BENTLEY MOORE EXECUTIVE

Vendor Risk Management Consulting Services

Vendor Risk Management Consulting Services

Introduction

As organisations increase their use of third-party vendors through full or partial outsourcing, they inevitably create a more complex third-party services landscape. Cloud providers, SaaS products, infrastructure vendors, specialist consultancies, niche service providers and outsourced operational partners all become integral to day-to-day operations and strategic delivery.

While this enables flexibility and access to specialist capability, it also introduces a significant and often under-managed risk profile. Service continuity, data protection, information security, operational resilience, financial exposure and regulatory compliance can all be materially affected by vendor performance and behaviour.

Because of this, organisations must implement a structured and effective Vendor Risk Management (VRM) approach.

Any VRM or third-party vendor risk management framework must be:

- **Robust** – able to address real-world complexity and risk, not just theoretical controls
- **Wide-ranging** – covering the full vendor lifecycle and all relevant risk domains
- **Cross-business** – operating across functions, not confined to procurement or IT
- **Embedded** – integrated into BAU, not treated as a one-off initiative

Bentley Moore Executive provides the expertise to design, implement and embed VRM frameworks that give organisations clarity, control and confidence in their vendor ecosystem.

The Challenge

For any business wanting to implement a VRM framework, there are multiple, interrelated considerations that must be addressed to make the framework effective in practice:

- **Determining the organisation's VRM needs** – understanding which vendors matter most, what types of risk they introduce, and which areas of the business are most exposed.
- **Defining and implementing VRM processes** – creating repeatable, end-to-end processes for onboarding, due diligence, assessment, approval, monitoring, remediation and exit.
- **Agreeing and defining vendor assessment criteria** – designing criteria that are proportionate to vendor risk (e.g. critical, high, medium, low) and that take into account financial stability, operational resilience, information security, data protection, continuity arrangements and regulatory implications.
- **Creating and managing vendor assessments** – operationalising assessments so they are actually completed, reviewed, challenged where needed, stored and updated.
- **Defining the process for selecting vendors** – ensuring that vendor selection is not purely commercial or convenience-driven, but informed by risk and long-term strategic suitability.

- **Defining contractual terms and conditions** – ensuring that contracts embed VRM requirements (e.g. data protection, audit rights, SLA/KPIs, exit provisions, security obligations, incident notification, business continuity).
- **Identifying and establishing enterprise-level requirements and agreements** – avoiding fragmentation and duplication by creating enterprise-wide standards and, where appropriate, enterprise-level agreements.
- **Supplier relationship management** – ensuring ongoing engagement, communication, escalation routes, and structured relationship governance with key vendors.
- **Supplier performance monitoring** – establishing dashboards, reporting and reviews to track performance, non-compliance and emerging risk.
- **Defining and implementing a VRM governance framework** – clarifying roles, responsibilities, decision rights and escalation paths.
- **Ending a vendor contract, relationship or renewal** – managing exit processes so risk is minimised and continuity is maintained.
- **Managing vendor exits** – planning and executing transitions away from vendors, including data, knowledge, access, and responsibility handover.
- **Establishing VRM as a part of BAU** – embedding VRM into day-to-day operations so it becomes part of "how we work", not an occasional fire drill.

Scenario 1 – Business Starting the VRM Journey with a Few Vendors

For organisations at the very beginning of their VRM journey, there is typically no existing VRM framework, limited internal expertise, and a small vendor population. In this context:

- The organisation may not yet fully appreciate the potential risk exposure, because individual vendors appear manageable.
- Processes are often informal (e.g. "we trust them", "we've always used them", "they came via a recommendation").
- Documentation, assessment and monitoring may be minimal or non-existent.

The positive aspect is that it is simpler and less resource-intensive to implement a scalable VRM framework at this early stage, before vendor sprawl and legacy complexity accumulate.

Scenario 2 – Business Starting the VRM Journey with a Complex Vendor Landscape

For organisations commencing the VRM journey with a large, complex third-party vendor landscape, the situation is materially more demanding:

- There may be hundreds of vendors across different business units and geographies.
- Contracts may be inconsistent, fragmented, overlapping or out of date.
- Different parts of the organisation may be using the same vendor under different terms and conditions.
- There may be no single, reliable inventory of vendors, services, risk exposure or contract end dates.
- Critical services may depend on vendors that have never been properly assessed.

In this scenario, implementing a VRM framework and applying it retrospectively can be a complex, multi-phase undertaking requiring:

- A coordinated programme of discovery, analysis, assessment and remediation.
- A blend of skills including risk, commercial, procurement, security, operations and governance.
- A dedicated VRM team, often working over many months to bring the landscape under control.

In both scenarios, organisations often **lack the in-house skills and experience** to design, implement and embed an effective VRM framework. External specialist support is therefore required, especially in the case of larger, complex landscapes where a multi-disciplinary team is needed and the work can extend beyond a year.

Bentley Moore Executive provides that specialist support.

Our Vendor Risk Management Consultancy Services

We provide VRM Consulting Services across the full lifecycle and operating model.

