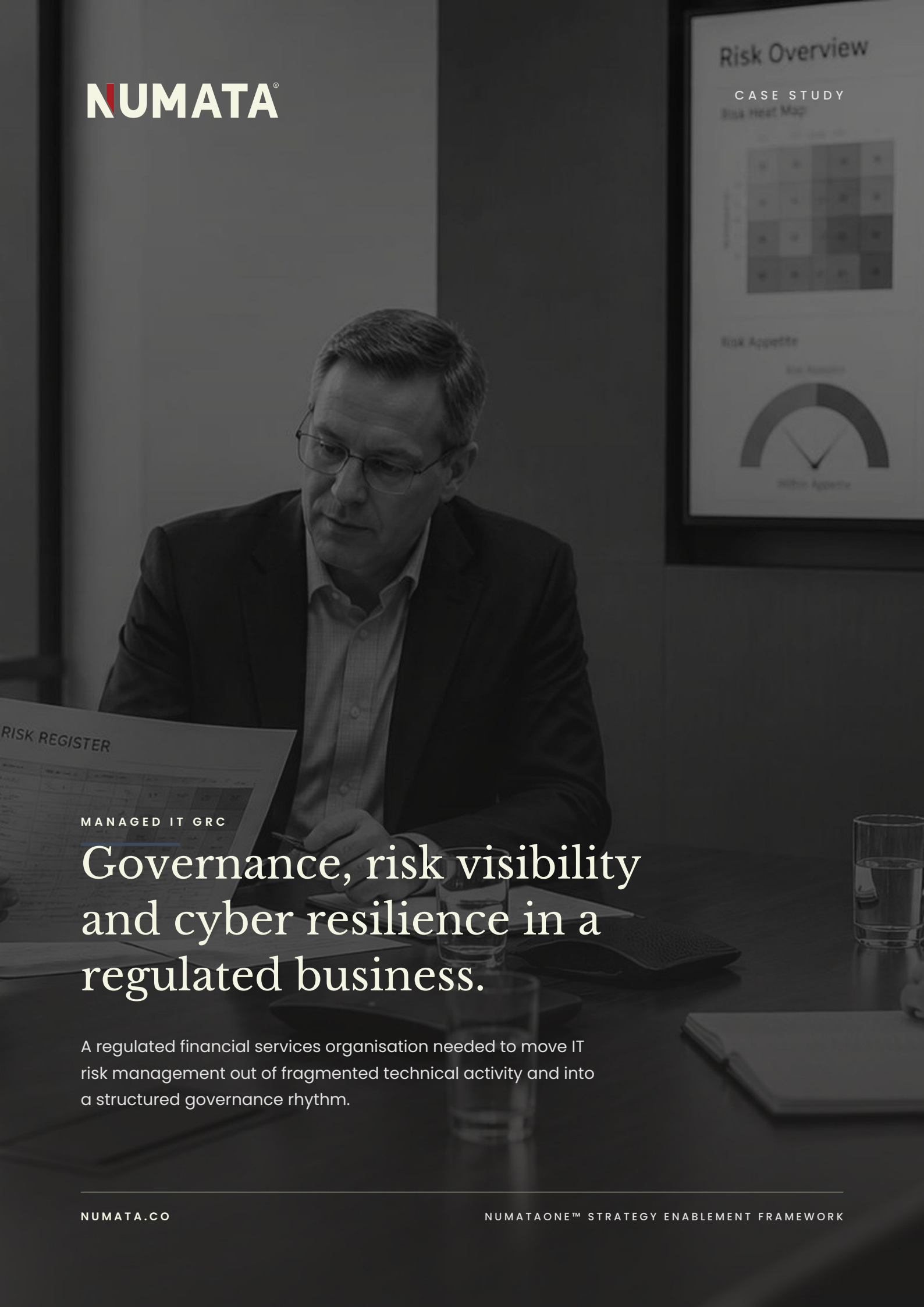
NUMATA®

CASE STUDY



MANAGED IT GRC

Governance, risk visibility and cyber resilience in a regulated business.

A regulated financial services organisation needed to move IT risk management out of fragmented technical activity and into a structured governance rhythm.

MANAGED IT GRC / REGULATED FINANCIAL SERVICES / ANONYMISED

AT A GLANCE

GRC

Managed governance, risk and compliance running as an ongoing capability

SteerCo

Recurring IT and GRC forum giving leadership oversight and accountability

SOC

Relationship expanded into managed security services after a competitive process

A regulated financial services organisation needed to move IT risk management out of fragmented technical activity and into a structured governance rhythm. Numata delivered a Managed IT GRC programme that gave leadership clearer visibility of risks, priorities, evidence requirements and security improvement actions, then expanded into broader managed security services.

THE CHALLENGE

The client needed more than a once-off compliance review. It required a practical operating model for IT governance, risk management, compliance readiness and cybersecurity oversight. Internal steering material pointed to the same gaps: IT oversight was not formalised in a governance forum aligned to risk and audit structures, priority risks and audit findings spanned storage capacity, ageing infrastructure, policy gaps, backup management, segregation of duties, unsupported software and security event monitoring, and evidence collection was manual. Regulatory and cyber resilience expectations relevant to financial services needed a clearer basis for alignment.

OUR APPROACH

01 Managed IT GRC service model: governance framework selection, risk management, compliance reporting, security control implementation, policy support, vendor risk and continuous monitoring.

02 GRC platform onboarding: baseline assessment, evidence collection, Plans of Action and Milestones, and consolidated controls across relevant standards.

03 Governance forum support: a recurring IT and GRC forum for oversight, decisions, accountability and transparency on how technology supports business objectives.

04 Cybersecurity alignment: vulnerability scanning, cyber-awareness activity, dark web and posture discussions, and control gap reviews tied to the GRC roadmap.

05 Controls and roadmap work: review of risk items, audit findings, priority projects and regulatory control alignment relevant to financial services.

06 Executive reporting: consolidated status, gaps, partial alignments and expected remediation actions for senior stakeholders.

WHAT WE DELIVERED

- Active managed GRC delivery: platform walkthroughs, controls assessment, roadmap activity and ongoing support.
- A formal IT and GRC governance forum operating inside the wider governance, risk and compliance framework.
- Consolidated risk visibility across IT landscape information, priority initiatives, risk register items, audit findings and remediation priorities.
- Immediate risk reduction: a priority storage risk addressed by increasing disaster recovery capacity, with monitoring retained and no related incidents recorded afterwards.
- Security posture progress: solution onboarding completed, vulnerability scanning commenced and known exploited vulnerabilities prioritised for remediation.
- Regulatory alignment: controls extracted, mapped and cross-walked against recognised cybersecurity frameworks to reduce manual assessment effort.

> “IT risk moved from fragmented technical activity into a structured governance rhythm, with clear visibility of risks, priorities, evidence and security improvement actions.”
>
> NUMATA ENGAGEMENT SUMMARY, ANONYMISED FINANCIAL SERVICES CLIENT

WHAT WE TOOK FROM IT

01 GRC is not a compliance checklist. It works when it is connected to business leadership, risk ownership, audit themes and technical remediation.

02 A governance rhythm makes risk actionable: recurring review turns register items and audit findings into decisions.

03 Platform-led evidence collection removes the manual effort that usually stalls compliance programmes.

04 Consistent delivery in the governance programme is what earns the wider cybersecurity mandate.

ABOUT NUMATA

Numata is a business technology services and solutions provider for small and mid-sized enterprises. We align technology to business outcomes across IT strategy, cyber, data, operations, modern work and AI, delivered through NumataOne™, our strategy enablement framework.

Speak to the team: numata.co/contact