Black Shard

BLACK SHARD · SOFTWARE ENGINEERING & CYBERSECURITY

Capability statement

An Australian software engineering and cybersecurity firm. We build and run software in regulated industries, then attack it the way an adversary would. Penetration testing, red teaming, advisory, compliance, breach remediation, secure-by-design builds.

Black Shard Pty Ltd · ABN 66 696 910 773
Level 35, 71 Eagle Street, Brisbane QLD 4000
info@blackshard.com.au · blackshard.com.au

JULY 2026

THE FIRM

We build software. Then we break it before attackers do.

Software that ships fast and stands up to attack, from one team accountable for both. We build it, then break it the way an adversary will, so weaknesses are closed before production finds them.

Every name here has trusted us with real work: systems we build and run, and systems we test and secure.

bold · GRM LAW · aurii · restart recruitment · stoneleaf CAPITAL · Fox Property Advisory

SECTOR	NAMED BUILD	RELATIONSHIP
Legal	GRM LAW	undefined
Health	Aurii	undefined
Financial services	Stone Leaf Capital	undefined
Property	Bold Property Group	undefined
Recruitment	Restart Recruitment	undefined
Government & suppliers	Essential Eight uplift & supplier readiness	

Four things we operate from

We secure what we build.

We do not only test from the outside. We build and run software in regulated industries ourselves, so we test the way an attacker thinks and fix the way an engineer ships.

Verifiable, never overclaimed.

We hold SMB1001:2026 Gold, issued by CyberCert and listed on the public registry. It is the one certification we name, and every other framework on our trust page is labelled for exactly what it is.

Compliance-fluent by default.

Essential Eight, SMB1001, ISO 27001, the Privacy Act. The frameworks Australian businesses are actually asked for are part of how we work from the start.

Honest about what we don't know.

Reading the reality means naming what we will need help with, up front.

ENTITY
Black Shard Pty Ltd

ABN
66 696 910 773

PHONE
1800 370 270

OFFICE
Level 35, 71 Eagle Street
Brisbane QLD 4000

CONTACT
info@blackshard.com.au
blackshard.com.au

DELIVERY
Brisbane office, delivered Australia-wide.

RESPONSE
Someone will contact you as soon as possible.

DIRECTORS
Kane Roberts · Gavin McInnes

INSURANCE
Professional indemnity, public liability, and cyber cover held; certificates of currency on request.

CERTIFICATION
SMB1001:2026 Gold, independently issued and verifiable on CyberCert's public registry.

SERVICES

Two practices. One team.

Six service families across software engineering and cybersecurity, delivered by one team accountable for both.

SOFTWARE ENGINEERING PRACTICE

Software engineering

Engineering for the systems a business runs on: web, native mobile, portals, and the platform underneath.

Product & platform engineering

Full builds from brand to production: web apps, native iOS and Android, client portals, and internal operations platforms.

Web development

Marketing sites, web applications, and client portals engineered for speed, accessibility, and a security posture you can verify.

Mobile app development

Native iOS and Android apps taken from concept through the App Store and Google Play, by a team that ships its own.

UI/UX design

Interface and product design that earns trust: UX flows, design systems, and brand identity for software people rely on.

Cloud engineering on Azure

The Azure architecture we run in production ourselves: Container Apps, PostgreSQL, Key Vault, and CI/CD with workload identity.

AI & automation engineering

Speech, document, and workflow automation wired into real operations, not bolted on.

Secure-by-design development

Security in the SDLC from the first commit, the way we build our own products in regulated industries.

ENGAGEMENT SHAPE An embedded build engagement with a weekly ship cadence, or a fixed-scope build with a defined brief and delivery date.

SECURITY PRACTICE

Penetration testing & red teaming

We attack your systems the way a real adversary would, then hand you a ranked fix list.

Penetration testing

Web app, API, and network testing against the OWASP and ASD playbooks.

Red teaming & adversary simulation

A goal-driven, multi-vector simulation against the systems and data an attacker actually wants.

Phishing & social-engineering simulation

Controlled phishing and pretext campaigns that measure real-world susceptibility.

