Anton J Aylward, CISSP, CISA

Skills

Foundation

Achievement Orientation
- Develops plans & sets concrete goals. Seeks out more effective methods. Decisions & priorities and chosen goals based on benefits and cost.

Vision
- Creates & communicates strategies and architecture to meet business needs and strategies. Long term, viable objectives.

Team Leadership
- Takes care of staff, protect from internal and external interference. Obtains the resources needed to do the job. Maintains morale, respect, camaraderie and working environment.

Initiative
- Acts before being forced to by events. Works out contingencies.

Teamwork & Cooperation
- Solicits input from other stakeholders and affected parties. Concern for others and "side effects".

Relationships
- Builds rapport thought informal contacts in context of day-today work.

Service Orientation
- Communicates with internal and external clients to clarify needs. Involves others in formulating requirements and deliverables.

Analytical Thinking
- Insight into causal relationships and interconnections. Systematically addresses and analyses complex situations & problems.

Conceptual Thinking
- Identifies discrepancies and inconsistencies and ratifies "real meaning" to establish insight. Seeks out underlying patterns.

Order and Quality
- Sets up systems and processes to ensure quality though clear requirements and responsibilities.

Flexibility
- Demonstrates flexibility when applying rules or procedures according to context; adapts to meet the larger needs of the organization.

Confidence
- Takes personal responsibility and admits mistakes.

Control
- Calm in crisis situations. Works to constructively address issues rather than 'personalities' in stress situations.

Management

Managerial Finance
- Principles of Economics & Finance
- Financing and Budgeting
- Cost analysis
- Business Case requirements

Personnel Management
- Organizational & Personal Behaviour
- Job description.
- Recruiting: interviewing & appraisal
  - Background checks
  - Security clearances
  - Employment agreements
- Reviews and guidance; performance appraisals
- Mentoring and guidance
- Disciplinary procedures & termination

Business Processes
- Business Process Risk Analysis
- Tactical and strategic planning, feasibility & risk
- Decision making and control

Negotiation: Contracts, RFPs & SLAs
- Working with suppliers and vendors
- Map Functional Requirements & Needs Analysis to RFP/SLA
- Performance & Conformance measurements

Entrepreneurism
- Analyse trade-offs, present alternatives
- Propose new working initiatives & projects
- Working with banks and venture capitalists

Communications
- Excellent command of English, good written and verbal communication skills, proficient in presentations.
- Graduate of Dale Carnegie course on Public Speaking and Leadership course.
- Experienced and confident presenter. Formal and informal presentations at conferences, workshops and in-house "lunch-and-learn".

- Has given presentations at conferences and trade shows. His presentation on TCP/IP security was voted on of the top 25 at Vanguard Security Expo, 1998.
- Interacts professionally with clients, business partners' technical staff, and senior management.
- Writes customer proposals. Writes and presents security and network solutions, feature-benefit project and budget proposals.
- Documents all aspects of his work.

Audit & Compliance

Passed CISA exam June 2002 - #113160

- Planning and execution of Information Technology audits, evaluating the risks associated with new technologies, new projects and business initiatives (TRA)
- Use of **COBIT** as principle audit model
- Use of Capability Maturity Model (**CMM**) to evaluate software reliability
- Sarbanes Oxley (**SOX**/**COSO**)
- **ITIL** & 'help desk'
- **FFIEC**, **Basel**-2 and banking regulation
- GASSP, ISO7799, **ISO27001**
- **PIPEDA**/Bill-198
- **IETF** and **NIST** Publications
- Systems Auditing: reviewing of network architecture, host configuration, firewall and router configuration., Hosts, LAN, WAN and services. Use of various scanning tools.
- Handling of response to security incidents
- Appraisal of management controls, policies and procedures
- Auditing of physical as well as electronic measures
- Auditing of security and integrity of installed systems and networks as well as new designs and plans.
- Presentations to management,
  - Prioritisation of issues,
  - Suggested solutions.

Governance & Business Value

- Analysis of organizationals structures, roles and responsibilities
- Application of ISO 38500, COBIT, BASEL etc
- Stakeholder involvement
- Identifying business value and bottlenecks
- Change management processes

Development of Security Policies and Procedures

Expert knowledge and experience with various security protocols, firewalls, penetrations testing tools, authentication systems, remote access, VPNs, PKI, digital certificates, network operating systems and vulnerabilities and network management.

Developed Policies for commercial, governmental and education settings.

