Vulnerability Assessment Group

Capability Statement

ABN: 93 784 971 092
54 Kathleen Street Trigg
Western Australia 6029
Telephone +61 8 9203 7214
Facsimile +61 8 9448 1755
Web: www.vulnerabilitygroup.com

DATE: 27 March 2013
DOC NO.: VAG Capability Statement Rev B15.docx

Contents

1 GOOD CORPORATE GOVERNANCE 3

2 VULNERABILITY ASSESSMENT GROUP (VAG) OVERVIEW 3

3 CRITICAL INFRASTRUCTURE PROTECTION 3

3.1 Overview 3

3.2 Physical and IT Network Focused Vulnerability Assessments 3

3.3 Security Based HAZIDs 3

3.4 Projects 4

3.5 Clients 4

4 RISK MANAGEMENT TOOLS 6

4.1 Safety and Risk Management / Safety Case Support 6

4.1.1 Overview 6

4.1.2 Safety Design Reviews 6

4.1.3 HAZID Workshops 6

4.2 Strategic Security Management 7

4.2.1 Security Auditing 7

4.2.2 Security Risk Assessment 7

4.2.3 Engineering Analysis and Explosion Modelling 8

4.2.4 Security Management Systems (SecMS©) Development 9

4.3 Business Continuity Planning 10

5 CRISIS AND EMERGENCY RESPONSE TRAINING 11

5.1.1 Team Simulations 11

5.1.2 Auditing and Review 11

5.1.3 Plan Development 11

6 MARITIME / OFFSHORE FACILITY SECURITY COMPLIANCE 12

6.1.1 Offshore Facility, Ship, Port Facility and Port Security Plans 12

6.1.2 AMSA Approved ISPS Course / MTSOFSA Training 12

6.1.3 External Security Plan Auditing 12

ATTACHMENTS 13

Attachment 1 CV's of Key Personnel

1 GOOD CORPORATE GOVERNANCE

Director liability, regulatory requirements, technology convergence and security concerns have caused many companies to question their existing risk management position.

VAG provides a unique framework and the supporting skill sets to manage risk, demonstrate good governance and develop a business case for risk mitigation by quantifying both statistical and asymmetric threats.

2 VULNERABILITY ASSESSMENT GROUP (VAG) OVERVIEW

VAG is an independent risk management consultancy. We employ a unique cross disciplinary team of qualified individuals with specialized skills and experience in Strategic Security Management, Information Technology Management and Safety and Risk. Our personnel have diverse backgrounds with experience at the highest levels of business, government, security and academia.

3 CRITICAL INFRASTRUCTURE PROTECTION

3.1 Overview

With strong engineering exposure VAG routinely assists companies to develop security focused risk assessments. The key to communicating risk and developing a security business case is quantifying risk in accordance with Hazard Identification (**HAZID**) and Hazard and Operability (**HAZOP**) studies. VAG has built its security based HAZID / HAZOP process through the application of safety and risk engineering workshop principles and our framework for risk quantification.

3.2 Physical and IT Network Focused Vulnerability Assessments

Mapping vulnerabilities from both a physical and IT network perspective is essential for critical infrastructure operators due to interconnectedness; convergence; cyber attacks; activism; physical attacks and terrorism.

VAG provides a framework for examining vulnerability and mapping interconnectedness from a network perspective. Examining a series of power generating stations, a gas pipeline or components of a SCADA system requires a systematic process and consistent approach to ensure that the network architecture is accurately represented in order to quantify risk.

3.3 Security Based HAZIDs

Our process and findings are protected via a secure program that has been recognised through the Australian Department of Transport Security Division and the Australian Commercialization of Existing Technologies (Commonwealth funded) Program. Our software provides a framework to incorporate the corporate risk thresholds of our clients

allowing VAG to map out security events, determine risk and allocate resources in line with corporate policy.

3.4 Projects

VAG has conducted numerous projects for a range of Critical Infrastructure Providers to include:

- Security in Design / Security Basis of Design (BoD) Development
- Security Management System Development
- Computer Network Vulnerability Assessments for Control System / SCADA and IT Networks
- Offshore & Onshore Security Risk Assessments (for gas plants, offshore processing facilities pipelines etc.)
- ISPS Code / MTOFSA 2003 Compliance Management and Auditing
- Business Continuity Planning
- Crisis and Emergency Response Training and Procedure Development

3.5 Clients

The following table outlines our exposure with Critical Infrastructure Operators. Referrals can be obtained on request.