The line between a scan and a penetration test is a human adversary.

SECURITY PRACTICE

Security advisory & vCISO

Ongoing security leadership and review, without hiring a full-time CISO.

Security posture assessment

A structured gap analysis against the Essential Eight and CIS Controls.

vCISO: fractional security leadership

Strategy, policy, board reporting, and incident readiness, sized to you.

Azure cloud security review

We run on Azure and secure it daily. We review yours the same way.

Entra ID & Microsoft 365 identity security

Identity is the perimeter now. We review and harden the tenant your business signs in to, the way we run our own.

Managed exposure monitoring

Scheduled external scans of your internet-facing systems by Assay, our own scanner, read by a senior engineer rather than forwarded raw.

Detection & response advisory

Make sure you would actually see an attack, and know what to do.

ENGAGEMENT SHAPE An ongoing monthly retainer, or a one-off assessment to start.

SECURITY PRACTICE

Compliance & certification readiness

Get audit-ready against the frameworks Australian businesses are actually asked for.

Essential Eight uplift

Assessment and uplift across the ASD Essential Eight maturity model.

SMB1001 certification readiness

We hold SMB1001:2026 Gold ourselves. We will get you ready to certify.

ISO 27001 readiness

Scope, gap analysis, and ISMS groundwork toward ISO 27001 certification.

Privacy Act / APP uplift

Map your data, meet the Australian Privacy Principles, prepare for reform.

ENGAGEMENT SHAPE A defined program with milestones toward your certification or audit date.

SECURITY PRACTICE

Breach remediation & incident response

Incident response and remediation engineering for organisations that have had, or suspect, a security incident.

Incident containment & triage

Establish what happened, what was reached, and stop it getting worse.

Root-cause analysis & remediation engineering

We fix the flaw behind the incident: the code, configuration, or infrastructure that let it happen.

Notifiable Data Breaches support

Work through the Privacy Act assessment and notification obligations with a team that knows the scheme.

Incident readiness

Build the response before you need it: the plan, the practice run, and proof your backups actually restore.

ENGAGEMENT SHAPE A fixed-scope engagement: containment and triage first, then remediation with a re-test to confirm the fixes closed.

SECURITY PRACTICE

Secure development & code review

Line-level code review, threat modelling, and security architecture from a team that ships production code.

Secure code review

A line-level review of your codebase for the risks that actually bite.

Security architecture & threat modelling

Design-stage review of where a system can be attacked, before you build it.

ENGAGEMENT SHAPE A standalone review with a re-review of the fixes, or an embedded engagement across a build.

If it involves building, running, or securing technology, it is in scope.

The full range, from one team: software engineering, penetration testing and red teaming, security advisory and vCISO, breach remediation, compliance readiness, and secure development.

HOW WE ENGAGE

Scoped first. Accountable throughout.

Fixed-scope engagement	STARTUPS & SMB	A penetration test, review, or build with a clear target, timeframe, and deliverable.
Ongoing advisory / vCISO	MID-MARKET & ENTERPRISE	A standing security seat: strategy, review, and board-ready reporting on a regular cadence.
Compliance program	REGULATED BUSINESSES	A milestone-driven program toward Essential Eight, SMB1001, ISO 27001, or Privacy Act readiness.
Embedded engineering	PRODUCT OWNERS	A standing build team that designs, ships, and operates software under an ongoing engagement.

Every engagement includes

A director on the work

A director reads the brief, scopes the engagement, and stays accountable for the result.

Fixed scope, quoted first

Scope, timeframe, and price are agreed before work starts.

Findings validated by hand

Every finding is checked by a human, written in plain English, and paired with a concrete fix. Raw scanner output is never forwarded.

A re-test to prove it

Fixed-scope offensive work includes a re-test, so fixes are confirmed closed rather than assumed.

Least-privilege access

We take only the access the work requires, and client data sits in Australian regions.

A report that is yours

Written for your engineers and your board, and kept confidential.

Three steps. One commitment.

Read the real risk.

We learn the system before we test it.

Test like an adversary.

We attack it the way someone who means harm would.

Fix like an engineer. Then prove it.