Have run workshops on policy development and policy enforcement/awareness.

- General and Specific formats
- Contingency Planning
- Security Awareness Training and Orientation

Project Management

- Excellent analytic and problem solving skills.
- Experienced team player with a strong sense of organisation & self discipline.
- Understanding of long term consequences of strategic and tactical decisions involved in configuration of hardware, software and networks.
- Can effectively and efficiently manage large, complex, technical engagements or segments of engagements. Provides senior level technical leadership on proposal writing, solution design, and implementation across multiple sites and locations.
- Able to lead team members, third parties, and technical counterparts in client organizations during the integration of technical methodologies.
- Translate management and corporate policies into workable, understandable designs.
- Determine how the project can best improve the company's profitability by both reducing costs and realising the best potential of the various available assets.
- Recommend strategies for the most cost-effective investment of resources to implement management's policies.
- Determine how the project can best bring about improvements to the company's profitability by both reducing costs and realising the best potential of the various available assets.
- Recommend strategies for cost-effective use of resources to implement management policies.
- Ascertain areas of concern to senior management for the best return on time and work invested.
- Ascertain the areas of concern to senior management resulting in the best possible return on time and work invested.
- Identify dependencies, critical areas and estimate the required costs and resources.
- Use of management tools and database systems for project planning and tracking.
- Use standardised solutions to standard, recurring problems so as to release time, talent and other resources for the key components of the project.
- System tuning for optimal performance of applications, monitoring & profiling of activities and identifying potential bottlenecks. Cost benefit analysis of options for upgrades.
- Experienced with a wide range of applications. Understands interactions and factors

Managerial Finance, Budgeting & Cost Accounting

- Planning and constructing business activities

- Formulating strategies
- Budgeting
- Forecasting
- Resource Allocation & Management
- Supporting financial reports preparation
- Safeguarding assets
- Financial Tools
  - Sunk cost, IRR, Discounted cash flow

Sales Support

Work closely with Account Managers assisting in identifying sales opportunities. Ensuring technical alignment with client business needs.

Technical support for sales, designing networks, firewalls and security policies for clients, assisting in budgeting and in closing sales.

Operating Systems

Strong understanding of the fundamentals and underlying principles of operating systems and their implementation.

UNIX & Linux

Over 28 years experience with many flavours of UNIX, covering kernel, applications and networking device drivers, schedulers and process control, interprocess communication, file system.

Exceptional understanding of how applications interact with the UNIX kernel, key to understanding performance, tuning & debugging strange interactions.

Various roles involved with porting UNIX to new hardware, and a wide range of platforms.

Experienced with the UNIX tools, shell scripts, awk, sed, perl.

Experienced and effective system administrator.

Expert at tuning & optimizing UNIX systems.

Used Linux, AIX, HP/UX, Solaris, DG/UX and others

Languages

Background in C and C derived languages. Has worked with most of the major "structured" languages of the Pascal/Algol family, as well as various 4GL and process control languages.

Has written many compilers and interpreters for special purpose application oriented languages.

Recent work in Perl and Ruby/Rails

Understands the principles and patterns that underlie compute language theory, and can pick up the basics of a new language in a few hours.

Database

Interaction of database services with operating system and underlying hardware, techniques for optimisation of services at all levels.

Secure installation without need for root.

Secure communications for administration and use

- ✔ Oracle
- ✔ Sybase
- ✔ Progress
- ✔ MySQL

TCP/IP

Over 20 years experience with IP-based networking. Excellent understanding of all the key protocols and their implementation, both at the system and application level. Prior experience of non-IP packet networking for military/aerospace applications.

Deep understanding of the security implications of the protocols & the various ways they can be implemented.

Installed transcontinental networks, liaison with long distance providers. Fail-soft DNS configuration, firewall isolation, managing routers, backup dial, integration with existing software packages. Integration with terminal dial-up & DHCP.

Firewalls

Integration of firewall into network architecture for most effective utilization of resources. Firewall policy and configuration design. Deployment. Integration with split-DNS, e-mail mechanisms. Configuration of proxies for enforcement of corporate policy. GUI & command-line Interfaces.

Previously active on the Internet's firewall and firewall-expert mailing lists.

