

Gil Smith CISA CGEIT

Qualifications and Associations

Bachelor of Science, Computing/Geography (Canberra)
Certified in the Governance of Enterprise IT (CGEIT)
Certified Information Systems Auditor (CISA)
Accredited Lead Auditor, ISO 20000 IT Service Management
Member British Computer Society ITSM Accreditation & Audit Panel
Member of the Information Systems Audit and Control Association
Member ACARA Audit and Risk Committee

Principal Consultant

Gil works in the provision of IT risk management and assurance related services for Hawk Information Technology Services. He has over thirty one year's IT audit and IT risk management experience, providing services and advice in support of external auditors, internal auditors and as an independent consultant to executive management, IT management and business unit managers. His maturity and experience in the industry allows him to consult to management at all levels on the effectiveness of their IT governance, to conduct in-depth technical and security reviews, to conduct detailed reviews of a wide range of business application systems and to assist management in improving their IT related processes in a practical and acceptable way. During this period, he has provided a range of IT audit and IT risk management services to numerous clients in a variety of industry groups in both the public and private sectors (NSW, nationally and internationally).

Principal Area of Practice

The principal areas of practice are numerous given his time in the industry and the following attempts to list those more recent subject areas first.

- IT Audit support for internal and external audit clients
- Assessment of IT applications controls (various including SAP); pre-implementation and post implementation; accuracy/completeness of entry and processing, access security, segregation of duties, recoverability, audit/management trail, data/processing integrity for specific applications
- Assessment of controls operating in the IT environment (various operating systems, network managers and RDBMS); access security, IT operations, systems backup/ recoverability, IT strategic planning, data and software integrity, data and software change control, business continuity
- IT project governance; involvement in projects for the purposes of assessing project governance, improving project governance and ensuring compliance with methodology
- Assessment of third party vendors; performance against contract and service level agreements; compliance with standards
- Evaluation of IT governance effectiveness and identifying areas for improvement
- Audits and pre-certification reviews for a range of standards applicable to today's ICT environments (eg ITIL, COBIT, PCI, ISO/IEC 31000, ISO/IEC 20000, ISO/IEC 27001)
- Data analyses/ design of data analytics in support of audit and also management requirements
- Assisting in the improvement of controls in IT environments, application systems and information systems
- Benefits realisation reviews; determining the extent to which planned benefits are obtained (eg as a result of system implementations, outsourcing contracts)
- Rationalisation/improvement of business processes, systems and information management; establishment of information management frameworks; detailed workflow and data flow analysis
- Assisting management construct effective and realistic IT strategic plans
- Independent assessment of commercial contracts from a technical perspective focusing on improving the definition of services, service levels, performance metrics, performance measurement, controls, quality assurance, governance and risk management; assessment of performance against contract
- Independent review of business requirements/solutions specifications (completeness, detail)

- Development/implementation of effective/practical information management policies and procedures assessment of risk associated with an organisation's IT infrastructure, resources, systems and data and assisting management with the implementation of appropriate risk mitigation measures.
- Assisting in the establishment and operation of IT Risk Management services
- Quality Assurance for major IT projects impacting the business
- Assistance to management and project managers regarding systems development and implementation methodologies, project management techniques, project management controls and project governance
- Assisting in the establishment and implementation of organisation-wide specific IT control frameworks such as COBIT (the international Information Systems Association of Certified Auditors product), ITIL
- Assessment of IT controls (business applications and general) for the purposes of determining compliance with Sarbannes Oxley requirements; identification, documentation, assessment; development of associated test strategies and assistance with testing and remedial action
- Assistance with restructuring IT activities to comply with national and international standards, e.g. ISO/IEC 20000, ISO9000, ISO/IEC 27001, ISO/IEC 31000, the international Information Systems Association of Certified Auditors product COBIT, ITIL, PCI and a number of other relevant Standards.

Gil has provided IT audit, IT governance, IT risk management services and IT project governance management to numerous public and private sector clients, including (limited to a selection of clients since April 1997):

