Open Future Forum

OPEN FUTURE FORUM

General Counsel AI Report

NOVEMBER 2026

November 2026 | Legal and operating synthesis | Murray Newlands | Open Future Forum

Prepared 2 November 2026. Evidence cutoff: 31 October 2026, 23:59 America/Los_Angeles. This report examines the continuing validity of authorization as contracts and deployed workflows change. It is not a GC survey or a jurisdiction-specific legal opinion.

About this publication: Open Future Forum publishes research for executive and investor audiences. Murray Newlands is its founder. This report separates OFF survey observations, external research, author analysis and illustrative scenarios. Vendor-authored guidance is identified as such and does not constitute an independent product assessment. The collection and supporting methods are available through the OFF research index: https://openfutureforum.com/research/

4,334 substantive body words | 5,757 total words
Tables, FAQs, methods and references are excluded from the body count.

In this report

01 The decision in brief
02 Executive summary
03 What November adds
04 Evidence and sample boundaries
05 1. Describe the authorized act in business terms
06 2. Identify changes that invalidate the original assumptions
07 3. Connect contract allocation to observable performance
08 4. Keep the legal record useful and proportionate
09 5. Preserve evidence while containing the incident
10 6. Allocate responsibility across counsel, security and technology
11 External evidence and its limits
12 An illustrative contract-agent change review
13 The next legal and operating review
14 Questions for counsel
15 Citable facts
16 Methods and limitations
17 References
18 Related research and citation
19 Editable working tool

The decision in brief

Treat authorization as a bounded decision whose continuing validity depends on the deployed workflow and governing terms. Counsel should be able to connect permitted data, actions, recipients and oversight to the actual system, then identify which changes require renewed review. The legal record should support that comparison and preserve the evidence needed when an action or outcome is disputed.

Executive summary

A contract can remain unchanged while an AI workflow becomes materially different. A team may add a data source, broaden the agent's actions, remove a review step or send information to another service. Conversely, a supplier may change terms or service arrangements while the customer's technical configuration appears unchanged. The legal question is whether the original authorization still supports the current use, and who is responsible for recognizing a change that requires review.

The updated OFF security sample provides context for that question. Of 207 respondents, 142 selected agent identity, access and permissions as a priority, 52 data leakage, 49 shadow AI and 42 AI-powered attacks. The answers record selected concerns, not verified incidents or legal violations. In a separate carried-forward operator instrument, 18 of 49 applicable respondents selected shared service accounts. That architecture label alone does not establish illegality, ineffective control or privilege loss. [SEC; ACCESS_APPLICABLE]

The October GC report already introduced a material-agent legal record, contract checklist and incident evidence chain. November retains those tools and develops their change conditions. The contribution is a comparison between the authorized use and the deployed use, with a record of which assumptions have changed and what decision follows. A document approved at launch should not become a permanent assurance for a broader system.

This report assigns distinct work to counsel, security, technology and the business owner. Counsel assesses the relevant legal and contractual constraints. Security tests effective access and intervention. Technology explains the configuration and dependencies. The business owner defines the intended action, accepted outcome and operating consequence. Their judgments should meet in one decision record without implying that any one function can certify every aspect of the workflow.

A hypothetical customer-contract agent shows how the method applies when drafting assistance expands into sending offers and updating records. The example connects contract allocation, operational authority, review evidence and incident preservation. It makes no claim about a real company or a universal legal outcome.

Repeated legal review can slow ordinary product changes when the original approval lacks clear boundaries. The proposed response is to define the changes that matter to the authorized use and delegate routine changes within an agreed boundary. Counsel should focus on altered rights, obligations and consequences, with enough operational evidence to make that judgment accurately.

What November adds

The first addition is a validity condition for authorization. The legal record should identify the workflow, purpose, data classes, actions, recipients and oversight on which the decision relied. A change in one of those conditions can require a new assessment even if the system retains the same name. The report does not suggest that every software update requires a full legal review; it identifies the conditions that make the original decision relevant or insufficient.

The second addition is a contract-to-configuration reconciliation. A term restricting a particular data use must correspond to an operational arrangement that the responsible team can explain. A promise of human approval should identify the action reviewed and the point at which review occurs. A right to suspend service should be considered alongside the information and cooperation needed to exercise it. The recommendation is to test the relationship between a term and its implementation, not to assume that either document proves the other.

