# AUSCSEC at a glance.

Based in Melbourne and Canberra, **AUSCSEC** is a technology company that specializes in Information Technology Cybersecurity consultancy services. Our personalized cybersecurity consulting and management service packages are designed with the client at the center of every discussion in co-design with us because no *'one size'* fits all and all businesses are unique. Our differentiators are: being vendor agnostic; bringing a holistic approach to cybersecurity and resilience; and a unique environmental assessment process that covers both an organisation's technical environment, their operational processes and their staff's attitude towards security, particularly cybersecurity. AUSCSEC in co-design with its clients starts with a technical assessment of your IT environment and a comprehensive assessment of process and people, from a tactical and strategic perspective across key tiers of the organization. Enabling AUSCSEC to prepare a remediation plan in line with any budgetary cycle & constraints to ensure maximization of every dollar spent.

AUSCSEC has accumulated numerous potential clients in the following industry sectors; transport and logistics, civil engineering, Technology, building construction and infrastructure, manufacturing as well as manufacturing in robotic and automated innovative waterjet products and services. AUSCSEC has strong relationships with Federal Government entities and a vast and strong network in the Federal environment in Canberra as well as State jurisdictions. AUSCSEC's joint experience of over **120 years** affords opportunities and maintains respect across many Federal and State jurisdictions.

## AUSCSEC Services.

- Cyber consultancy
- Cyber awareness
- Cyber assessment and audit
- Cyber remediation
- Cyber strategy
- Cyber resilience management
- Cyber recovery

## Why AUSCSEC.

- AUSCSEC's vision is to build a legacy of true Cyber secure organizations, one that starts removing the Fear, Uncertainty and Doubt (FUD) associated with Cybersecurity and then commences the journey of helping you solve the Cybersecurity problems. We start by addressing the "human" issues first and foremost.
- Founders of AUSCSEC have more than **120 years** of combined experience in the Intelligence, ICT, and Cybersecurity fields.
- AUSCSEC works with you in co-designing Cybersecurity and resilient programs to fit all budgets and planning cycles to help you secure your most valuable assets and keep you there.

## AUSCSEC's values.

- **A**ccountability – to secure our clients, communities and the nation.
- **U**nderstanding – of the challenge at hand and the trust placed in us.
- **S**ecure – operate as a secure pair of hands.
- **C**ommitment – to each other and our clients.
- **S**uccess – define it and achieve it.
- **E**xceptional – delivery to outcomes.
- **C**ontinuous – in co-designing our client's cyber resilience.

# AUSCSEC at a glance.

Email:contact@auscsec.com.au
Phone:**02 9994 8947**
Web Site: **www.auscsec.com.au**

## AUSCSEC directors

**Debbie Lutter –** Debbie is the CEO of AUSCSEC and has worked as a Senior Signal Analyst and Telecommunications engineer as a public servant in Federal Government across the Australian Signals Directorate within the Defence portfolio, Medicare Australia, Child Support Agency and Centrelink within the Health and Department of Human Services portfolios, and more recently within the Department of Agriculture and Water Resources Portfolio agencies. Debbie is a strategic thinker with years of practical experience designing roadmaps for all levels of Cybersecurity readiness and has built many Strategic plans for numerous Federal and industry entities.

**Graham Gathercole—**has been an IT professional for over 40 years and was in Federal Government's Senior Executive Service for over 15 years. Graham has been at the SES Band 2 level for over 10 years as the Chief Information Officer at Medicare and the Department (Dept) of Agriculture, also as General Manager of ICT Infrastructure at the Dept of Human Services. As an SES Band 1 at Medicare Australia he was responsible for all of Medicare's Applications. Prior to this he was the software capability manager at the Australian Signals Directorate for 13 years.

**Tom Royal**—With over 50 years of experience in the Transport and Logistics industry Tom brings a depth of Business Acumen that is second to none. He is passionate about helping to keep Australian businesses secure and has already tapped into his enormous network in the Transport and Logistics industry to influence CEO's across all sectors to rethink their Cyber security strategy. He is highly respected in the local Melbourne area and has far reaching relationships throughout Victoria with several of his industry contacts spanning every state. Tom is the connector and brings like-minded industry sectors together to help reshape their ICT environments to keep them secure.

# AUSCSEC at a glance.

Email:contact@auscsec.com.au
Phone:**02 9994 8947**
Web Site: **www.auscsec.com.au**


AUSCSEC Assessment/Audit scans are performed through a series of interviews of key organizational personnel, the scanning interviews can be broadened to include less senior and more coal-face orientated workers to get a broader view of organizational culture and attitude towards cyber security and the use of organizational resources to access the internet, especially for personal use.

Interview questions are designed to allow AUSCSEC to assess organization cyber security hygiene and resilience holistically across people, process and technology around the following key criteria:

- Leadership,
- ASD's Essential 8,
- Key Information Security Manual criterion,
- Staff Culture and attitude to cyber security,
- Key ICT processes such as change control, release management and planning incident management, and
- Various NIST frameworks and standards and ISO standards where applicable.

