South Carolina Bar
Continuing Legal Education Division

2026 SC BAR CONVENTION

In-house Counsel Committee

"Navigating the Dual Role of In-house Counsel: Legal Gatekeeper and Business Partner"

Friday, January 23

SC Supreme Court Commission on CLE Course No. 260133

South Carolina Bar
Continuing Legal Education Division

Vendor Management-Safe Guarding Business Relationships

Mary E. A. Lucas
Barbara Wojtysiak

Vendor Management – Safeguarding Business Relationships

Bob O'Malley
Associate Counsel
REV Federal Credit Union
Mary E. A. Lucas
Acting General Counsel
Open Technology Fund

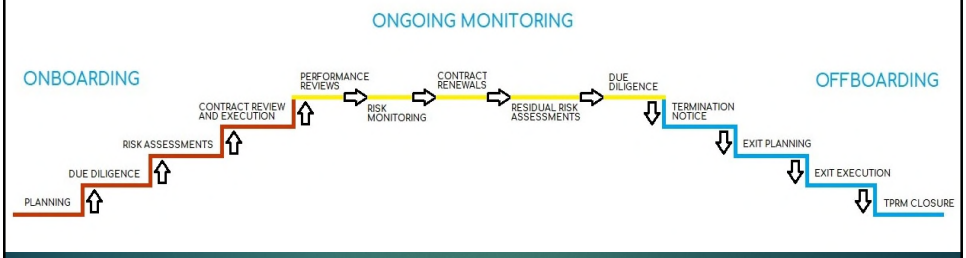
1

Vendor Management Overview

- • Oversight of third-party providers to ensure regulatory compliance.
- • Key functions: due diligence, risk assessment, contract negotiation, ongoing monitoring.
- • Regulators
- • Third-party risk ties directly to operational resilience.

2

Vendor Life Cycle



3

Regulatory Landscape

- • What are the regulators Third-Party Risk Management Guidance?
- • What are the regulators expectations for service provider oversight?
- • Are there data privacy standards?
- • Importance of documenting oversight programs.

4

Due Diligence

- • Financial stability review.
- • SOC 1/SOC 2 Type II reports.
- • Cybersecurity posture and InfoSec questionnaires.
- • BSA/AML obligations for certain vendors.
- • Insurance requirements: cyber, E&O, liability.
- Rely on your team/intuitions experts in these subjects (Don't go rouge)

5

Contract Review Essentials

- • Aligning legal terms with operational and regulatory risk.
- • Ensuring clarity on service levels, deliverables, and responsibilities.
- • Identifying and closing risk gaps before execution.

6

Confidentiality & Data Security

- • Protection of NPI (GLBA compliance).
- • Encryption, access controls, data segregation.
- • Subprocessor restrictions.
- • Breach notification timelines and cooperation duties.

7

Cybersecurity Requirements

- • Incident response obligations.
- • Vendor patching and vulnerability reporting.
- • Right to audit security controls.
- • Alignment with NIST and FFIEC CAT expectations.

8

Service Level Agreements (SLAs)

- • Uptime guarantees and performance metrics.
- • Reporting, monitoring, and credit/remedy structures.
- • Escalation paths for failures.

9

Business Continuity & Disaster Recovery

- • Vendor BCP testing requirements.
- • Recovery Time Objective (RTO) & Recovery Point Objective (RPO).
- • Evidence of annual testing.
- • Geographic redundancy.

10

Termination

- • Termination rights for cause and convenience.
- • Transition assistance and wind-down obligations.
- • Avoiding vendor lock-in.
- • Data return and destruction.

11

Indemnification

- • Vendor indemnity for data breaches, regulatory fines, IP infringement.
- • Survival periods and caps.
- • Relationship to insurance coverage.

12

Limitation of Liability

- • Caps based on contract value or insurance limits.
- • Carve-outs: confidentiality, gross negligence, willful misconduct.
- • Vendor attempts to exclude regulatory penalties—push back.

13

Choice of Venue & Governing Law

- • Preference for South Carolina law.
- • Risks of out-of-state jurisdictions.
- • Conflict-of-law considerations.

14

Dispute Resolution

- • Mediation → arbitration → litigation models.
- • Arbitration pros/cons.
- • Carve-outs for injunctive relief.

15

Ongoing Monitoring

- • Annual due diligence updates.
- • Performance monitoring and SLA scorecards.
- • Financial condition reviews.
- • Reportable events and change notifications.

16

Vendor Risk Tiering

- • Critical vs. non-critical vendor categories.
- • Risk rating methodology.
- • Oversight intensity tied to tier.

17

Exit Strategy & Contingency Planning

- • Moving to alternative vendors.
- • Data migration obligations.
- • Minimizing operational disruption.