The third addition concerns evidence after a disputed action. The company needs to distinguish what was authorized, what the system could do, what it attempted, what actually happened and what a human reviewed. Those records may sit in different systems with different clocks and retention periods. November's incident chain identifies those distinctions and the responsible owners, while leaving legal preservation and disclosure decisions to counsel under the applicable facts and rules.

The updated security distribution provides new context. The operator access methods remain carried forward. The GC event roster does not supply a suitable new instrument measuring legal-team adoption, liability or contract practice, so no such benchmark is presented. The edition is a full synthesis with explicit data limits.

The report also avoids presenting private event anecdotes as verified case studies. An account of discovering many more agents than expected can suggest an inventory question, but without a verifiable source and permission it is not published here as a factual incident. The worked example is instead labelled as hypothetical from its introduction.

Evidence and sample boundaries

SEC has 207 eligible unique responses and permits multiple selections. The later security event adds 65 completed responses before overlap with the earlier source is resolved. The cumulative result is not a representative monthly incident rate, and selected concerns cannot establish that any respondent experienced a breach or violated an obligation.

ACCESS has 71 responses. Twenty-two selected not applicable yet, leaving an applicable base of 49. Eighteen selected shared service accounts and 24 per-agent credentials; the other applicable categories have small counts. The report does not infer effective permissions, identity attribution or legal compliance from those labels. Those questions require examination of the actual deployment.

The common buying instrument records 60 of 467 respondents selecting no single owner. It describes purchase ownership under the question's wording, not a determination of legal responsibility or a count of

companies without governance. It should not be used to identify a person liable for an agent's conduct. [SIGN]

External references are separated by type: ABA ethics guidance under Model Rules, a technical protocol specification, government security guidance, a voluntary risk framework and a specific SEC disclosure regime. They are not interchangeable sources of law. The proposed tools require adaptation to the relevant jurisdiction, contracts, professional responsibilities and company circumstances.

Exhibit 1. Security concerns and the legal questions they raise

Selection	Count and base	Question requiring deployment-specific evidence
Agent identity, access and permissions	142/207; 69%	Which person or process authorized the actual action?
Data leakage	52/207; 25%	What information moved, to whom, under which permitted use?
Shadow AI	49/207; 24%	Was the use authorized, and what facts establish its scope?
AI-powered attacks	42/207; 20%	What occurred, what evidence remains and which response obligations apply?
Nothing urgent yet	15/207; 7%	No inference of absence of exposure or effective controls

Exhibit note: SEC, updated cumulative; multiple selections. These are priorities, not observed events or legal findings. Exact question and observation windows are in Executive AI Statistics.

1. Describe the authorized act in business terms

Authorization should begin with the business act, not the model name. Preparing a draft, sending an offer, changing a customer record and initiating a payment have different consequences. A legal review that describes all of them as using an AI assistant may fail to identify the decision the organization is actually delegating. The business owner should explain the intended act, its recipient and the consequence of an error.

The record should distinguish access to information from permission to use it for a particular purpose. A system may be technically able to retrieve a document while the proposed use requires a separate contractual or legal assessment. Similarly, permission to generate a draft does not necessarily imply permission to communicate it externally or execute the proposed transaction. These distinctions should be described concretely enough for technology teams to implement the intended boundary.

Counsel should identify which source of authority governs each material condition. The source may be a contract, internal delegation, customer instruction, applicable law or professional duty. The record should not describe an internal preference as a legal requirement or assume that a supplier's standard terms answer

the customer's separate obligations. The relevant documents and facts need to be assessed in their proper roles.

An authorized act should also identify the actor responsible for the business decision. A model output can inform that decision without becoming the accountable party. Where an automated process performs the act, the company should identify who approved the scope and who can change it. This is a governance recommendation; the legal allocation of responsibility depends on the actual facts and applicable authority.

Human involvement should be described precisely. A person reviewing a sample after actions occur is providing a different control from a person approving each action before execution. Both can be useful in context. The legal record should state what the human sees, what they can change and whether they have time and authority to intervene. A generic human-in-the-loop label can conceal those differences.

The resulting authorization can be narrow and practical. It may permit drafting from specified sources, require approval before external transmission and prohibit certain changes without renewed review. That boundary should be usable by the teams operating the system. The purpose is to make the intended delegation clear enough that later changes can be assessed against it.