	Safety and Risk HAZID / HAZOP	IT / SCADA Computer Network Vulnerability Assessment	Business Continuity / Criticality Analysis	Security in Design (Basis of Design (BOD) input)	Intentional Explosion Analysis Modeling	Security Management System Development	Pipeline Security Risk Assessment	Port / Port Facility Security Risk Assessment	Onshore Facility Security Risk Assessment	Offshore Facility Security Risk Assessment	Onshore Facility Security Plans	Offshore Facility Security Plans	Ship Security Plans	Auditing / Compliance (ISPS Code / MTOFSA)	Emergency Response Plans / Procedures	AMSA Approved ISPS Model Course Training	Crisis / Emergency Management Training	
Agility							X								X		X	**Roma to Brisbane Pipeline**
Australian FPSO										X		X	X	X	X	X		**Four Vanguard**
BHPBilliton (Petroleum)			X						X		X		X	X		X		**Australian Business Unit (BCP), Tubridgie Gas Plant / Griffen Export Facility / Griffen Venture, Stybarrow Venture / MV Carp / Pyrenees**
ConocoPhillips			X	X		X		X	X	X	X	X	X	X	X	X		**Bayu Undan (CPP, WP1, FSO), Darwin LNG Facility, Australian Production Unit (BCP)**
City West Water		X																**Western Melbourne Suburbs and Altona Treatment Plant**
Department of Transport		X																**IT network that surrounds billing and payment infrastructure**
Dampier to Bunbury Pipeline		X					X											**WestNet / DBNGP**
ENI	X			X		X	X	X	X	X	X	X		X		X		**Blacktip SPM, WHP, Yelcherr Beach Port, Kitan Glas Dowr**
ExxonMobil								X		X		X						**Barry Beach Marine Terminal / Wandoo**
Fremantle Port Authority			X															**FPA Criticality Analysis**
Frontier Drilling													X	X				**Frontier Duchess, Frontier Discovery**
Inpex	X			X		X			X									**Ichthys**
Kleenheat Gas															X		X	**Corporate / National Training, Kwinanna Facility**
Maersk												X				X		**Maersk Ngujima-Yin**
Modec													X	X		X		**MV-11, MV-16, MV-1**
Offshore Marine																X		**AMSA Approved SSO Course**
Port Hedland Port Authority								X										**Port Hedland Port**
Santos									X	X	X	X		X		X	X	**Moomba Facility / Modec Venture 11**
Shell														X				**NW Sanderling, Snipe, Stormpetrel, Sandpiper**
Summit Fertilizers					X													
TK Shipping												X	X	X				**Karratha Spirit / Dampier Spirit**
Total Marine																X		**AMSA Approved SSO Course**
Unocal								X		X								**Erawan (CPP, Airfield, FSO) Songkhla Air Field / Supply Base**
Vermilion										X		X		X				**Wandoo A/B**
Wesfarmers Energy																	X	
Western Power		X																**Power Generation, Power Distribution & Communications Networks**
Woodside Energy		X		X		X	X	X	X	X	X	X	X	X	X	X		**PCAD, Karratha OGP, Pluto, GWA, NRA, Cossack Pioneer, Northern Endeavour, Otway OGP, Thylacine A, Ocean Legend, Angel, Vincent, Nganhurra, Ngujima-Yin, Okha, Trunkline, King Bay Supply Base, Dili**
Yarra Valley Water Co.		X																**Yarra Valley Water SCADA Network**

4 RISK MANAGEMENT TOOLS

4.1 Safety and Risk Management / Safety Case Support

4.1.1 Overview

VAG has a highly-experienced HAZID Facilitator who regularly delivers workshop-based risk identification and assessment exercises. He has authored Pipeline Safety Management Plans, Construction Stage Safety Cases, Operations Stage Safety Case, Interface Management Plans and various technical safety studies.

4.1.2 Safety Design Reviews

VAG can deliver safety design reviews of major offshore oil and gas developments. A typical scope will involve the participation of VAG personnel in the client's independent Project HSE Review team - where a small group of highly experienced offshore professionals with complementary skills and knowledge will perform a structured and in-depth audit of a project. Design review work also involves VAG personnel providing independent expert review of specific problems in safety design - typically in an independent arbitrator role on disputes between contractual parties.

4.1.3 HAZID Workshops

Our Facilitator can develop and deliver a Project-wide HAZID program including the preparation and delivery of any HAZID training required for Project personnel or contractors. Given that the large majority of risk-based decisions on a Project will be made during HAZIDs it is crucial to have a consistent and rigorous approach to this process.

The success of a HAZID depends on many factors and it requires conscientious and detailed preparation to:

- define the scope (a key failing of many HAZIDs);
- agree on appropriate team attendance, including operations representatives;
- select the appropriate perspectives from the classic PHASE-ACTIVITY-AREA-SCENARIO-SYSTEM categories with which to decompose the scope into nodes for team assessment;
- select appropriate Keywords and Guidewords from the many thousands available (rather than just use the same generic list from the last HAZID);
- screen key issues that will require particular attention;
- ensure that the workshop is a quality exercise, with full participation of attendees, and
- make a rich and informative record of the HAZID.

These are key differentiators of VAG's HAZID philosophy.

4.2 Strategic Security Management

4.2.1 Security Auditing

VAG routinely assists companies assess their critical infrastructure. As independent 3rd party auditors, VAG provides a holistic review of the effectiveness of security systems by working closely with clients to understand their operations. Site surveys and operational reviews provide clients with current security best practice input and factor into the development of the threats examined during the risk assessment.

4.2.2 Security Risk Assessment

Security risk assessment workshops are applicable to individual facilities / business units (BUs) or critical components of IT / control systems and provide a means of systematically identifying potential vulnerabilities and existing or unknown security threats.

The security risk assessment is a qualitative process that uses pre-agreed risk ranking criteria. Workshops are run in conjunction with relevant operational and management personnel and quantify security risk allowing the company to incorporate security into the overall risk management framework.

Security risk assessment reports capture findings, recommendations and responsibilities and provide an auditable trail that demonstrates to the board, audit teams and regulators that the company actively fulfils its duty of care by identifying and managing security risk.