- City of Sydney - IT internal audit ongoing, 2012 – current; (IT governance review, City wide IT risk assessment, data analytics, in-depth review of expenditure life cycle, specific business applications reviews, IT general controls reviews, data security, data analytics, IT procurement, software license management, online business gateway, Pathway applications controls, PCI security and controls)
- Australian Ethical Investments 2014-2015; development of APRA compliant Business Continuity Plans and related policy and Data Security Policy
- Westfund - ongoing IT internal audit role, 2011 - current; (performing an assurance role with respect to the integrity of the data conversion and load and performance of a post implementation review of the system implementation and data conversion and load; review of the applications controls in Paragon21 modules, Membership, Claims, Agency, Financial Systems, data analytics)
- Great Lakes Council (IT general controls review 2015)
- Bega Valley Shire Council (IT general controls review 2014)
- CUBIC Transportation Systems (2014 IT physical security at data centres, planning for Sarbannes Oxley audit coverage 2015)
- Wollongong City Council - ongoing IT internal audit assignments 2014 – current; (IT general controls/risk assessment and mitigation planning, data security, IT governance consulting/guidance)
- Building Employees Redundancy Trust (BERT) (ongoing IT audit in support of external audit; 2012 - current)
- Collection House (ongoing IT audit in support of external audit; review and process improvement in AGILE development/implementation environment, IT general controls; 2012 – current)
- Orange Business Systems (conduct of SAS 70 assignments annually; ongoing)
- NSW Trade & Investment (consulting assistance to IT for transitioning of systems as a result of amalgamation of State government entities)
- Transport for NSW – provision of assurance services with respect to the accuracy and completeness of accounts payable data migrated as part of the transition of accounts payable services from five entities.
- Australia Competition and Consumer Commission (audit of IT related aspects, including data security and data integrity, of organisations that have provided undertakings to the ACCC under the Trade Practices Act in order to alleviate competition concerns); (2008 – 2013)
- TransGrid (IT internal audit of: DRP including SCADA, Oracle RDBMS Security, performance of third party against contract/SLAs, in-depth technical reviews of VMWare, SVC, Windows AD, Ellipse; 2009-2012)
- AEMO (IT market audit) – IT auditor for the Electricity Market Audit, assessing compliance with the National Electricity Rules. In-depth assessment of controls operating in the electricity market IT environment and primary business systems and databases (2010-2014)

- NSW Trade & Investment (formerly NSW Industry & Investment, Department of Primary Industry and including Forests NSW and Fisheries NSW) - IT internal audit 2009 – 2013 (a wide variety of technologies and business systems are subject to review to determine the effectiveness of controls); subsequent 2014 independent consulting assignment to coordinate the development of a business plan to transition major business systems between organisations.
- Screen Australia (IT internal audit 2009 – 2014)
- Prime Infrastructure, incorporating WestNet Energy (formally Babcock and Brown Infrastructure); IT data security and data ring fencing 2008 - 2010
- Babcock and Brown Power (IT data security and data ring fencing 2008 - 2010)
- DEEWR (detailed review of the effectiveness of the Department's Disaster Recovery Plans, the governance structure and the processes related to their development, maintenance and testing)
- Papua New Guinea Banking Corporation (IT internal audit; IT risk management consulting; business continuity planning; over 6 years)
- Reckitt & Colman Pty Limited (assistance with implementation of CoBiT framework and related processes in the IT environment)
- FreightCorp (IT internal audit – 3 years)
- Australian Nuclear Science Technology and Research Organisation (ANSTO) (IT internal audit and IT risk consulting – 3 years)
- ANZ Bank, Shared Services Division; managing the IT component of the implementation of Information Security, ISO27001; full time 4 months.
- Macquarie University (IT internal audit and IT risk management – 6 years)
- Macquarie Graduate School of Management (IT risk consulting assignment)
- Macquarie International (IT risk consulting; a number of assignments)
- Waterways Authority (for Ferriers Chartered Accountants) (IT risk consulting assignment)
- PNG Harbours Board (IT risk consulting assignment)
- Hobsons Australia (and participating Universities) (IT risk consulting; a number of assignments)
- CiBiS (IT risk consulting; improvement of contracts with third party providers, SLAs and SOWs)
- NCELTR (National Centre for English Language Training; Macquarie University) (Investigation)
- International Education Network (IEN) (Risk assessment and workshop facilitation)
- Equities trader (Assessment of compliance with ASX standards)
- Panthers Entertainment Group (IT internal audit – 1 year)
- Commonwealth Bank of Australia (Sarbanes Oxley; establishment of test strategy for general controls)
- Division of Economics and Financial Studies (Macquarie University)
- PricewaterhouseCoopers (mentoring and coaching in the IT Assurance area, 9 months)
- CHUBB Australia (Sarbanes Oxley; testing of IT controls; 2 years)
- NSW Auditor-General's Office (IT audit support of annual financial audits for a variety of government Departments and entities)
- NSW Auditor-General's Office (assistance with framework implementation and compliance with AS/NZ7799)
- Department of Corrective Services (Independent audits of information security and preparedness for ISO27001 accreditation audits).

Employment History

RSM Bird Cameron

2008 – 2013 (Nov) Head of Risk Advisory Services (IT) – Sydney.

Gil Smith-Information Systems Risk Management P/L

1997 – 2008 Director, providing IT internal audit and IT risk management services (Sydney registered company providing services nationally and internationally).

Price Waterhouse

1987 – 1988 Computer Information Systems Audit, Manager (Hong Kong)

1988 – 1994 Computer Information Systems Audit, Manager (Sydney)
1994 – 1995 Computer Information Systems Audit, Senior Manager (Sydney)
1995 – 1997 (April) Director, Information Systems Risk Management (Sydney).

Australian National Audit Office (ANAO)

1983 – 1986 Computer Auditor, Computer Audit Manager.

Department of Defence

1975 – 1983 Programmer, Database Administration, Analyst, Applications Systems Project Leader
(application systems development).