ADACOM

SECURITY BUILT ON TRUST

IRMS Design & Implementation

About ADACOM

ADACOM, a Byte subsidiary, is a leading cybersecurity solutions and services provider, delivering cutting-edge security strategies to organizations worldwide. With expertise in enterprise security architecture, managed security services, and threat intelligence, ADACOM empowers businesses to strengthen their cyber resilience.
Our portfolio integrates next-generation security technologies with advanced services, ensuring robust protection against evolving cyber threats.

Incident Response Management System

ADACOM helps organisations establish an IRMS that connects cyber incident response with executive decisions, business continuity and secure recovery. The service turns defined responsibilities and response procedures into an exercised capability for protecting critical business services.

Business value

When a cyber incident disrupts operations, leaders need clear authority, reliable information and agreed recovery priorities. IRMS establishes how security teams, business owners and management work together throughout the incident lifecycle.

- **Reduce disruption.** Prioritise containment and recovery using business impact, service dependencies and agreed recovery objectives.
- **Accelerate decisions.** Define escalation thresholds, delegated authority and approval requirements before a crisis.
- **Strengthen accountability.** Record decisions, preserve evidence and maintain consistent executive and stakeholder communications.

IRMS Operation model

Layer	What we establish
Governance	Executive sponsorship, incident ownership, decision authority and risk acceptance.
Coordinate	A shared incident picture across SOC or CSIRT, IT, business owners, Legal, Privacy and Communications.
Response & Recovery	Detection, triage, containment, eradication and recovery with defined approvals and acceptance criteria.
Assurance & improvement	Exercises, performance reporting, management review and tracked corrective actions.

Service coverage

The design covers the agreed business services, entities and locations, including IT, cloud, identity, third parties and OT where applicable. Scenario selection reflects organisational exposure and can include ransomware, data exfiltration, supplier compromise, AI-enabled fraud and incidents involving enterprise AI agents.

You are PROHIBITED from copying, reproducing, distributing transmitting, modifing, creating derivative works, or in any other way exploit any part of the content of this document.

ADACOM

SECURITY BUILT ON TRUST

IRMS Design & Implementation

Continuous improvement through PDCA

PDCA keeps the IRMS effective through recurring reviews, exercises and lessons learned.

Plan Define scope, assess risks and agree response objectives, responsibilities and resources.

Do Implement procedures and playbooks, train teams and operate the incident response capability.

Check Review KPIs, exercises and incident records through audits and management review.

Act Close corrective actions, update controls and playbooks, and revise priorities for the next cycle.

Implementation and deliverables

A tailored engagement with defined acceptance criteria

We work with an executive sponsor, the CISO or incident response lead and relevant service owners. The engagement is structured around five phases, with scope, milestones and responsibilities agreed at mobilisation.

Phase	Core activities and outputs
01 Assess	Review current capabilities, critical services and dependencies. Deliver a readiness assessment, gap register and prioritised roadmap.
02 Design	Define scope, policy, governance, roles and severity criteria. Deliver the IRMS manual, RACI and escalation and decision matrices.
03 Implement	Develop agreed playbooks, evidence procedures and communication templates. Align workflows with existing SOC, case management and continuity processes.
04 Validate	Train relevant teams and run a cross-functional tabletop exercise. Test escalation, containment decisions, communications and recovery acceptance.
05 Handover	Deliver controlled documentation, the exercise report, corrective action plan and KPI baseline. Establish ownership and the review schedule.

Key deliverables

The service produces an IRMS governance and documentation pack, scenario playbooks, stakeholder contact and notification matrices, incident and decision registers, evidence handling templates, recovery acceptance criteria and a management reporting template. Regulatory notification workflows are tailored with the organisation's Legal and Privacy teams.

Measurable readiness

We define measurement start and stop points, data sources and accountable owners. Baselines and targets are agreed during design and tested through exercises or subsequent operations.

Typical measures include time to incident declaration and containment, critical services with exercised playbooks, notifications completed within applicable deadlines, recovery against agreed objectives and corrective actions closed on time.

Governance and acceptance

ADACOM leads assessment, design, documentation and validation. The client approves policy and operational authorities, supplies service and dependency information, and retains accountability for business risk and regulatory decisions. Acceptance requires approved documentation, an executed exercise and an owned action plan.

Standards and engagement options

The methodology draws on ISO/IEC 27001, ISO/IEC 27035, ISO 22301, NIST CSF 2.0 and NIST SP 800-61 Rev. 3. Requirements mapping can support NIS2 and DORA readiness where applicable. IRMS implementation does not itself confer certification or establish regulatory compliance.

Duration, playbook coverage and integrations are agreed in the statement of work. Technical integrations, 24/7 monitoring, incident response retainers, digital forensics and ongoing IRMS maintenance can be scoped separately.

Contact Us

www.adacom.com

GREECE / HQ
25, Kreontos str.,
104 42, Athens
+30 210 51 93 700
info@adacom.com

GREECE / Thessaloniki Office
10th km Thessalonikis - Thermis
570 01, Thermi, Thessaloniki
+30 2310 474 296
info@adacom.com

CYPRUS
70 Stadiou str.,
Strovolos, 2057, Nicosia
+357 22 444 071
infocy@adacom.com

KINGDOM OF BAHRAIN
Manama Center, Blog: 316
Road: 383, Building: 128 Flat/
Office: 2030
info@adacom.com

You are PROHIBITED from copying, reproducing, distributing transmitting, modifing, creating derivative works, or in any other way exploit any part of the content of this document.