2. Identify changes that invalidate the original assumptions

A launch review is tied to a set of facts. Those facts can change through product development, supplier updates or business decisions. Counsel should work with the operating teams to identify which changes are relevant to the original authorization. The trigger should reflect the consequence, rather than treating every routine update as equivalent or relying on the product name to imply continuity.

Examples include adding a sensitive data source, expanding the recipient group, granting a new action, removing a review step or introducing a new service provider into the workflow. A change in customer terms or the supplier's permitted data use may also matter. The record should identify who monitors each relevant change and how it reaches the person authorized to reassess the use.

Technical and contractual changes can move independently. A supplier may alter a commercial or data-processing arrangement without requiring a visible application release. An internal team may change a tool's permissions without amending the supplier agreement. The review process should therefore draw on both contract management and operational change records. Neither is a complete substitute for the other.

The reassessment should be scoped to the change. If the authorized purpose and data remain the same but a minor interface changes, the existing legal analysis may remain applicable. If an agent gains authority to bind the company to new terms, the review is different. A clear trigger framework allows routine work to remain delegated while directing attention to changes that affect rights, obligations or material consequences.

The decision should record what remains valid and what has been renewed. It may preserve the existing authorization, add a condition, restrict the new scope or require another agreement. The record should also identify any temporary exception and when it ends. An exception without an accountable owner or review point can quietly become the normal operating state.

The company should test whether the process works with an actual change. Select a recent material modification and trace it from the operating record to the relevant contractual and legal assessment. If the change never reached the appropriate owner, the problem is a handoff that can be repaired. The goal is an effective review route, not a larger inventory of approvals that cannot be connected to deployed behavior.

3. Connect contract allocation to observable performance

Contract terms should address the service the parties expect to deliver and receive. For an AI workflow, that includes the permitted task, relevant data use, acceptance process and allocation of work when an output is wrong or an action is disputed. A broad warranty or disclaimer may be commercially important, but it does not explain how the parties will recognize and resolve an operating problem.

Usage pricing requires a defined billable event. The parties should understand whether retries, failed attempts, test activity or duplicate events create charges. Outcome pricing requires a definition of the accepted result and a process for disagreement. A fixed subscription can still require clarity about capacity, service scope and additional charges. These are contract-design questions prompted by the commercial model, not conclusions drawn from OFF's pricing percentages.

The agreement should distinguish a service promise from a technical control. A supplier may promise a capability that the customer must configure or operate. The customer may retain responsibility for its data, approval process or integration. The parties should identify those dependencies and the evidence each can provide. Otherwise, a problem can produce competing assertions that the other side failed to perform an undefined prerequisite.

Change provisions should connect to the authorized use. Relevant questions include how material service changes are communicated, what information is available about downstream providers and what happens if the changed service no longer fits the customer's requirements. The appropriate language depends on bargaining position, use case and applicable obligations. This report does not provide a universal clause or imply that every supplier will accept the same allocation.

Suspension and termination should be considered operationally. The customer may need access to records, export capability or limited cooperation to investigate and transition. The supplier may need a clear process for restricting dangerous use. Counsel should ask the operating team what information and service are necessary to exercise the negotiated rights. A right that cannot be used in practice may offer less protection than its wording suggests.

For legal work, professional responsibilities require separate attention. ABA Formal Opinion 512 addresses matters including competence, confidentiality, supervision and fees under the Model Rules. Its guidance is relevant to lawyers' use of generative AI, but it does not determine every corporate contract or replace jurisdiction-specific rules. Counsel should assess the actual professional context rather than treating a general enterprise procurement approval as sufficient for every legal task. [E-ABA512]

4. Keep the legal record useful and proportionate

A material-agent legal record should identify the authorization and the evidence needed to assess it. It should not become an indiscriminate copy of every prompt, output and customer document. Excessive collection can create unnecessary exposure and make relevant evidence harder to find. The responsible teams should agree what the record must establish and which source systems should retain the underlying material.

The record should distinguish identity from attribution. A credential can identify a service while leaving uncertainty about the human instruction, application decision or downstream action associated with an event. Conversely, a shared service account can operate within a system that retains useful attribution records. The access-method label alone does not answer the legal question. Counsel should ask what can actually be reconstructed for the act under review.