Each service component can be delivered as a stand-alone engagement or as part of a holistic, end-to-end VRM implementation.

1. VRM Processes

We work with you to design, document and implement end-to-end VRM processes that are proportionate, practical and scalable:

- **End-to-end VRM process definition** – defining the full lifecycle from vendor identification, screening and due diligence, through onboarding, monitoring, remediation and exit.
- **Determining the organisation's VRM needs** – assessing your current vendor landscape, risk appetite, regulatory context and operational priorities to determine what VRM needs to cover and at what level of depth.
- **Creating scalable workflows** – ensuring processes can handle growth in vendor numbers without becoming unmanageable.
- **Integration into BAU** – embedding VRM steps into existing processes (e.g. procurement, onboarding, change management, supplier performance reviews) so that VRM is not an isolated activity.
- **RACI and hand-off points** – clearly defining who does what, when, and how information flows between teams (procurement, legal, IT, security, operations, risk, finance).

2. Vendor Assessments

Vendor assessments sit at the heart of VRM. We design and implement assessment models that are risk-based and workable in real life:

- **Risk-based tiering and classification** – categorising vendors (e.g. critical / high / medium / low) according to impact on services, data, operations, financial exposure and regulatory obligations.
- **Assessment criteria definition** – defining criteria that cover:
  - Financial stability
  - Information security and data protection

  - Operational resilience and continuity
  - Regulatory and legal compliance
  - Service capability and delivery maturity
  - Culture, behaviour and alignment with client values
- **Assessment tools and templates** – creating standard questionnaires, scoring matrices and evidence requirements.
- **Assessment execution** – advising or supporting the collection, review and challenge of assessment responses, including follow-up queries and remediation requirements.
- **Periodic reassessment** – implementing regular reassessment cycles for higher-risk vendors, and event-driven reviews (e.g. incidents, changes in scope, ownership changes).

3. Vendor Selection

VRM must be present at the **front end** of the vendor lifecycle, not just after contracts are signed:

- **Embedding VRM into procurement** – integrating risk criteria and assessment steps into tendering, RFPs and competitive sourcing activities.
- **Selection decision support** – providing risk-based analysis alongside commercial and technical evaluations so that decision-makers see a complete picture.
- **Suitability and strategic fit** – assessing whether a vendor can realistically scale, adapt and support the client's medium-term needs, not just the immediate requirement.
- **Pre-contract due diligence** – completing critical VRM checks **before** contract execution to avoid being locked into high-risk relationships.

4. Contract Terms and Conditions

We ensure that contractual arrangements reflect the organisation's risk appetite and VRM requirements:

- **Standard VRM-aligned clauses** – defining baseline expectations for:
  - Data protection and privacy
  - Information security controls
  - Incident reporting and breach notification
  - Right to audit and assess
  - Business continuity and disaster recovery
  - Subcontractor management
  - Exit and transition obligations
- **Enterprise-level standards** – developing standard contract addenda or schedules that can be reused across multiple vendors to ensure consistency.
- **Risk-adjusted terms** – differentiating between critical and low-risk vendors so that contractual requirements remain proportionate.
- **Alignment with regulatory guidance** – ensuring key clauses support compliance (e.g. around outsourcing, cloud use, data processing).

5. Vendor Management

VRM does not stop once vendors are onboarded. We design frameworks that support ongoing relationship and performance management:

- **Relationship management structures** – defining relationship leads, engagement forums and escalation routes for key vendors.
- **Performance monitoring** – designing SLA/KPI frameworks, reporting dashboards and review cadences (e.g. monthly, quarterly).
- **Behavioural monitoring** – identifying patterns in behaviour, responsiveness, communication and cooperation that indicate risk.
- **Issue and incident handling** – integrating vendor-related incidents into risk registers, problem management and service management processes.
- **Remediation and improvement planning** – managing underperformance through corrective action plans, with clear timescales and consequences.

6. VRM Governance Frameworks

Governance makes VRM visible, accountable and sustainable:

- **VRM governance design** – defining governance forums, decision rights and escalation paths (e.g. VRM committee, risk committee alignment, executive reporting).
- **Cross-organisation touchpoints** – ensuring VRM has defined interfaces with IT, security, operations, procurement, commercial, legal, risk and finance.
- **Reporting and MI** – designing reports and risk dashboards that highlight key vendor risks, trends and issues in a way that decision-makers can use.
- **Policy and standards** – creating VRM policies, standards and guidance so expectations are clear across the organisation.

7. Vendor Exit

Vendor exit is a high-risk phase if not planned and managed correctly. We support:

- **Exit strategy definition** – establishing principles, criteria and playbooks for vendor exit and transition.
- **Service continuity planning** – ensuring that exiting a vendor does not create service outages or operational gaps.
- **Data and knowledge repatriation** – managing retrieval or secure destruction of data, documentation and knowledge held by the vendor.
- **Transition to new vendors or in-house** – coordinating roles, responsibilities, timelines and handover between outgoing and incoming arrangements.
- **Exit risk management** – identifying and mitigating risks such as data loss, dependency exposure, or failure to transfer knowledge.