Those interviews, when coupled with physical inspections of ICT environments, including data centers, and AUSCSEC's vulnerability scans can provide an organization with a solid perspective on their cyber hygiene and resilience and AUSCSEC can additionally provide a roadmap to a better state should one be required.

# AUSCSEC at a glance.

Email:contact@auscsec.com.au
Phone:**02 9994 8947**
Web Site: **www.auscsec.com.au**

## Service offering—Assessments

| Service Offering Assessment Scans | Estimated Effort | Scope |
|---|---|---|
| Initial Free Consultation | ½ to 1 day | Self-Assessment, Brief Client Interview (pref. CEO), Requirements gathering and discussion of potential options available |
| Simple Technical Environment Scan | 1-3 days / up to 3 resources | Self-assessment, Brief CEO Interview,<br>Technical Environment Vulnerability scan<br>Critical vulnerability report |
| Simple Assessment | 5-10 days / up to 3 resources | Self-assessment<br>CEO Interview<br>Vulnerability scan and analysis in consideration to the client's environment<br>Critical vulnerability report<br>2 follow-up scans and vulnerability reporting of original scan following any remediation activities. |
| Assessment & HL remediation plan | 15-20 days / up to 3 resources | Self-assessment, CEO & Operations manager Interview<br>Backup and recovery interviews<br>Vulnerability scan<br>Critical vulnerability analysis & report<br>High level remediation recommendations for critical vulnerabilities including high level analysis of recoverability.<br>2 follow-up scans and vulnerability reporting of original scan following any remediation activities. |
| Detailed Assessment and remediation plan | 20-60 days / up to 3 resources | Self-assessment, CEO, key executives and IT vendor executive interviews, Datacentre visit and detailed review of backup and recoverability<br>Vulnerability scan<br>Critical & major vulnerability analysis & report<br>Remediation plan<br>Implementation plan and high-level schedule, 3 post implementation follow-up scans |

# AUSCSEC at a glance.

Email:contact@auscsec.com.au
Phone:**02 9994 8947**
Web Site: **www.auscsec.com.au**

## Service offering — Scans

| Targeted Scans | Estimated Effort | Scope |
|---|---|---|
| Malware Scan | 1 day | Scan only for the presence of viruses and<br>2 post remediation scans |
| WannaCry Ransomware Scan | 1 day | Scan only for the presence of the WannaCry Ransom virus and 1 post remediation scan |
| Zero Logon Scan | 1 day | Remotely scan only across the Microsoft environment for elevated Net-logon privileges and 1 post remediation scan |
| Ripple 20 Scan | 1 day | Remotely scan only across the Microsoft environment for elevated Net-logon privileges and 1 post remediation scan |
| Website Scan | 2 – 5 days | Scan a website and its applications for vulnerabilities and provide guidance and assessment on remediation. 2 post remediation scans |
| Intel AMT security bypass scan | 1 day | Scan the chipsets on selected AMT processors in the infrastructure environment, up to maximum of 10 chipsets, further chipset numbers by negotiation. 2 post remediation scans |
| Meltdown and Spectre scan | 1 day | Scan selected processors in the environment for cve 2017-5715, cve 2017-5753 and cve 2017-5754, plus 1 post remediation scan |
| Badlock Detection | 1 day | Scan the Microsoft environment cve 2016-2118 and cve 2016-0128 and 1 post remediation scan |
| Drown Detection | 1 day | Scan for cve 2016-0800, SSL2 protocol vulnerability and 1 post remediation scan |
| Bash Shellshock detection | 1 day | Scan unix environments utilizing Bash for the Shellshock vulnerability and 1 post remediation scan |
| Shadow Brokers Scan | 1 – 5 days | Scan for vulnerabilities disclosed in the Shadow Brokers leak plus 2 post remediation scans |
| Solarwinds Scan | 2 days | Scan only for the presence of the **Solarwinds** Ransom virus and 1 post remediation scan |

# AUSCSEC at a glance.

Email:contact@auscsec.com.au
Phone:**02 9994 8947**
Web Site: **www.auscsec.com.au**

## Service offering — Scans

| Audit and Specialised Scans | Estimated Effort | Scope |
|---|---|---|
| Audit Cloud Infrastructure | 1 day | Scan your cloud infrastructure and validate its configuration and 1 post configuration adjustment scan |
| Internal PCI network scan | 1 day | Scan your internal PCI environment for vulnerabilities and 1 post remediation adjustment scan |
| Offline configuration audit | 2 days | Scan the ICT environment and report on device configurations and post configuration adjustment scan |
| Policy Compliance Audit | 5 days | Define a compliance policy baseline for your environment and scan against that policy and 1 post configuration adjustment |