Version and timing information can be essential. The system's current configuration may differ from the configuration at the time of a disputed action. Logs from different services may use different clocks or identifiers. The operating record should preserve enough context to connect the relevant instruction, permission, action and result, with known limitations. An apparently precise timeline should not conceal uncertainty about synchronization or missing events.

Retention should be tied to applicable obligations and legitimate operating needs. Counsel should determine the appropriate preservation requirements and interaction with existing schedules for the relevant matter. This report does not prescribe one retention period. Nor does it assume that every record is privileged because a lawyer receives it or that using an AI tool automatically destroys privilege. Those questions require the actual facts and governing law.

Access to the record should reflect its sensitivity and purpose. Technical staff may need operational details that an investor or supplier does not. Counsel may need a preserved record for a specific matter without broadening access to unrelated information. The record should identify the custodian, permitted reviewers and process for authorized production. This supports use of the evidence while avoiding unnecessary duplication.

The useful test is whether an appropriate reviewer can answer the material question. Who authorized the action? What was the system permitted to do? What happened? What did a human review? Which contractual or legal condition is relevant? The record can be compact if those answers are traceable. A large archive with no reliable link between them provides less practical assurance.

5. Preserve evidence while containing the incident

An incident response may require immediate operational action before the full facts are known. Security and technology teams should be able to contain the relevant activity under the company's response arrangements. Counsel should work alongside them to identify preservation, notification and other obligations. The process should not assume that stopping a system and preserving evidence are mutually exclusive, though specific choices may involve tradeoffs that must be recorded.

The initial record should separate known facts from hypotheses. A customer complaint, a model message and a verified external action have different evidentiary weight. The team should identify the source of each assertion, the time it was recorded and what remains uncertain. This prevents an early explanation from becoming accepted fact merely because it appears in several internal updates.

Containment should be described in terms of its actual scope. Disabling one interface may leave queued work or downstream access active. The security team should explain what was stopped and what could continue. Counsel can then assess the relevant consequences and obligations using a more accurate account of the event. A general statement that the agent was turned off may be inadequate for that purpose.

The evidence chain should connect authorization, effective permissions, the initiating event, attempted actions, observed results, human intervention and subsequent changes. It should identify missing records and competing explanations. The company should avoid modifying an original record to make it fit a preferred chronology. Necessary operational changes should be recorded with their purpose and timing, with appropriate preservation directed by counsel.

Legal clocks require precision. For covered Form 8-K registrants, the SEC's Item 1.05 framework generally uses four business days after a determination of materiality for a material cybersecurity incident, subject to its provisions and exceptions. That is not a universal deadline from discovery and not a rule governing every AI error. The responsible legal team must assess applicability and other potentially relevant obligations. [E-SEC-CYBER]

The incident review should end with more than a technical fix. If the event shows that the deployed use exceeded its authorized scope, the legal record and change process should be updated. If the evidence remains incomplete, that limitation should affect the conclusions drawn. The company should distinguish restored service from a completed legal or factual assessment and assign responsibility for each remaining decision.

6. Allocate responsibility across counsel, security and technology

The business owner should define the purpose, expected result and consequence of failure. Without that information, legal and technical teams may review a generic system rather than the actual commitment. The owner should also identify who accepts the output and who decides whether the workflow remains useful. Those business decisions should be visible in the same record as the technical and legal boundaries.

Technology should explain the deployed configuration, service dependencies and changes. Security should assess effective access, monitoring and intervention within its remit. Counsel should evaluate relevant legal and contractual constraints and advise on evidence, preservation and disclosure questions. These roles can overlap in practice, but the record should make clear which assertion each function is responsible for supporting.

A cross-functional review should resolve disagreements explicitly. Security may show that a configuration is technically restricted while counsel identifies a contractual limitation on the intended data use. The business may consider a result acceptable while the customer contract defines acceptance differently. The decision

should address both issues rather than treat one approval as overriding the other without an accountable judgment.

Routine changes can be delegated within a documented boundary. The teams should agree which facts can change without reopening the entire review and which changes require escalation. This allows the process to remain usable as the product evolves. A policy that requires senior legal review for every minor release may be ignored; a policy that never reaches a material change provides little protection.