18

Conclusion & Key Takeaways

- • Vendor management is a regulatory expectation and operational safeguard.
- • Contract terms must reflect risk.
- • Monitoring is as important as onboarding.
- • Questions?

19

Navigating the Dual Role of In-House Counsel: Legal Gatekeeper and Business Partner

Vendor Management

Mary E. A. Lucas, Esq.
Open Technology Fund

1

Why it Matters

- Vendors often hold access to company systems, proprietary data, sensitive data, and intellectual property;
- Regulations (and likely other contracts) require it;
- Vendor performance management;
- Protecting the organization from monetary and reputational risk; and
- Establishing and/or supporting a proper internal vendor management program (policies, procedures, personnel).

2

Vendor Risk Categories

- Data and network systems risks;
- Regulatory risks;
- Operational risks;
- Financial risks;
- Reputational risks;
- Ethical sourcing risks; and
- Performance risks.

3

Where to Begin

INVENTORY YOUR VENDORS;

LOOK FOR DUPLICATION OF SERVICES;

RISK PROFILES (WHAT DOES THE VENDOR HAVE THAT CAN CAUSE YOU RISK)—DOES YOUR ORGANIZATION EVEN KNOW;

WHAT LEGAL FRAMEWORKS APPLY (REGULATIONS RELATED TO PRIVACY, BANKING, ETC);

IS THERE INSURANCE COVERAGE;

WAS THE SECURITY POSTURE OF THE VENDOR VETTED; AND

WAS VENDOR DUE DILIGENCE CONDUCTED BEFORE PROCUREMENT AND IS IT ONGOING?

4

Prospective Vendor Management

Proper procurement and vetting

- Make sure all potential vendors have what you want before considering them
- RFP
- Sole Source
- Rolling applications
- Etc.

Due diligence

- Due diligence questionnaire
- Info. Sec. proof of audit compliance
- Regulatory compliance
- Subcontracting
- Insurance
- AI use
- SAM/OFAC/etc. checks
- Evaluate what "side" agreements may be required

Contracting

- Scope of services and SLAs (measurable standards)
- Data protection agreements
- Info. Sec. requirements including cybersecurity insurance
- Limitations of liability
- Indemnification (intellectual property, data breaches, regulatory violations)
- Confidentiality
- Audit and assessment rights
- Subcontractor restrictions and/or mandatory flow down provisions
- Termination rights

5

Data and Cybersecurity Contracting

- Data handling/processing, sharing, retention, portability, erasure;
- Notification of data breach timeliness;
- Encryption, access control, logging;
- On-premise and cloud security;
- Third-party assessments (SOC2, ISO 27001);
- Incident response cooperation provisions;
- Confidentiality (internally and externally);
- Cybersecurity insurance required;
- AI-specific safeguards (model training restrictions, transparency, data segregation, etc.).

6

IP Contracting

- Ownership of data, systems, trade secrets, etc. from the outset, ongoing, and in the end;
- Licensing scopes and restrictions;
- Deliverables and ownership thereof;
- Open-source usage requirements;
- AI-generated work considerations; and
- Infringement indemnity and defense obligations.

7

Ethical Sourcing Contracting

- Anti-bribery/anti-corruption provisions;
- Human rights/child labor restrictions;
- Sustainability disclosures;
- Diversity and inclusion commitments; and
- Vendor code of conduct acknowledgement.

8

Performance Management Contracting

- Vendor performance reviews;
- KPI reporting;
- SLA tracking and penalties (service credits, termination rights, etc.);
- Change management procedures; and
- Continuous improvement requirements.

9

Ongoing Contracting Management

- Who is responsible for overseeing vendor compliance with each requirement;
- Repeat due diligence;
- Annual assessments regarding performance, risk, insurance, changes to key stakeholders;
- Updates to contracts and controls;
- Monitoring subcontractors/subprocessors;
- Training staff/stakeholders management and escalation; and
- Incident response coordination.

10

Keep your eye on . . . :

- AI vendor oversight;
- Cyber insurance;
- Regulatory expansion;
- Supply chain resilience;
- Subcontracting;
- Automation; and
- Third-party assistance.

11

Common Issues

- Late legal involvement > Require intake questionnaires
- Incomplete vendor scoping > Standard vendor requirement checklist
- Negotiation delays > Pre-approved fallback provisions
- Lack of visibility into vendor program > Centralized vendor inventory/registry
- Exit strategies > Termination checklist

12

Best Practices

- Cross-functional alignment (Legal, IT, Compliance, Finance, Exec. Leadership)
- Training/Education
- Risk-based approach
- Standardize templates/contractual provisions
- Vendor inventory with automated notification annually to reassess
- Third party assessments, support, etc.
- Measured vendor performance tied to penalties/termination

13

Questions?

