policies, standards, procedures, and audit plans consistent with industry best practices.
* Advised Institute management of appropriate information and computer security controls, including planning, analysis, design, development, testing, conversion, and operations.
* Wrote audit reports for distribution to Institute leaders identifying strengths and weaknesses in locally developed or purchased software.
* Evaluated adequacy of system management procedures regarding the acquisition, analysis, design, development, and testing of application systems.
* Participated in establishment and operation of software quality assurance function responsible for developing and implementing software coding standards and software development life cycle (SDLC) methodology, including standards for analysis, design, coding, testing, and migration of computer programs.
* Participated in the implementation of Institute’s PeopleSoft Human Resources ERP application. Acted as consultant to information technology management regarding appropriate confidentiality, integrity, and availability program requirements.
* Assisted in developing the first University System of Georgia Computer and Network Security Policy for the Institute.

---------------------------------------------------------------------

**U. S. Air Force**

The Pentagon

Washington, DC

Retired Rank: Major

Assigned: 5/86-11/90

Duties and Accomplishments: Information Systems Security Officer

* Supervised staff of computer security specialists responsible for the security of the National Military Command Center (NMCC) and the Alternate National Military Command Center (ANMCC) computing systems. Verified that operating system and application programs were properly configured for reliable and secure operations.

**Education:**

Georgia State University

Atlanta, Georgia

Bachelor of Science, Major-Mathematics, Emphasis in Statistics

Minor-Psychology

------------------------------------------------------------

University of Central Oklahoma

Edmond, Oklahoma

Master of Business Administration

------------------------------------------------------------

Northcentral University

Prescott Valley, Arizona

Ph.D. (Concentration): Computer and Information Security

Dissertation: Exploring the Effects of the Ada Programming Language on Software Quality

**Other Qualifications:**

Assistant Professor – Online, Web-based, information security instruction

Working knowledge of the following subjects/products:

SOX Section 404, ISO 17799, ISO 27001/2, FISCAM, HIPAA, FISMA, RMF, PCI-DSS, DIACAP, FERPA, COBIT, NIST SP 800-37, NIST SP 800-53, and NIST SP 800-53A, CMS MARS-E.

Oracle DBMS, Microsoft Office

Application Security AppDetective

Nessus Vulnerability Scanner

Microsoft Windows OS

Oracle Solaris OS

Red Hat Linux OS

Member: Association of Computing Machinery (ACM)

Delta Mu Delta Honor Society

Certified Information Systems Security Professional (CISSP)

Certified Information Systems Auditor (CISA)

Certified, NSA Information Assessment Methodology (IAM)

Qualified ISO/IEC 27001 Lead Auditor