The record should identify who can authorize a temporary exception and what evidence is required to close it. An exception might permit a restricted pilot while a contract question is resolved, provided the scope is appropriate and the necessary decision-makers agree. The recommendation is to make the accepted uncertainty explicit. It is not a general legal endorsement of operating while an obligation remains unresolved.

The board or relevant committee should receive material decisions and unresolved consequences at the appropriate level. Directors do not need a full technical log, but management should be able to explain the authorized use, the change under consideration and the evidence supporting its recommendation. This connects the legal record to oversight without turning the GC into the sole owner of every AI operating decision.

Exhibit 2. Material-agent legal record with change conditions

Record field	Responsible contributor	Condition requiring review
Purpose, accepted outcome and business consequence	Business owner	New customer promise, task or recipient population
Permitted data and uses	Counsel with data and business owners	New source, purpose, recipient or relevant term
Authorized actions and review point	Business owner with counsel and security	Broader authority or changed human approval
Effective configuration and dependencies	Technology and security	New tool, credential path or downstream service
Contract allocation and billing event	Counsel with commercial and finance teams	Changed obligations, acceptance or charge calculation
Evidence, custodians and retention	Counsel with records and technical owners	New matter, preservation requirement or source limitation
Decision and exception expiry	Authorized executive	Condition breached, evidence expires or scope changes

Exhibit note: Proposed record extending October's tool. It is not a statement that these fields satisfy every legal obligation or that every change requires the same review.

External evidence and its limits

ABA Formal Opinion 512, issued in July 2024, addresses lawyers' generative-AI use through the Model Rules, including confidentiality and supervision. It is professional ethics guidance whose application depends on the relevant jurisdiction and circumstances. The report uses it to distinguish legal-service obligations from a general corporate software approval, not to pronounce a specific deployment compliant or unlawful. [E-ABA512]

The MCP authorization security considerations specify technical requirements within that protocol, including token audience validation and restrictions on token passthrough. Those requirements help explain why a recognizable credential label does not establish the effective authorization path. A protocol specification is not a legal allocation of agency, liability or contractual responsibility. The actual implementation also needs examination. [E-MCP]

CISA's May 2026 official announcement of joint agentic-AI guidance emphasizes constrained autonomy, identity management and oversight. This report relies on the accessible announcement, not a claim to have reviewed every provision of the linked full guidance. It supplies security context for the legal questions, rather than a new generally applicable law. [E-CISA]

NIST's voluntary AI Risk Management Framework offers a way to organize context, responsibilities and risk work. It can support a structured review but does not certify legal compliance. The current official page indicates revision work; this report does not describe an unverified new 2026 standard as binding authority. [E-NIST]

The SEC cybersecurity disclosure rule and current staff interpretations provide a specific example of why the event, determination and reporting deadline must be distinguished. The example applies within the relevant securities-law framework. Counsel must identify other obligations separately rather than use one familiar deadline as a universal incident rule. [E-SEC-CYBER]

The sources do different work. Ethics guidance informs lawyers' professional responsibilities; a protocol explains a technical boundary; agency guidance and a voluntary framework support risk analysis; the SEC rule creates specified disclosure requirements for covered entities. Combining them into a generic compliance checklist would obscure their scope. The legal record should identify the particular authority and fact relevant to each decision.

Counsel rarely controls all the facts needed for review. The response is a clear handoff to the function that can produce the evidence, with a decision about what may proceed while uncertainty remains. A legal team should be able to qualify its advice to the stated operating facts and identify the changes that would require reconsideration. That is more useful than a broad approval detached from the deployed system.

For a changed contract agent, counsel should first identify the new action and the organization on whose behalf it occurs. Technical owners can then demonstrate the permission path, commercial owners can explain the customer promise, and counsel can assess the relevant legal instrument. If those facts remain uncertain, the advice can be limited to a narrower operating scope with a stated condition for reconsideration. None of the cited sources supplies that factual record. Their value is to clarify the question

being asked and the authority relevant to it, so that a technical control, an ethics obligation and a contractual allocation do not become interchangeable assurances.