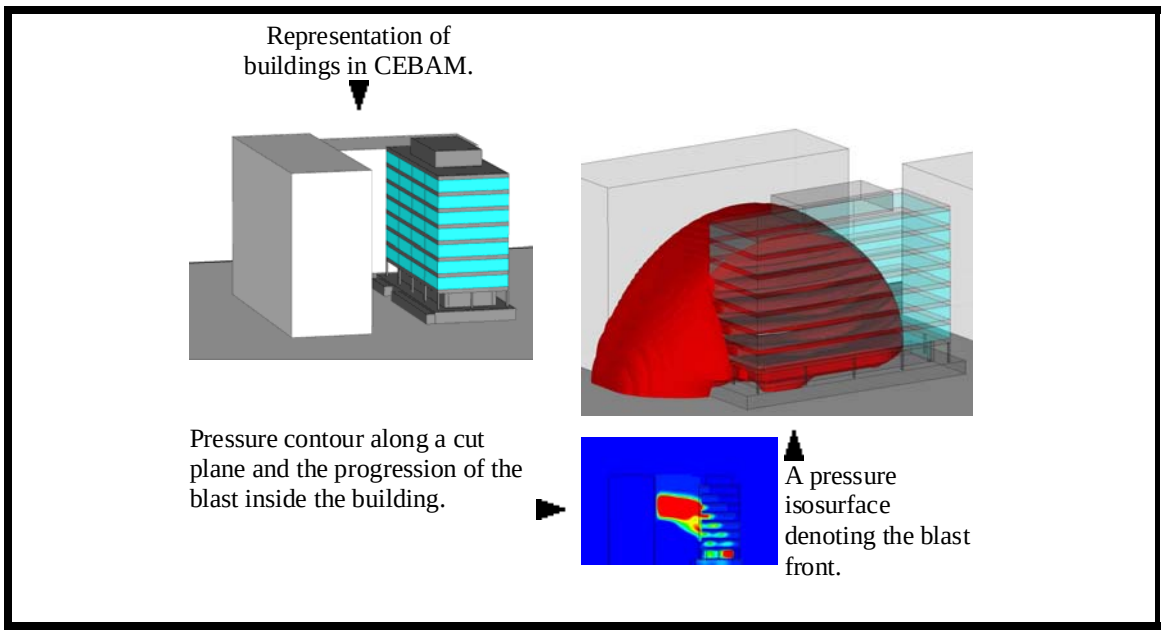
4.2.3 Engineering Analysis and Explosion Modelling

Whether examining vulnerabilities identified during security risk assessments or modelling accidental explosion events of existing hazards, VAG can determine the result through analytical and computational engineering models.

Recent models have been developed for:

- Anti-Terrorism Threat Analysis;
- Industrial Explosion Hazard Assessment;
- Explosives Safety and Protective Design; and
- Weapon Systems Evaluation.

Using a tailored graphical interface we can construct a virtual representation of any facility and calculate the resulting blast loads. During model construction, we can define failure criteria for structural components and the graphical output will show whether failure has occurred.



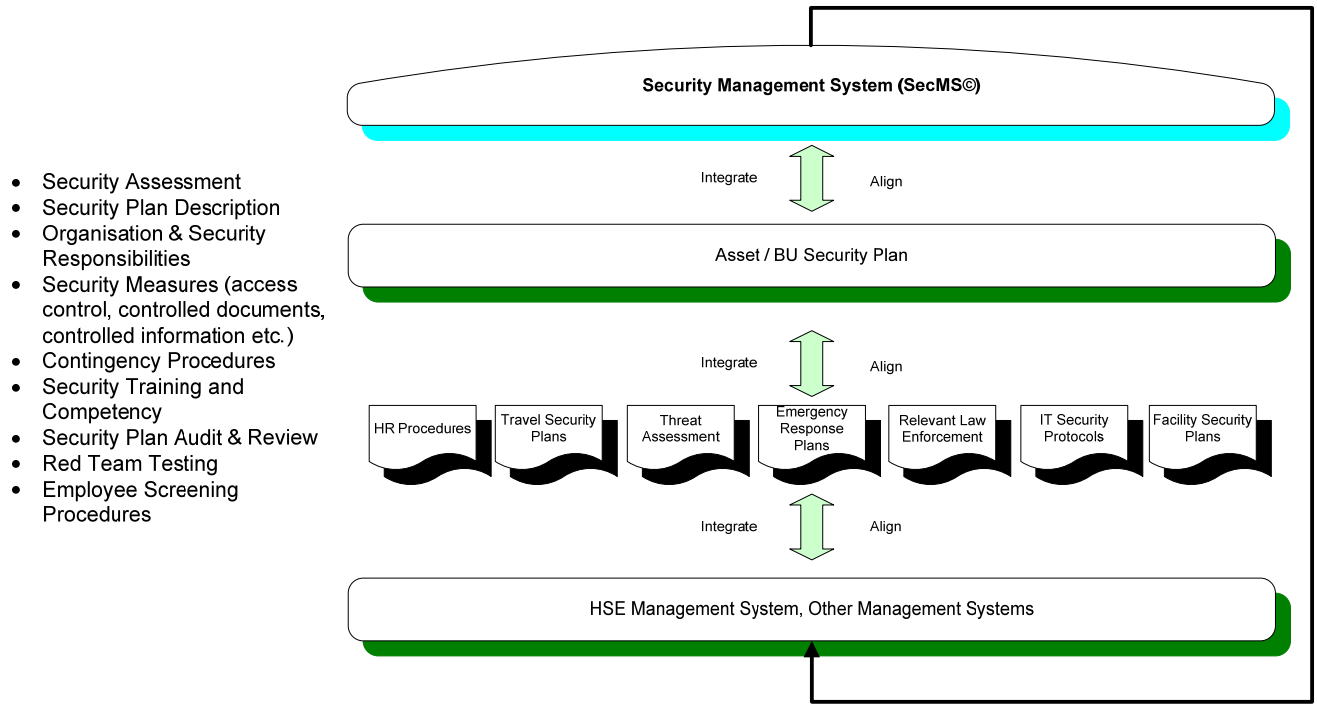
VAG can model blast events in complex 3-D environments (large urban areas) to provide information to first responders regarding evacuation, marshalling and command and control placement.

4.2.4 Security Management Systems (SecMS©) Development

Security Management Systems (SecMS©) are a whole of organisation approach to security formalisation. Designed in accordance with international risk management standards, a SecMS© systematically formalises security in an organisation while taking into account existing processes and policies (from the IT, HSE and other management systems). With broad experience across the oil and gas, mining and transportation industries, VAG is well positioned to assist companies:

- Identify what is critical to the organisation;
- Identify business continuity dependencies;
- Treat security gaps; and
- Integrate and align relevant information into a formalised system.

