



ABIRYVA

COMPANY BOOKLET / OCTOBER 2026

Clear decisions. Secure technology. Stronger resilience.

Practical advisory across cybersecurity, AI governance,
cloud security, transformation and resilience.

WHO WE ARE

Technology decisions, grounded in your priorities.

Abiryva supports organisations that need a clearer view of technology risk, governance and change.

We bring strategy, assurance and delivery oversight together so leaders can understand their options, agree practical priorities and move forward with a defined scope.

Understand the context

We begin with your objectives, existing environment, constraints and the decisions you need to make.

Connect governance and delivery

Advice is linked to ownership, controls, implementation priorities and the evidence needed to track progress.

Build capability that lasts

Documentation, workshops, exercises and knowledge transfer help your team use the results after the engagement ends.

We welcome conversations with public-sector organisations, healthcare teams, enterprises and other organisations seeking practical technology and security support.

FIVE SERVICE LINES

Focused expertise. A joined-up approach.

Start with the area that matches your immediate priority. Related capabilities can be brought together within an agreed engagement.

01 **Cybersecurity, GRC and CISO Advisory**

Leadership, assurance and practical control improvement.

02 **AI Governance and Secure Adoption**

Governance and assurance for responsible AI adoption.

03 **Cloud, Workplace and Endpoint Security**

Secure cloud foundations, identities, devices and collaboration.

04 **Digital and Public-Sector Transformation**

Clear strategies, delivery governance and technology roadmaps.

05 **Resilience, Incident Readiness and Capability**

Continuity, recovery and incident preparedness through planning and exercises.

LEADERSHIP AND GOVERNANCE

Secure decisions. Responsible adoption.

Cybersecurity, GRC and CISO Advisory

- CISO and cybersecurity leadership advisory
- Fractional CISO support
- Cybersecurity strategy and operating models
- Governance, risk and compliance (GRC)
- Cyber risk assessments and risk-register development
- ISO/IEC 27001 readiness, implementation support and transition
- Information security policies, standards and procedures
- Internal audit and control reviews
- Regulatory and framework mapping
- Third-party and supplier security risk
- GRC platform advice and implementation support, including OneTrust and ServiceNow
- Security awareness and phishing programme design
- PCI DSS gap analysis and readiness support
- Security architecture and control design
- Vulnerability and external attack-surface management coordination
- SIEM and security monitoring design or improvement

AI Governance and Secure Adoption

- AI governance strategy and operating model
- AI policies, standards and acceptable-use guidance
- AI use-case inventory and risk assessment
- Generative AI and Microsoft Copilot readiness
- Secure AI adoption and pilot assurance
- AI privacy, security and data-protection controls
- AI risk-register development and governance reporting
- AI regulatory and framework alignment
- Staff AI awareness and training

FOUNDATIONS AND CHANGE

Modernise with security and oversight.

Cloud, Workplace and Endpoint Security

- Azure cloud strategy, architecture and security
- Azure migration and landing-zone advisory
- Microsoft 365 security and configuration advisory
- Cloud security posture and control reviews
- Identity and access management
- Endpoint security and hardening
- Mobile Device Management (MDM) requirements, design and vendor selection
- Cisco Meraki MDM solution design or implementation support, subject to the agreed delivery and licensing route
- Microsoft Defender and endpoint protection advisory
- Secure workplace and collaboration design
- Cloud and endpoint migration assurance
- Technology procurement and solution selection

Digital and Public-Sector Transformation

- Digital and technology strategy
- IT and digital transformation advisory
- Target architecture and technology roadmaps
- Technology business cases and investment advice
- Programme and project assurance
- Project and transformation governance
- Requirements gathering and procurement-ready specifications
- Systems integration and data-flow design
- Public-sector technology and digital-government advisory
- Service-management and operating-model improvement
- Technology implementation oversight
- Vendor and delivery coordination

PREPARE, EXERCISE, IMPROVE

Resilience, Incident Readiness and Capability

Understand critical dependencies, prepare for disruption and build confidence through practical exercises.

- Business Continuity Planning (BCP)
- Disaster Recovery (DR) planning and testing
- Business impact analysis (BIA)
- Incident-response plans and readiness reviews
- Cyber incident tabletop exercises
- Security Operations Centre (SOC) strategy and operating-model design
- Security incident monitoring and response coordination through suitable specialists
- Recovery planning and crisis-management support
- Cybersecurity training and awareness
- Role-based security training and executive briefings
- Exercise design, lessons learned and remediation tracking

Capabilities that connect

Training can support all five service lines. SIEM and monitoring design sits within cybersecurity advisory and supports incident readiness. Business continuity and disaster recovery sit within this resilience service line.

HOW AN ENGAGEMENT RUNS

A clear next step, at every stage.

The scope, responsibilities and outputs are agreed around your needs. Delivery can be phased to match capacity and priorities.

01 **Discovery**

A 30-minute discovery call to discuss your situation, the decisions ahead and whether further support would be useful.

02 **Understand and assess**

Agree the scope, review relevant information and engage the stakeholders needed to establish the current position.

03 **Prioritise and plan**

Define practical actions, owners and dependencies. Translate findings into a roadmap or delivery brief.

04 **Support and assure**

Provide the agreed advisory, assurance, coordination or implementation support, with progress reviewed against scope.

05 **Handover and improve**

Share the agreed documentation, lessons and next steps so your team can maintain momentum.

START A CONVERSATION

Book a discovery call.

Tell us what you are working towards, where the difficulty sits and what a useful outcome would look like.

30 minutes to explore your priorities.

Book through the Abiryva website. We verify your email before opening the discovery call calendar.

abiryva.com/contact.html

Email

info@abiryva.com

Phone

+353 85 160 2043

Contact address

Manorfield, Kinnegad

Westmeath, N91DF89, Ireland

Technology expertise

Technology references describe areas of expertise. They do not, by themselves, indicate vendor accreditation or an authorised reseller relationship. Where external specialists deliver work, responsibilities and licensing are identified in the agreed scope.