PKI & VPN

- Virtual Private Networks using a variety of mechanisms
- Remote Access Policies & Implementations
- Identification & Authentication Systems
- Digital Certificates
- Encryption algorithms: efficiency and trade-off
- RSA, PGP, TokenID

E-Mail

- Configuration of E-mail for reliable and secure communication. (PGP/X509)
- Use of E-mail to drive other applications (UNIX)
- E-mail handling policies, implications of archiving and retention.
- Mechanisms for blocking SPAM and malware.
- Virtual E-mail domains. (UNIX)
- E-mail handling hardware configurations.
  - Proxy servers.
  - Dedicated mail hosts.
  - Name hiding. (UNIX)
  - Aliasing. (UNIX)

Audit

Conduct IS Audits in accordance with generally accepted IS audit standards and guidelines to ensure the organization's information technology and business systems are adequately controlled, monitored and assessed.

- Develop and/or implement a risk-based IS audit strategy and objectives, in compliance with generally accepted standards, to ensure that the organization's information technology and business processes are adequately controlled, monitored, and assessed, and are aligned with the organization's business objectives.
- Plan specific audits to ensure that the IS audit strategy and objectives are achieved.
- Obtain sufficient, reliable, relevant, and useful evidence to achieve the audit objectives.
- Analyze information gathered to identify reportable conditions and reach...

Management, Planning and Organization of IS

Evaluate the strategy, policies, standards, procedures and related practices for the management, planning, and organization of IS

- Evaluate the IS strategy and the processes for its development, deployment, and maintenance to ensure that it supports the organization's business objectives.
- Evaluate the IS policies, standards, and procedures (for example, performance management, change management, project management, security policies) and the processes for their development, deployment, and maintenance to ensure that they support the IS strategy.
- Evaluate IS management practices (for example, IS staffing practices, IS training practices, information security management) to ensure compliance with IS policies, standards, and procedures. ...
- Knowledge of the components of an IS strategy and an IS policy
- Knowledge of leading practices in regard to IS strategy, policy, standards, and procedures
- Knowledge of methods and approaches for the development, deployment, and maintenance of an IS strategy
- Knowledge of IS project management practices
- Knowledge of IS risk management practices
- Knowledge of IS change management practices
- Knowledge of IS quality management practices
- Knowledge of IS information security management practices ...

Technical Infrastructure and Operational Practices

Evaluate the effectiveness and efficiency of the organization's implementation and ongoing management of technical and operational infrastructure to ensure that they adequately support the organization's business objectives.

- Evaluate the acquisition, installation, and maintenance of hardware to ensure that it efficiently and effectively supports the organization's IS processing and business requirements and is compatible with the organization's strategies.
- Evaluate the development/acquisition, implementation, and maintenance of systems software and utilities (for example, operating system, database management systems, security packages) to ensure ongoing support of the organization's IS processing and business requirements and compatibility with the organization's strategies.
- Evaluate the acquisition, installation, and maintenance of the network...
- Knowledge of risks and controls related to hardware platforms, systems software and utilities, network infrastructure, and IS operational practices
- Knowledge of systems performance and monitoring processes, tools, and techniques (for example, network analyzers, system error messages, system utilisation reports)
- Knowledge of the process of IT infrastructure acquisition, development, implementation, and maintenance
- Knowledge of change control and configuration management principles for hardware and systems software

Protection of Information Assets

- Evaluate the logical, environmental and IT infrastructure to ensure that it satisfies the organization's business requirements for safeguarding information assets against unauthorized use, disclosure, modification, damage or loss.
- Evaluate the design, implementation and monitoring of logical access controls to ensure the integrity, confidentiality and availability of information assets (for example programs and data)
- Evaluate network infrastructure security to ensure integrity, confidentiality, availability and authorized use of the network and information transmitted.
- Evaluate the design, implementation and monitoring of environmental controls (for example fire suppression, uninteruptable power supply) to prevent and/or minimise potential losses.
- Evaluate the design, implementation and monitoring of physical access controls to ensure that the level of protection for assets and facilities is...
- Knowledge of design, implementation and monitoring of logical access controls.
- Knowledge of logical access control principles, tools and techniques.
- Knowledge of encryption techniques and standards and their applications.
- Knowledge of public key infrastructure (PKI) components (for example, certification authorities [CA], registration authorities)
- Knowledge of digital signature techniques
- Knowledge of physical security controls (for example biometrics, card swipes)
- Knowledge of network security concepts
- Knowledge of techniques for identification, authentication and restriction of users to authorized functions and data (for example dynamic passwords)