Remediation that lands, and a re-test to confirm it.

TRUST & COMPLIANCE

Security you can verify.

What we hold is independently issued and checkable; what we self-assess is labelled exactly that.

STANDARD	SMB1001:2026 Gold (Level 3)
HELD BY	Black Shard Pty Ltd · ABN 66 696 910 773
ISSUED BY	CyberCert
ACTIVE	16 June 2026 to 17 June 2027
BASIS	Formal director attestation against the standard's 27 controls
VERIFY	https://certification.cybercert.ai/issued/3b8d8245-6bdb-4cd2-b073-b727020cc058

The frameworks we build to

ASD Essential Eight

SELF-ASSESSED · MATURITY LEVEL 1

The Australian Signals Directorate's eight mitigation strategies: patching, application control, multi-factor authentication, restricting administrative privileges, and the remaining strategies. We self-assess at Maturity Level 1, and most of these controls overlap directly with the SMB1001 controls we attest to, so the two reinforce one another rather than sitting apart.

Privacy Act 1988 · Australian Privacy Principles

ALIGNED

As an Australian operator handling personal information, we build to the Australian Privacy Principles under the Privacy Act 1988: collection limits, purpose, access and correction, and breach handling. This is the regime that applies to us, designed in rather than retrofitted.

ASD Information Security Manual (ISM)

ALIGNED

The Australian Government cyber security framework for systems that handle official information. We design and operate the controls behind our software to the ISM where it applies, so work that touches government-grade obligations starts from the right baseline.

CIS Controls v8

SELF-ASSESSED

The Center for Internet Security vendor-neutral critical security controls. We measure our engineering and operations against them as a cross-check on the Australian frameworks, so nothing important falls between the two.

The posture behind the certificate

Least-privilege access

People and systems get only the access the work requires, and no more. Administrative privilege is restricted and granted deliberately, not by default, and access is reviewed as roles change.

Encryption in transit and at rest

Data is encrypted on the wire and where it is stored. We rely on the encryption primitives the underlying platforms provide rather than rolling our own.

Backups and recovery

Production data is backed up so we can recover from loss or corruption. Recovery is treated as something to rehearse, not assume.

Incident handling

We have a defined path for identifying, containing, and communicating a security incident, including the notification obligations the Privacy Act places on us where a breach is likely to cause serious harm.

Vendor and sub-processor discipline

We keep the set of third parties that touch data deliberately small, prefer platforms that hold their own independent assessments, and choose Australian regions for the services that host client data.

Coordinated disclosure. If you believe you have found a vulnerability in a Black Shard system, email info@blackshard.com.au with enough detail to reproduce it. We acknowledge reports within 48 hours, we do not take legal action against good-faith research, and we credit reporters who want it. Our security.txt is published per RFC 9116.

RECENT WORK

We build and run the software we secure.

These five are the recent public slate; much of what Black Shard ships runs privately.

Bold Property Group

A new buyer’s agency, built from the brand to the deal-flow systems.

PROPERTY · UNDEFINED · LIVE

BOLDPROPERTYGROUP.COM.AU

GRM LAW

A Brisbane law firm. Black Shard built and operates the compliance and operations portal the firm runs on.

LEGAL · UNDEFINED · LIVE

PRIVATE PORTAL

Aurii

Clinical voice software for Australian private-hospital specialists, built on Azure from the apps to the audit trail.

HEALTH · UNDEFINED · LIVE

AURII.COM.AU

Restart Recruitment

A senior-specialist and executive search firm built to run fewer searches at a time, properly.

RECRUITMENT · UNDEFINED · LIVE

RESTARTRECRUITMENT.COM.AU

Stone Leaf Capital

An Australian capital-markets firm. Black Shard was engaged to build the firm’s technology, brand, and operating systems.

FINANCIAL SERVICES · UNDEFINED · LIVE

STONELEAFCAPITAL.COM.AU

info@blackshard.com.au

Someone will contact you as soon as possible. Brisbane office, delivered Australia-wide.

Level 35, 71 Eagle Street, Brisbane QLD 4000

blackshard.com.au