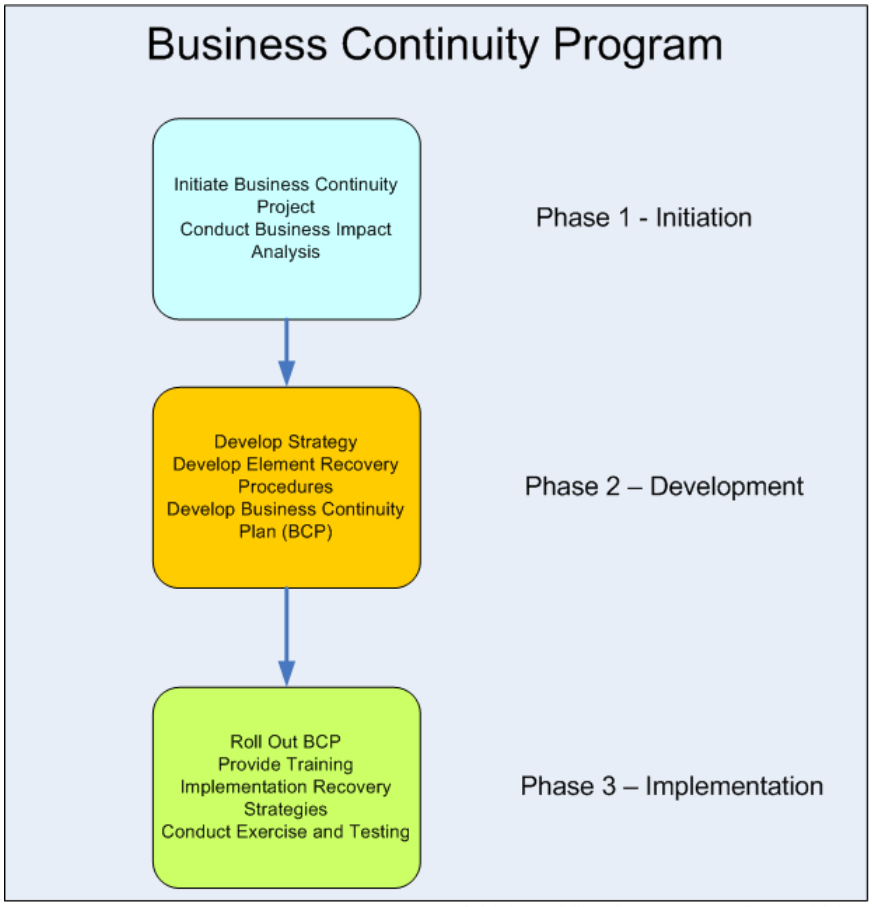
The following diagram depicts the formalisation process:



4.3 Business Continuity Planning

A developed Business Continuity Plan (BCP) fits into the broader the broader business continuity management program. VAG assists companies navigate a three phased approached which is outlined as follows:

- Phase 1 – Business Impact / Criticality Analysis – define business critical elements and the duration of time before which business critical elements inflict unacceptable consequences on the business;
- Phase 2 – Develop Critical Element Recovery Procedures and align with a Business Continuity Plan; and
- Phase 3 – Roll out the business continuity plan, provide training and then exercise the organisations ability to enact the plan.

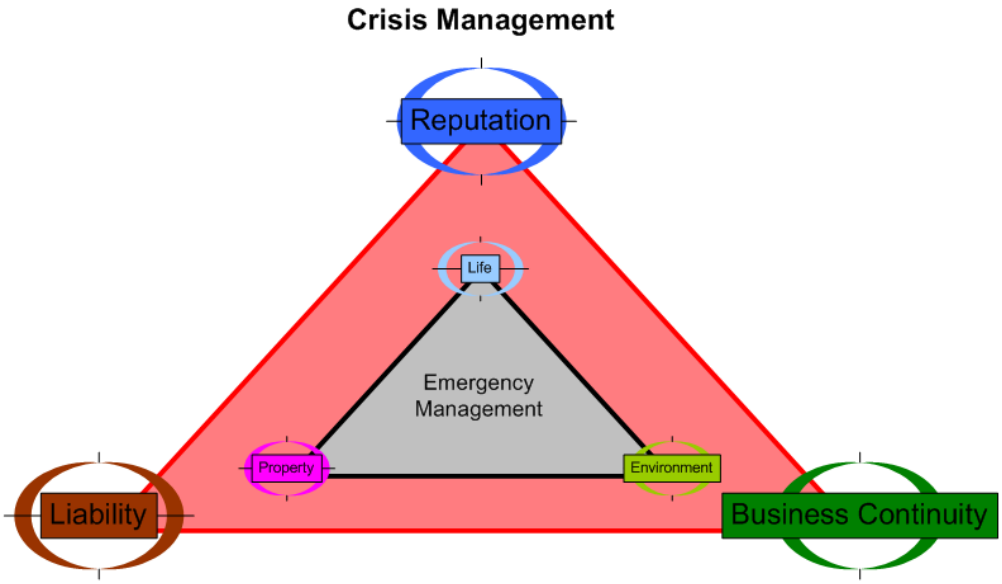


5 CRISIS AND EMERGENCY RESPONSE TRAINING

5.1.1 Team Simulations

In order for an organisation to effectively deal with unforseen events it must be trained in its roles and responsibilities. Proactive training engenders self assurance and team work amongst the staff imparting a positive 'can do attitude' which develops confidence in the plan and in the organisation's ability to deal with difficult situations.

VAG provides a training package that focuses on team members and generating a greater understanding of their roles and responsibilities as outlined in their plan, as well as providing an environment (through exercise simulations) where the team can practice the management of multiple stakeholders which may include: Media; Staff; Regulators; Next of Kin; Clients; Partners; and Industry Bodies.



5.1.2 Auditing and Review

VAG regularly reviews procedural documentation and acts as an independent auditor during client run crisis management and emergency drills. Our personnel provide industry experience and can benchmark plans and competencies against international standards.

5.1.3 Plan Development

VAG has extensive experience in benchmarking and writing both Emergency Response and Crisis Management Plans. Our plans are tailored to suit the organisation and can be incorporated with the Incident Control Systems (ICS) or other existing company standards to suit the company's individual emergency and crisis management structure.