14

South Carolina Bar
Continuing Legal Education Division

The Legal-Decision vs. Business-Decision Dichotomy-Influence Strategic Direction

Abigail Miranda
Ashley Kelley

No Materials Available

South Carolina Bar

Continuing Legal Education Division

Litigation Management: Maximizing outcomes Through Effective Partnerships

Allison Raffety
Harriet O'Malley
&
Matthew Hamrick

Harriet O'Malley, Esq.

Associate at Womble Bond Dickinson

Matthew Hamrick, Esq.

Head of HR at Mercedes-Benz Vans, LLC

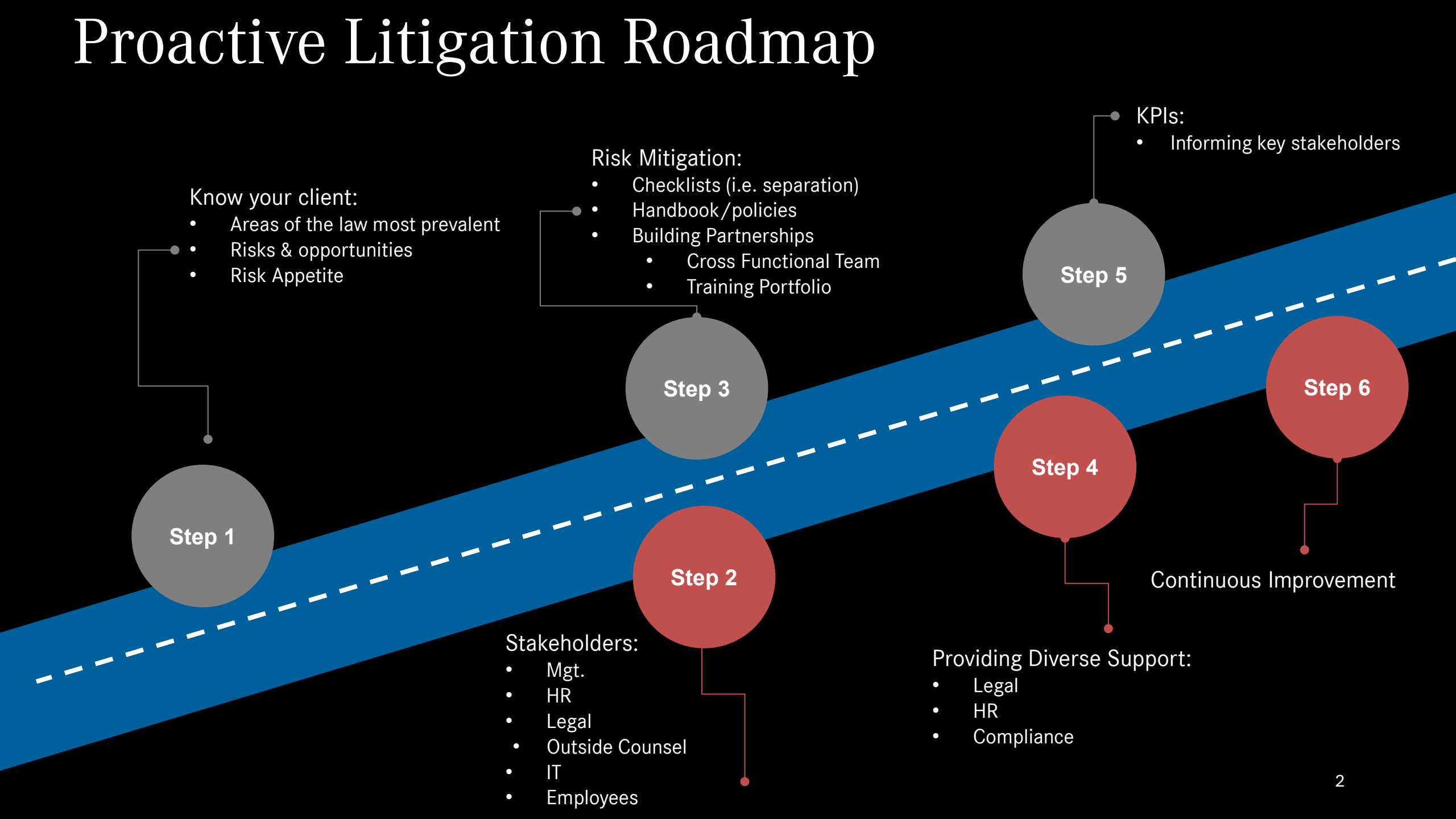
Alison Raffety, Esq.

Deputy General Counsel & Local Compliance Officer

Mercedes-Benz Vans, LLC

Litigation Management

Proactive Litigation Roadmap



Reactive Litigation Roadmap