Each of these areas can be provided as a discrete service or as part of a holistic VRM engagement delivered end to end.

Additional Areas of VRM Expertise

To strengthen organisational control and long-term capability, Bentley Moore Executive also supports several advanced VRM dimensions.

VRM Maturity Assessment

We provide structured assessments of your current VRM maturity to:

- **Baseline the current state** – understanding existing processes, governance, tools, assessments and controls.

- **Identify gaps and weaknesses** – highlighting areas where risk is unmanaged, processes are ad hoc, or responsibilities are unclear.
- **Map against good practice and regulatory expectations** – positioning your current approach against recognised standards.
- **Develop a maturity roadmap** – outlining practical steps to progress from initial or fragmented VRM towards a robust, embedded capability.

This gives the organisation a clear view of where it stands and what it will take to reach the desired maturity level.

VRM Operating Model Design

We design VRM operating models that are both **practical and sustainable**, covering:

- **Roles and responsibilities** – defining who is responsible, accountable, consulted and informed at each stage of the vendor lifecycle (e.g. VRM lead, risk function, procurement, IT, security, service owners). This ensures that VRM is not "everyone's job and no one's job", but is supported by clear ownership.
- **Process architecture** – mapping how VRM processes interact with procurement, IT change, service introduction, project governance, risk management and audit, so that vendor risk is considered wherever vendors are used or changed.
- **Governance forums** – establishing which committees or boards review vendor risk, approve high-risk arrangements and oversee remediation activities (e.g. VRM committee, operational risk committee, technology governance boards).
- **Performance measures** – defining metrics that indicate the effectiveness of VRM (e.g. percentage of critical vendors assessed, overdue assessments, number of high-risk findings, remediation timeliness, incident trends linked to vendors).
- **Capability and resourcing** – determining the skills, capacity and types of roles required to operate VRM on an ongoing basis (e.g. VRM analysts, risk specialists, commercial support, security input).

The aim is to design an operating model that **supports and enables** VRM activity, rather than creating theoretical structures that cannot be operated in practice.

VRM Tooling & Enablement

Where appropriate, we advise on and support the deployment of tooling to make VRM more efficient, transparent and repeatable:

- **Tooling assessment** – reviewing existing tools (e.g. spreadsheets, contract repositories, service management systems, GRC platforms) and identifying their suitability for VRM.
- **Requirements definition** – specifying what VRM tooling must support (e.g. vendor inventory, risk scoring, assessment workflows, document storage, reporting).
- **Tool selection and configuration** – advising on tools or platforms that align with your needs and helping configure them to reflect your VRM processes and operating model.

- **Dashboards and reporting** – designing visual views (e.g. heatmaps, risk status, vendor tiers, remediation status) that provide meaningful insight for management.

Cross-Functional Integration

Effective VRM does not sit in isolation. We help integrate VRM with:

- **Cyber security** – aligning vendor risk with security assessments and incident management.
- **Data protection and privacy** – ensuring vendors handling personal or sensitive data are managed in line with data protection obligations.
- **Risk & compliance** – ensuring vendor risks are included in enterprise risk registers and subject to appropriate oversight.
- **Procurement & commercial** – aligning contract terms, supplier selection and negotiation with VRM expectations.
- **IT & operations** – ensuring service owners and operational leads understand and manage their vendor-related risks.
- **Finance** – aligning VRM with financial exposure, cost control and budget planning.

This integration ensures VRM becomes part of how the organisation makes decisions and manages risk across all major functions.

Regulatory & Compliance Alignment

For regulated or high-scrutiny environments, we align VRM with:

- **Relevant regulatory expectations** (e.g. around outsourcing, cloud use, operational resilience).
- **Data protection legislation** (e.g. GDPR) for vendors processing or storing data.
- **Sector-specific guidance** where applicable (e.g. financial services, public sector).
- **Audit and assurance requirements** – ensuring VRM activities produce evidence suitable for internal and external audit.

Delivery Models

Our VRM services can be delivered through different engagement models:

- **Advisory engagements** – where we design the framework and support your teams to implement it.
- **End-to-end implementation** – where we lead the full design, implementation and embedding of VRM.
- **Targeted interventions** – focused on specific gaps (e.g. VRM governance, assessments, vendor exit, contract remediation).
- **Interim VRM function** – acting as an external VRM function while internal capability is built.
- **Hybrid models** – combining advisory, delivery and capability build to transfer knowledge into BAU.

About Bentley Moore Executive

Bentley Moore Executive is a London-based consulting firm specialising in Vendor Risk Management, governance, assurance and complex third-party landscapes.

We help organisations:

- Understand their vendor risk exposure
- Design and implement robust VRM frameworks
- Improve supplier performance and accountability
- Reduce risk, duplication and unmanaged complexity
- Embed VRM into BAU for long-term resilience

Contact Us

Should you wish to discuss any of your Vendor Risk Management requirements and how we can help you, you can contact us as follows:

0333 012 9079
info@bentleymoore.co.uk
www.bentleymoore.co.uk/services
www.linkedin.com/company/bentley-moore-executive

Our Services

Website Services

Scan Me

Contact Details

Jason

Dave