

Executive Cyber Security, Business Continuity & Incident Response Testing Services

Prepare. Lead. Respond
with Confidence.

Australia's trusted partner for executive-level cyber crisis simulations

In an era of growing cyber threats—from ransomware to nation-state attacks—Australian executives are under increasing pressure to demonstrate operational resilience and regulatory readiness. When an incident strikes, how confident are you that your board, C-suite, and response leaders will know exactly what to do?

Our Executive Cyber Security, Business Continuity and Incident Response Testing Services are designed specifically for senior leadership teams in Australia's public and private sectors. We offer tailored, end-to-end exercises that test not just your plans—but your people, processes, and confidence under pressure.

Why this matters – now more than ever

Australian regulations (including **APRA CPS 230, Essential Eight**, and the **Security of Critical Infrastructure Act**) now demand clear proof that organisations can withstand, respond to, and recover from any incident that impacts customer facing critical services and business functions. But having a plan is not enough.

- Does your executive team have clarity on decision making during a crisis?
- Can you maintain operational control during a crisis?
- Are roles, responsibilities, and communications tested and clear to all team members?
- Are decisions aligned with legal, regulatory, and reputational consequences?

Our proven methodology goes beyond checklists to deliver meaningful, role-relevant testing tailored to your operating context and threat landscape.

What we offer – Full lifecycle support

We offer comprehensive services across the entire incident response testing lifecycle, built for executive stakeholders:

1. Discovery & Maturity Assessment

- Understand your organisation's risk appetite, cyber maturity, business continuity and IT Disaster Recovery maturity and critical business processes
- Align to industry frameworks (NIST CSF, ISO 27001, APRA CPS 230, ISM, AESCSF)
- Benchmark against similar organisations in Australia

2. Tailored Scenario Design

- Simulate high-impact, relevant incidents such as:
 - Ransomware across critical systems;
 - Website defacement;
 - Critical systems unavailability / Wide scale IT outage;
 - Business Email Compromise (BEC);
 - Supply chain, critical third party impact or cloud-based infrastructure compromise;
 - Insider threat or accidental data exposure;
 - Major business continuity impact across critical services
- Review and plan technical and executive decision points
- Plan for organisation and business aligned success metrics and focus areas from the exercise

3. Executive Briefing & Pre-Exercise Preparation

- Align roles and clarify responsibilities for board, executive, legal, communications, and operations teams
- Deliver custom briefing packs to ensure realistic participation
- Ensure alignment with Business Continuity, Crisis Communications, Cyber Incident Response and IT DRP Plans and Playbooks

4. Live-Facilitated Simulations & Tabletop Exercises

- Real-time testing led by experienced cyber crisis facilitators
- Simulate Multi-faceted crisis scenario testing critical decision making and co-ordination
- Guided escalation paths, injects, and executive as well as operational decision-making
- Facilitation of internal coordination and external communication (media, regulators, partners)

5. Post-Exercise Analysis & Recommendations

- Detailed report with heatmaps, maturity scores, and improvement actions
- Executive summary and Board-level briefings
- Insights on operational gaps, communications readiness, and role effectiveness

6. Local Threat Intelligence & Industry Insights

- Learn from recent breaches and regulatory responses across Australia
- Sector-specific insights
- Advisory on upcoming legislative changes and best practices

Who should engage us

- **CISOs** wanting to elevate cyber maturity across the executive team
- **CROs and BCM / IT DRP / Cyber Response leads** needing assurance of resilience capabilities
- **Boards and Executive Teams** preparing for CPS 230 attestation
- **Risk, Audit and Compliance** leaders seeking evidence-based readiness
- **Public Sector Executives** aligning with VPDSS, ISM, and the Critical Infrastructure Act

Why work with us

- **Local Expertise** – Deep knowledge of Australian threat landscape and regulations
- **Executive Relevance** – Exercises crafted for the C-suite, not just IT
- **Proven Methodology** – Structured, repeatable, and regulator-aligned
- **Independent & Unbiased** – Vendor-neutral and confidential
- **Real Results** – Post-exercise improvements that drive true readiness

Let's test before you're tested

Cyber crises do not give you time to prepare. We do.

Let's ensure your organisation's leaders can make the right calls when it matters most.

Contact us today to schedule an executive incident response simulation or request a tailored briefing for your leadership team.

For further information please contact:



Darren Booth

Partner
03 9286 8158
darren.booth@rsm.com.au



Ashwin Pal

Partner
02 8226 4500
ashwin.pal@rsm.com.au



Riaan Bronkhorst

Partner
08 9261 9100
riaan.bronkhorst@rsm.com.au



Kaustubh Vazalwar

Director
03 9286 8255
kaustubh.vazalwar@rsm.com.au