Anton J Aylward, CISSP, CISA
Information Security Auditor
Willowdale
24 June, 2009
aja.Sytem!.ca
(416) 497-0201

Security Consulting

- Advocating, communicating and augmenting the principles of IT Security Strategies and a robust Security Architecture Process
- Outlining the basic security principles and guidelines for security and technology decisions for the enterprise
- Identifying organizational determinants and drivers such as skills, processes, structures, and culture and their financial impact on the Enterprise Security Architecture
- Contributing to the design of the enterprise-wide technical architectures based on enterprise business requirements and information technology strategies and standards using the COBIT methodology
- Designing and directing the governance activities associated with ensuring compliance with the Enterprise Security Architecture and standards
- Analysing enterprise business drivers to determine security and governance requirements for the business information and technical architecture
- Assessing the overall performance of security measures, techniques, investigations, training, information and awareness programs
- Developing, implementing and communicating relevant and effective security policy objectives and procedures
- Analysing the extant IT environment to detect critical security deficiencies and recommend solutions for improvement
- Documenting all aspects of Information Security operations: Decisions, Policy, Guidelines and Operations
- Contributing to and consulting on ongoing security initiatives and strategic planning
- Reviewing and contributing to changes to existing application, network and infrastructure architectures a security models and configurations
- Collaborating with Corporate Security as part of ongoing Security Event Investigations
- Providing review & analysis of security incidents and logs
- Consulting to both infrastructure and application development projects to ensure security good practices are followed and identify when it is necessary to modify the technical architecture to accommodate project and enterprise security needs

Disaster Recovery and Business Continuity

- Evaluate the process for developing and maintaining documented, communicated and tested plans for continuity of business operations and IS processing in the event of disruption.
- Evaluate the adequacy of backup and recovery provisions to ensure he resumption of normal information processing in the event of z short term disruption and/or the need to re-run or restart a process.
- Evaluate the organization's ability to continue to provide information systems processing capabilities in the event that the primary information processing facilities are not available (for example disaster recovery).
- Evaluate the organization's ability to ensure business continuity in the event of a business disruption.
- Knowledge of business continuity planning and business impact analysis techniques.
- Knowledge of disaster recovery and business continuity techniques (for example hot site, cold site, fail-safe network design, reciprocal agreements).
- Knowledge of disaster recovery planning and business continuity processes.
- Knowledge of media backup and documentation backup procedures (for example off site storage, frequency)
- Knowledge of testing concepts and methods for disaster recovery and business continuity
- Knowledge of insurance in relation to business continuity and disaster...

Business Application System Development, Acquisition, Implementation and Maintenance

- Evaluate the methodology and processes by which the business application system development, acquisition, implementation and maintenance are undertaken to ensure that they meet the organization's business objectives.
- Evaluate the processes by which application systems are developed and implemented to ensure that they contribute to the attainment of the organization's business objectives.
- Evaluate the processes by which application systems are acquired and implemented to ensure that they contribute to the attainment of the organization's business objectives.
- Evaluate the processes by which application systems are maintained to ensure the continued support of the organization's business objectives.
- Knowledge of systems development methodologies and tools (for example, prototyping, rapid application development [RAD], systems development life cycle [SDLC], estimation techniques, object-oriented design techniques).
- Knowledge of documentation and charting methods (for example, flowcharting, entity-relationship [ER] diagrams, modelling, UML).
- Knowledge of application change control and implementation best practices.
- Knowledge of software quality assurance methods (for example, testing methodologies, tools, standards)
- Knowledge of risks and controls associated with various design and development practices (for example, three-tier client/server applications, object...

Business Process Evaluation and Risk Management

- Risk models and modelling
- Operational risk analysis in business processes
- Control Recommendations
- IT Asset and Portfolio Management

- Evaluate business systems and processes to ensure that risks are managed in accordance with the organization's business objectives
- Evaluate the efficiency and effectiveness of information systems in supporting business processes through techniques such as benchmarking, best practice analysis and business process re-engineering (BPR) to ensure optimisation of business results.
- Evaluate the design and implementation of programmed (for example automated) and manual controls to ensure that identified risks to business processes are at an acceptable level.
- Evaluate the business process change projects (for example, project culture, organization's, management, financing) to ensure that they are properly organised, staffed, managed and controlled....
- Knowledge of best practice business processes.
- Knowledge of e-Business application in business process.
- Knowledge of business process controls (for example, management controls, automated controls, manual controls).
- Knowledge of business process performance indicators (for example, indicators to ensure the business objectives are being met).
- Knowledge of business project organization, management and control practices.
- Knowledge of project progress monitoring and reporting mechanisms.
- Knowledge of methods of business process design, re-engineering and improvement...
- General knowledge of the following standards, practices and frameworks:
  - Sarbanes-Oxley/Bill C-198
  - ISO-27001
  - PCI:DSS
  - NIST SP800-53