6 MARITIME / OFFSHORE FACILITY SECURITY COMPLIANCE

6.1.1 Offshore Facility, Ship, Port Facility and Port Security Plans

VAG has developed numerous port, port facility and ship security plans in accordance with the International Maritime Organisation (IMO) International Ships and Port Security (ISPS) Code and Australia's Maritime Transport and Offshore Facilities Security Act (MTOFSA) 2003. VAG conducts the security risk assessment in accordance with the relevant contracting government / flag state requirements. The security plans are developed through a three part process which includes:

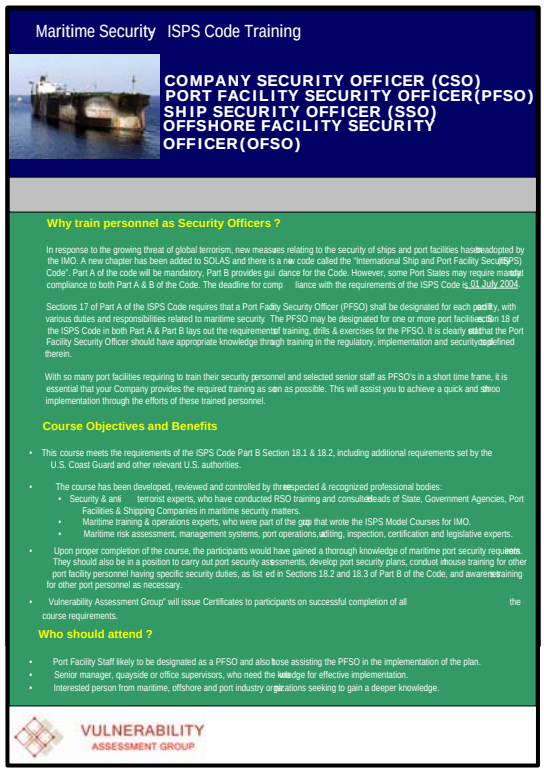
- Security Audit / Operational Review;
- Security Risk Assessment Workshop; and
- Security Plan Development.

The security plans are developed in accordance with the IMO guidance and identify roles and responsibilities as well as mitigation measures for security risks during Maritime Security (MARSEC) Levels 1 – 3.

6.1.2 AMSA Approved ISPS Course / MTSOFSA Training

VAG offers an accredited Australian Maritime Safety Authority (AMSA) Security Course which complies with IMO ISPS requirements for:

- Company Security Officer;
- Offshore Facility Security Officer;
- Port Facility Security Officer; and
- Ship's Security Officer.



6.1.3 External Security Plan Auditing

VAG provides external auditing to satisfy MTOFSA External Auditing Requirements which state:

"An external audit must be undertaken by someone outside the organisation, who is also independent of those responsible for implementing security measures. The audit may be conducted by an external consultant who developed the security plan, as long as they are not also responsible for the plan's implementation. An audit which is undertaken by the Office of Transport Security (OTS) does not constitute an external audit.

ATTACHMENTS

Attachment 1
CV’s of Key Personnel

Chandler Comerford GAICD

Director

KEY SKILLS AND EXPERIENCE

As a director of the Vulnerability Assessment Group, Chandler is responsible for development of the group's methodologies to include: Network Infrastructure Mapping, Threat Vector Diagram Development, SCADA / Control Systems and IT Vulnerability Assessments, and Physical Security Auditing.

Chandler manages the workshop facilitation process and project delivery for all VAG work conducted in the 'Critical Infrastructure' space. Chandler is regularly asked to speak at security functions and has presented at the National SCADA community of interest forums, Engineers Australia; the Australian Homeland Security Research Centre as well as the Trusted Information Sharing Network (TISN) 'Group of Eight' Critical Infrastructure Protection Forum.

As a former US Special Forces Officer (US Navy SEAL) Chandler has extensive experience with unconventional warfare and terrorism. As a member of the Special Operations Command Pacific Joint Combined Exercise Training Team (JCET), Chandler worked as a Military Advisor training foreign Special Forces groups throughout South East Asia.

A former safety and risk engineer with robust exposure across a range of private and government organisations Chandler has also built and facilitated a vulnerability assessment process which allows critical infrastructure owners and operators to identify and quantify unknown risks in order to develop secure operations, satisfy corporate governance requirements and implement strategic policy.

With extensive experience consulting in a range of environments Chandler has conducted numerous SCADA / Control Systems / IT and Physical vulnerability assessment workshops for the Water, Power, Gas Pipeline, Offshore Oil and Gas, Rail and Maritime industries.

His areas of expertise:

- SCADA / Control Systems / IT / Physical Vulnerability Assessments
- Workshop facilitation / staff training
- Project Management
- Security Basis of Design (BOD) and Functional Specification development
- Security systems auditing
- Business continuity / crisis planning
- Security Management Systems Development
- Safety and risk assessment studies
- HAZID and HAZOP studies
- QRA modeling

VULNERABILITY
ASSESSMENT GROUP

TITLE
- Director
- Research Fellow – Australian Homeland Security Research Centre

QUALIFICATIONS
- GAICD
- B.S. Oceanography "With Merit", United States Naval Academy
- Licensed Security Agent
- Licensed Security Consultant
- Cert IV - Training and Assessment
- Cert IV – Security and Risk Management

INTERNATIONAL EXPERIENCE
- Australia
- USA
- Thailand
- Sri Lanka
- Philippines
- Palau
- Guam
- Jordan

ADDITIONAL SKILLS
- Anti Terrorism / Force Protection Officer (US Navy)
- Advanced Applied Explosives Course
- Basic Underwater Demolitions School (BUD/s)
- US Navy Range Safety Officer (Dynamic, Explosive, Static)
- Combat Diver
- US Navy Diving Supervisor
- Survival Resistance Escape Training
- Military Free Fall Parachutist
- Long Range Maritime Operations
- Urban Reconnaissance and Surveillance
- HUET training
- Internationally Accredited PADI Divemaster