Evidence comparison

Source	Contribution to this decision	Limit on interpretation
ABA Opinion 512 [E-ABA512]	Lawyers' confidentiality and supervision duties	Model Rules guidance; jurisdiction and facts govern application
MCP specification [E-MCP]	Protocol authorization requirements	Technical specification does not allocate legal liability
CISA announcement [E-CISA]	Constrained autonomy and oversight context	Announcement reviewed; full linked guidance not claimed
NIST [E-NIST]	Organizes risk context and responsibilities	Voluntary; no legal certification
SEC rule [E-SEC-CYBER]	Specified incident disclosure requirements	Covered entities and materiality determination; exceptions apply

An illustrative contract-agent change review

Consider a hypothetical company using an agent to prepare customer-contract responses. Its initial authorization permits drafting from approved templates and specified customer records. An employee reviews and sends the response. The product team proposes adding two capabilities: sending a standard offer directly and updating the customer-management system after acceptance. Those capabilities change the business acts and the evidence required, even if the product keeps the same name.

The business owner first defines the proposed offer, eligible customers and consequences of an incorrect communication. Counsel reviews the relevant commercial terms and internal authority. Technology explains how the agent selects the template, identifies the recipient and records acceptance. Security examines the effective permissions and intervention route. The review should address the actual proposed actions, rather than simply confirm that the original drafting tool was approved.

The teams then compare the intended boundary with the deployed configuration. If the integration permits broader changes than the authorized offer workflow, the discrepancy requires resolution. If the contract requires employee approval before an offer is sent, a later sample review does not implement that condition. The relevant response may be a configuration change, a revised process or a new business and legal decision under the applicable facts.

Exhibit 3. Contract-clause review linked to operating evidence

Contract subject	Operating evidence to request	Question for counsel and the business owner
Permitted purpose and data use	Actual sources, recipients and service path	Does the deployed use fit the agreed scope?
Acceptance and outcome	External result and customer-review record	What event resolves completion and any dispute?
Usage charges and credits	Eligible-event rules and reconciliation	Are retries, tests and failed actions treated as agreed?
Changes and downstream providers	Change notices and dependency record	Which changes require notice, consent or reassessment under the actual terms?
Suspension, termination and transition	Effective intervention and export capability	Can the negotiated right be exercised with available evidence and cooperation?
Incident cooperation and records	Custodians, access and preservation route	What can each party provide, and on what terms?

Exhibit note: Proposed review questions, not model legal clauses. The appropriate terms and obligations depend on the actual agreement and governing law.

Suppose a customer later disputes an offer attributed to the agent. The company should avoid assuming that the agent's final message establishes what was sent or accepted. The response team needs the authorized template and limits, the configuration at the relevant time, the initiating instruction, the outbound communication, the customer response and the subsequent record change. If some evidence is unavailable, the limitation should remain visible in the factual assessment.

Incident evidence chain for the hypothetical workflow

Evidence stage	Question answered	Likely custodian
Authorization and governing terms	What was permitted at the time?	Business owner and counsel
Configuration and effective permissions	What could the system actually do?	Technology and security
Initiating event and attempted action	What caused the workflow to act?	Application owner
External communication and state	What was sent, accepted or changed?	Relevant business system owner
Human intervention and containment	Who reviewed or changed the course of events?	Operating and incident teams
Preservation and subsequent decisions	What was retained, changed or concluded?	Counsel and designated custodians

Exhibit note: Proposed evidence chain. Preserve original records and known timing limitations under the company's applicable process; no universal legal conclusion follows from the presence or absence of one field.

The company may contain the sending capability while leaving drafting available, if that response fits the facts and its authorized operating process. It should record the actual scope of containment and verify what downstream activity can continue. Counsel then assesses the relevant obligations from the available facts, while the operating team determines what is required to restore an acceptable service.

The final review should update the authorization record. It should identify whether the original boundary was adequate, whether the configuration departed from it and whether the evidence process supported a reliable reconstruction. The useful result is a clearer decision about the workflow and its conditions. A new contract clause alone would not resolve a configuration problem, and a technical fix alone would not answer every contractual or legal question.

The next legal and operating review

Select one material workflow that has changed since its last review. Compare the current purpose, data, actions, recipients and oversight with the facts on which the earlier authorization relied. Ask the business and technical owners to explain the differences. Counsel can then identify which differences affect the relevant rights and obligations and what decision is required.

Use that review to test the handoff, not just the document. Could the company detect the change, obtain the necessary facts and route the decision to the right person? Could it reconstruct a disputed action without relying on a model's account of its own behavior? If the answer is uncertain, assign a specific repair with a defined owner and closure condition.