Information Security

Passed CISSP exam June 1997 - #4350
one of the first CISSPs in Toronto
ISSA - April 1995 - #3715

Operations Security

- Identification of critical information, processes, people, communication channels and other assets
- Identification of the relevant adversaries, competitors or criminals with both intent and capability to acquire , damage or otherwise harm any of the above.
- From the adversary's, perspective, identify potential vulnerabilities and means to access or harm any of the above.
- Assess the risk of each vulnerability by its respective impact to mission accomplishment / performance.
- Generate / recommend specific measures that counter identified vulnerabilities. Prioritize and enact relevant protection measures.
- Evaluate measure effectiveness, adjust accordingly.

Risk Management

- Principles of Risk Management
- Threats and vulnerabilities
- Risk Assessment
- Qualitative vs. quantitative
- Annual loss expectancy calculations
- Countermeasure selection
- Risk reduction/assignment/acceptance
- Project level Risk Assessment & Management

Access Control Principles & Methods

- Host & Network based
- Role based
- Access management issues

Security Management Principles & Practices

- Change Control/Management
  - Hardware configuration
  - System and application software
  - Change control process
- Data classification
  - Objectives of a classification scheme
  - Criteria by which data is classified
  - Commercial data classification
  - Government data classification
- Employment policies & practices
  - Background checks
  - Security clearances
  - Employment agreements
  - Hiring and termination practices
  - Job descriptions
  - Job rotations
  - Separation of duties & responsibilities
- Roles and responsibilities
  - Individuals
  - Data Owners & Custodians
  - Separation of Duties
- Security awareness training
- Security management planning

Applications & Systems Development

- Systems development controls
  - System development life cycle
  - Requirements determination
  - Protection specifications development
  - Design review
  - System test review
  - Certification and accreditation
  - Service level agreement
- Application Security & Controls
  - Distributed environment
    - Agents

    - Applets
    - Active-X
    - Java
- Local Attacks
    - Viruses, Trojan Horses Worms & other malware
    - Logic Bombs

Physical Security

- Facility requirements
    - Restricted areas/work areas
    - Escort requirements/visitor control
    - Fences, gates, turnstiles, mantraps
    - Security Guards/Dogs
    - Badging
    - Keys and combination locks
    - Lighting
    - Site selection, facility design, and configuration
    - Motion detectors, sensors, and alarms
    - CCTV
- Technical controls
    - Smart cards
    - Audit trails/access logs
    - Intrusion detection
    - Biometric access controls
- Environment/Life Safety
    - Power and HVAC considerations
    - Water leakage and flooding
    - Fire detection and suppression
    - Natural disasters

Hardware

Understands hardware from semiconductors up to transcontinental networks, having designed and deployed both. At home with wires and meters as much as with software.

Familiar with semiconductor fabrication principles and techniques. Has worked with germanium, silicon and silicon-on-sapphire.

Circuit fabrication techniques from wire-wrap to multi-layer surface-mount to military and avionics standards.

Obsolete Skills

- VLSI Chip Design
- Linear Circuit Design
- Drafting
- Technical Writing
- Cable Pulling & Wiring installation
- Circuit Board design: layout & fabrication
- Digital Logic circuit design, prototype, test.
- Cabinetry design & fabrication: wood & steel.
- HVAC & 3-phase installation
- “Raised Floor” machine room design
- Software Architecture and Programming:
    - 4GLs & Database languages
    - C/C++
    - UNIX Kernel & Drivers
    - Compilers and Interpreters
    - Forth, Smalltalk
    - Debugging
- Mainframe Interfacing
- Load Balancing
- Technical Sales Support
- Switched mode PSU design
- Accounting and ERP applications

TO BE DONE

Software and Hardware Development

Web development & security

Telecommunications & Network Security

Forensics

Systems Architecture

Anton J Aylward, CISSP, CISA
Information Security Auditor

Willowdale
24 June, 2009

aja.Sytem!.ca
(416) 497-0201