MEMBERSHIPS
- Australian Institute of Company Directors (AICD)
- United States Naval Academy Alumni Association
- UDT/SEAL Association

Gerard Burke CEng, MICE

Risk & Safety Consultant

VULNERABILITY
ASSESSMENT GROUP

TITLE
- Consultant

QUALIFICATIONS
- Chartered Engineer (1988)
- MSc Fire Safety Engineering (1983)
- BSc (Hons) Civil Engineering (1981)

INTERNATIONAL EXPERIENCE
- Argentina
- Australia
- China
- Denmark
- France
- Germany
- Indonesia
- Netherlands
- Norway
- Monaco
- Philippines
- Singapore
- UK
- USA

ADDITIONAL SKILLS
- Experienced Facilitator
- Offshore survival training (UK, Norway, Australia)
- HUET (UK, Australia)
- Freefall Lifeboat Training (Norway)
- Ship fire fighting & BA training (UK)
- Fire legislation & building control (UK)
- Classified Radiation Worker (UK)
- Nuclear Reactor Operator Training (UK)
- Radiological Protection (UK)
- ISRS Auditing
- Loss Causation / Accident Investigation
- QRA, FTA, ETA, FMECA, etc

MEMBERSHIPS
- Corporate Member, Institution of Civil Engineers, UK (1988)

KEY SKILLS AND EXPERIENCE

Gerry Burke is a recognised safety and risk management authority in offshore oil and gas, now entering his fourth decade of experience in the major hazard industries around the globe. He has built and led world-class safety teams in Australia and the UK, providing leadership, driving safety innovation, finding safety solutions and giving training in safety and risk. He has probably managed, delivered or worked on more Safety Cases for a wider range of facilities in more industries than anyone else in the Southern Hemisphere.

Gerry is a chartered civil engineer whose early experience was in coal mining and construction but since 1982 has worked exclusively in safety and risk. His formal training was gained with the UK Atomic Energy Authority in a diverse regulatory and advisory role for a range of reactor and radiochemical facilities plus MOD(Navy) in a period spanning the Chernobyl disaster.

His fire expertise and nuclear safety training saw him seconded to the offshore industry immediately post-Piper Alpha to kick-off risk assessments of oil platforms. He was present at the genesis of the UK Offshore Safety Case regime and has followed its development there and in other countries since. He left government service in 1990 to hold key technical and managerial roles with leading safety consultancies including DNV, Atkins and IRC. He consults to the energy, resources and transportation sectors on risk and safety matters.

Today he is interested in lifecycle management of safety and risk from pre-feasibility through to decommissioning and abandonment. He is concerned with the efficient management and effective use of safety information by organizations. He is particularly intrigued by the risk-based decision-making processes used in the boardroom and at the coalface.

His skills and experience include:

- Leadership, management and business development
- Workshop facilitation
- Safety and risk management training
- Risk-based decision-making processes
- Safety Case development & maintenance
- Risk management and ALARP demonstration
- Qualitative risk ranking methods
- QRA and reliability assessment
- Fire and explosion analysis and engineering
- Escape, evacuation, rescue & recovery analysis
- Fixed and floating oil and gas production facilities
- Subsea facilities and pipelines
- Mobile offshore drilling units

Professor Craig Valli PhD

Computer and Network Security Consultant

VULNERABILITY
ASSESSMENT GROUP

TITLE
- Consultant

QUALIFICATIONS
- Doctor of Information Technology
- Master of Management Information Systems
- Bachelor of Education

INTERNATIONAL EXPERIENCE
- Australia
- Singapore
- UK

ADDITIONAL SKILLS
- Computer and Network Forensics
-

MEMBERSHIPS
- Australian Information Security Association
- Australian Computer Society
- Australian New Zealand Forensic Science Society
- Research Network for a Secure Australia
- TISN

KEY SKILLS AND EXPERIENCE

Craig is currently the Director of the Security Research Institute at Edith Cowan University. Edith Cowan is a world leader in Digital Forensics, Computer and Network Security curriculum design and research. He has over 20 years experience in the IT Industry and consults to industry on network and computer security issues.

He is the Chair and Founder of the Australian Digital Forensics Conference and Co-Chair of the Australian Information Security Management Conference. Craig is Editor of Journal of Network Forensics and also a Co-Editor of the Journal of Information Warfare. He serves on numerous security related committees. Craig has over 40 publications to his name on security related topics.

His areas of expertise:
- Network Vulnerability assessment
- Network Penetration Testing
- Network Security
- Risk management / threat assessment
- Computer Forensics
- RFID
- Policy development
- Honeypots
- Intrusion Detection Systems
- Internet Misuse
- Wireless Security
- Networked SCADA Security
- Computer and Network Security Education

Andrew Woodward PhD

VULNERABILITY
ASSESSMENT GROUP

Wireless Computer and Network Security Consultant

TITLE
- Consultant

QUALIFICATIONS
- PhD
- BSc (Hons)
- Grad Cert. Education (Tertiary Teaching)
- Certified wireless network administrator (CWNA)

INTERNATIONAL EXPERIENCE
- Australia
- China
- Singapore
- Canada

ADDITIONAL SKILLS
- Systems Administrator
- Digital forensics practitioner
- Honeypots
- Compute clustering

MEMBERSHIPS
- AISA (Australian Information Security Association)
- RNSA (Research Network for a Secure Australia) Academic Member
- ACS (Australian Computer Society)
- TISN (Trusted Information Securing Network)

KEY SKILLS AND EXPERIENCE

Andrew is currently an academic at Edith Cowan University and is actively researching and teaching in the areas of wireless network security, network security and digital forensics. Edith Cowan is a world leader in digital forensics, computer and network security curriculum and research.