November's recommendation is to keep the legal record connected to the system as it actually operates. Authorization, contract allocation and evidence should be reviewed together when the relevant facts change.

That gives counsel a sounder basis for advice and gives the business a clearer boundary within which it can continue to develop and use the workflow.

Questions for counsel

Is this a survey of general counsel?

No. The report is a legal and operating synthesis informed by separate OFF instruments and identified primary sources.

Does a shared service account establish illegality?

No. The access-method answer does not establish effective permissions, attribution, legal duties or a violation. [ACCESS_APPLICABLE]

Does a security concern prove that an incident occurred?

No. SEC records selected priorities and concerns, not verified events.

Is ABA Formal Opinion 512 a universal corporate AI law?

No. It is professional ethics guidance addressing lawyers' use of generative AI through the Model Rules. Jurisdiction and circumstances matter. [E-ABA512]

Does every change require a complete new legal review?

No. The proposed approach identifies changes material to the authorized use and delegates routine changes within an agreed boundary.

Does sending a record to counsel automatically make it privileged?

No such conclusion is made. Privilege, preservation and production questions require the actual facts and applicable law.

Is the SEC deadline four business days from discovering any AI error?

No. The cited regime concerns material cybersecurity incidents for covered registrants and generally measures from the materiality determination, subject to its provisions. [E-SEC-CYBER]

Citable facts

- Agent identity, access and permissions: 142/207, 69%, updated security sample. [SEC]

- Shared service accounts: 18/49 applicable responses, 37%; 22 of 71 total responses were not applicable yet. [ACCESS_APPLICABLE]

- No single buying owner selected: 60/467, 13%; not a legal-responsibility finding. [SIGN]

Methods and limitations

Calculation-v1.1 excludes byte-identical exports and invited-only records and selects the latest eligible nonblank response per normalized respondent identifier per question. Security is updated cumulative; access and buying ownership are carried forward. Question bases, multiple-selection status and applicable exclusions are preserved.

The samples are selective and self-reported. No legal violation, liability outcome, privilege loss, incident rate or GC adoption benchmark is inferred. External sources have distinct legal, technical and advisory scopes. The contract-agent example and working tools are original recommendations requiring adaptation to actual facts, contracts and jurisdictions.

References

[OFF-DATA] Open Future Forum. Executive AI Statistics, November 2026. SEC, ACCESS, ACCESS_APPLICABLE and SIGN.

[E-ABA512] American Bar Association, Standing Committee on Ethics and Professional Responsibility. Formal Opinion 512, Generative Artificial Intelligence Tools. 29 July 2024. https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/ethics-opinions/aba-formal-opinion-512.pdf

[E-MCP] Model Context Protocol. Authorization Security Considerations, specification 2026-07-28. https://github.com/modelcontextprotocol/modelcontextprotocol/blob/main/docs/specification/2026-07-28/basic/authorization/security-considerations.mdx

[E-CISA] CISA and partners. Official announcement of Careful Adoption of Agentic Artificial Intelligence Services. 1 May 2026. https://content.govdelivery.com/accounts/USDHSCISA/bulletins/41544ff

[E-NIST] NIST. AI Risk Management Framework 1.0, current official resource page. https://airc.nist.gov/airmf-resources/airmf/

[E-SEC-CYBER] US Securities and Exchange Commission. Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, final rule, 26 July 2023; current Form 8-K staff interpretations consulted 2 November 2026. https://www.sec.gov/files/rules/final/2023/33-11216.pdf and https://www.sec.gov/rules-regulations/staff-guidance/corporation-finance-interpretations-cfis/exchange-act-form-8-k

[OFF-PRIOR] Open Future Forum. General Counsel AI Report, October 2026. https://openfutureforum.com/research/dealmakers/general-counsel-october-2026

Related research and citation

The November CISO report examines effective authority and revocation, AI Leaders addresses release evidence, Board considers material oversight decisions, and Investment Banking follows commercial claims through revenue and disclosure review.

Suggested citation: Newlands, Murray. General Counsel AI Report, November 2026, Legal and Operating Synthesis. Open Future Forum. Evidence cutoff 31 October 2026.

Open Future Forum research: https://openfutureforum.com/research/

Editable working tool

Legal approval validity record: download the editable CSV worksheet. The worksheet implements the report's recommendation; it is not a validated score, mandatory standard or completed assessment.