Andrew has an extensive publishing record in wireless network security and digital forensics, and has presented papers in Australia, the UK and the USA with a focus on information warfare and information security management. Andrew is also an editor for the Journal of Network Forensics.

Andrew has consulted to government departments, corporations and law enforcement agencies in the areas of wireless network vulnerability assessment, computer forensics, RFID security and network penetration testing.

His areas of expertise:
- Wireless network security (802.11, RFID, Bluetooth)
- Wireless and wired network vulnerability assessment and penetration testing
- Risk management / threat assessment
- Workshop facilitation / staff training
- Policy development
- Computer and Network forensics

Publications

Woodward, A. & Valli, C. (2008). Issues common to Australian critical infrastructure providers SCADA networks discovered through computer and network vulnerability analysis. In Proceedings of the 6th Australian Digital Forensics Conference, School of Computer and, Information Science, Edith Cowan University, Perth, Western Australia 1st December 2008

Valli, C. & Woodward, A. (2008). The 2008 Australian study of remnant data contained on 2nd hand hard disks: the saga continues. In Proceedings of the 6th Australian Digital Forensics Conference, School of Computer and, Information Science, Edith Cowan University, Perth, Western Australia 1st December 2008

Turner, B. & Woodward, A. (2008). Securing a Wireless network with EAP-TLS: perception and realities of its implementation. . In Proceedings of the 6th Australian Information Security Management Conference, School of Computer and, Information Science, Edith Cowan University, Perth, Western Australia 1st December 2008

Turner, B. & Woodward, A. (2008). Network security isn't all fun and games: an analysis of information transmitted whilst playing Team Fortress 2. In Proceedings of the 6th Australian Information Security Management Conference, School of Computer and, Information Science, Edith Cowan University, Perth, Western Australia 1st December 2008

McEniery, D. & Woodward, A. (2008).
Golygowski, L. & Woodward, A. (2008). Wireless device identification for forensic purposes. Journal of Network Forensics. (Accepted)

Woodward, A. (2008). What Artefacts do Current BitTorrent Clients Leave Behind? The 2008 International Conference on Security and Management, Las Vegas, Nevada, July 14-17
Woodward, A. & Hannay, P. (2008). Forensic implications of using the firewire memory exploit with Microsoft Windows XP. The 2008 International Conference on Security and Management, Las Vegas, Nevada, July 14-17

Hannay, A. & Woodward, A. (2008). Cold boot memory acquisition: An investigation into memory freezing and data retention claims. The 2008 International Conference on Security and Management, Las Vegas, Nevada, July 14-17

Hannay, P., Woodward, A. & Cope, N. (2007) A forensically tested tool for identification of notebook computers to aid recovery: LIARS phase I proof of concept. In Proceedings of the 5th Australian Digital Forensics Conference, School of Computer and, Information Science, Edith Cowan University, Perth, Western Australia 3rd December

Hansen, P. & Woodward, A. (2007) Network Security - Is IP Telephony Helping The Cause? In Proceedings of the 5th Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia, 4th December

Hilven, A. & Woodward, A. (2007). How safe is Azeroth, or, are MMORPGs a security risk? In Proceedings of the 5th Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia, 4th December

James, P. & Woodward, A. (2007). Securing VoIP: A Framework to Mitigate or Manage Risks. In Proceedings of the 5th Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia, 4th December (Best paper)

Valli, C. & Woodward, A. (2007). Oops they did it again: The 2007 Australian study of remnant data contained on 2nd hand hard disks. In Proceedings of the 5th Australian Digital Forensics Conference, School of Computer and, Information Science, Edith Cowan University, Perth, Western Australia 3rd December

Woodward, A. and Williams, P.A.H. (2007). Wireless Rx - Risk Assessment and Recommendations for Securing a Wireless Network in a Medical Practice. In: Proceedings of the 2007 International

Conference on Security and Management, Las Vegas, Nevada, June 25-28

Ng, D. and Woodward, A. (2007). Implications for use of different encryption algorithms on power consumption for mobile devices in the healthcare industry. In: Proceedings of the 2007 International Conference on Security and Management, Las Vegas, Nevada, June 25-28

Woodward, A. & Valli, C. (2007) Do Current Erasure Programs Remove Evidence of BitTorrent Activity?, 2nd Conference on Digital Forensics, Crystal City, Arlington, Virginia

Knights, L., Fonceca, M., Mack, G. & Woodward, A. (2006). Risks and responsibilities in establishing a wireless network for an educational institution In Proceedings of the 4th Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia

Crowley, M. & Woodward, A. (2006) Does your wireless network have criminal intent? In Proceedings of the 4th Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia

Woodward, A. (2006) Bitlocker - The end of digital forensics? In Proceedings of the 4th Australian Digital Forensics Conference, School of Computer and, Information Science, Edith Cowan University, Perth, Western Australia

Woodward, A. (2006) LIARS - Laptop inspector and recovery system. In Proceedings of the 4th Australian Digital Forensics Conference, School of Computer and, Information Science, Edith Cowan University, Perth, Western Australia

Woodward, A. (2006) Data Confidentiality and Wireless Networks: Mutually Exclusive?, SAM2006: Proceedings of The 2006 International Conference on Security and Management, Las Vegas Nevada, June 26-29, pp 404-409

Valli, C., Woodward, A., Wild, K. and Karvinen, R. (2005) An investigation into long range detection of passive UHF RFID tags, In Proceedings of 3rd Australian Computer, Information and Network Forensics Conference, School of Computer and Information Science, Edith Cowan University, Mount Lawley, Western Australia.

Williams, P., Woodward, A. (2005). Elicitation and customisation of generic skills in a security major, CISSE-AP - 1st Colloquium for Information Systems Security Education Asia Pacific, 21st -22nd November 2005, UniSA, Adelaide, South Australia.

Woodward, A. (2005). The Effectiveness Of Commercial Erasure Programs On Bittorrent Activity, In Proceedings of the 3rd Australian Computer, Network & Information Forensics Conference, School of Computer and, Information Science, Edith Cowan University, Perth, Western Australia pp.108-114.

Woodward, A. (2005). Recommendations for wireless network security policy: an analysis and classification of current and emerging threats and solutions for different organisations, In Proceedings of the 3rd Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia, pp.133-140.

Woodward, A. (2004). Wireless jacks - An analysis of 802.11 wireless denial of service attacks and hijacks. 3rd European Conference in Information Warfare. Royal Holloway, London, June 2004

Woodward, A. (2004). An analysis of current 802.11 wireless network layer one and two attacks and possible preventative measures. Journal of Information Warfare 3(3): pp37-47

Woodward, A. (2004). The risks, costs and possible solutions involved in setting up and running wireless local area networks. 2nd Australian Information Security Management Conference 04, 25 & 26 November 2004, Esplanade Hotel, Perth, WA

Woodward, A. & Wolski, P. (2004). Sleep Attack - Exploring a possible denial of service attack based on power save mode in 802.11 devices. 5th Australian Information Warfare and Security Conference 04, 25 & 26 November 2004, Esplanade Hotel, Perth, WA

Peter Hannay

Application and Network Security Consultant

VULNERABILITY
ASSESSMENT GROUP

TITLE
- Consultant

QUALIFICATIONS
- BCSci - Honors (Software Engineering & Computer Security)

ADDITIONAL SKILLS
- Systems Administrator
- Digital forensics practitioner
- Honeypots
- Computer clustering

MEMBERSHIPS
- AISA (Australian Information Security Association)
- ANZFSS (Australia New Zealand forensic science society)
- ACS (Australian Computer Society)

KEY SKILLS AND EXPERIENCE

Peter is currently an academic at Edith Cowan University and is actively researching and teaching in the areas of network security, mobile security and digital forensics. Edith Cowan is a world leader in digital forensics, computer and network security curriculum and research.

Peter has consulted to government agencies and corporations in the areas of hardware security assessment, software security assessment, data recovery, computer forensics and network penetration testing.

His areas of expertise:
- Wireless and wired network vulnerability assessment and penetration testing
- Software Security Assessment
- Hardware Security Assessment
- Embedded Device Security Assessment
- Curriculum Development
- Forensic Software Development

Publications

Hannay, P. (2008). Forensic Acquisition and Analysis of the TomTom One Satellite Navigation Unit. In Proceedings of the 6th Australian Digital Forensics Conference, School of Computer and, Information Science, Edith Cowan University, Perth, Western Australia 1st December 2008

Smart, J., Tedeschi, K., Meakins, D., Hannay, P., & Bolan, C. (2008). Subverting National Internet Censorship - An Investigation into Existing Tools and Techniques. In Proceedings of the 6th Australian Digital Forensics Conference, School of Computer and, Information Science, Edith Cowan University, Perth, Western Australia 1st December 2008

Woodward, A. & Hannay, P. (2008). Forensic implications of using the firewire memory exploit with Microsoft Windows XP. The 2008 International Conference on Security and Management, Las Vegas, Nevada, July 14-17

Hannay, A. & Woodward, A. (2008). Cold boot memory aquisition: An investigation into memory freezing and data retention claims. The 2008 International Conference on Security and Management, Las Vegas, Nevada, July 14-17

Hannay, P. (2007, 3rd December, 2007). A Methodology for the Forensic Acquisition of the TomTom One Satellite Navigation System - A Research in Progress. Paper presented at the The 5th Australian Digital Forensics Conference, Edith Cowan University, Mount Lawley Campus, Western Australia.

Hannay, P., & James, P. (2007, 3rd December, 2007). Pocket SDV with SDGuardian: A Secure & Forensically Safe Portable Execution Environment Paper presented at the The 5th Australian Digital Forensics Conference, Edith Cowan University, Mount Lawley Campus, Western Australia.

Hannay, P., Woodward, A., & Cope, N. (2007, 3rd December, 2007). A forensically tested tool for identification of notebook computers to aid recovery: LIARS phase1 proof of concept. Paper presented at the The 5th Australian Digital Forensics Conference, Edith Cowan University, Mount Lawley Campus, Western Australia.

VULNERABILITY
ASSESSMENT GROUP

NINA BURAKOWSKI

Security Intelligence Analyst

TITLE
- Security Intelligence Analyst

QUALIFICATIONS
- Master in International Relations, Curtin University of Technology
- Bachelor of Arts, University of Western Australia

ADDITIONAL SKILLS
- Fluency in English, German, French
- Certificate in Intelligence
- Training in Emergency Management
- Training in exercise management
- Knowledge of Australia's counter-terrorism arrangements

KEY SKILLS AND EXPERIENCE

Nina has international experience across the private and public sectors in research and analysis, emergency management and communications development. Exposure has been gained in the energy, resource, engineering and aviation sectors.

Nina's career focus has been on mitigating and managing political, country and sociocultural risks to an organisation's people, assets and operations. Nina has authored a broad range of analytical reports on various countries and events. These provided forecasts and assessments of political and security developments, actionable intelligence and a platform to maximise business opportunities and manage strategic and operational risks.

Nina was instrumental in the creation of a dedicated intelligence function for one of Australia's largest petroleum companies. This function provided the organization with targeted intelligence assessments to maximise business opportunities and minimise operational and strategic risks. This included the authoring of a broad range of intelligence reports on countries and events pertinent to the organization. These reports provided detailed forecasts and assessments of political and security developments, actionable intelligence and a solid platform for informed strategic decision-making for senior management.

Nina has also assisted in the establishing of a state-of-the art Crisis Centre for the Victorian Government to be activated in the event of a major emergency. This role included the coordination of Australia's largest conducted Counter-Terrorism exercise for a government department.

Her areas of experience

- Analytical products
- Research and Analysis
- Intelligence
- Threat assessment
- Emergency Management
- Risk Management (AS 4360)