MINISTRY OF LAW
SINGAPORE

2026

Guide for Using Generative AI in the Legal Sector

PUBLISHED ON 06 MAR 2026

Contents

1. Introduction 2

1.1. Purpose 2

1.2. Scope and Applicability 2

1.3. Definition and Core Concepts 3

2. Evolution of AI in Legal Practice and the Rise of GenAI 4

2.1. Examples of AI (including GenAI) Use Cases in the Legal Sector 6

3. Key Principles for Use of GenAI in Legal Work 13

3.1. Professional Ethics 13

Why is this important? 13

What should legal professionals do? 14

3.2. Confidentiality 18

Why is this important? 18

What should legal professionals do? 18

3.3. Transparency 21

Why is this important? 21

What should legal professionals do? 22

4. Implementing GenAI in Legal Practice 23

4.1. Step 1: Develop an AI adoption framework 23

4.2. Step 2: Diagnose and analyse needs 25

4.3. Step 3: Identify and evaluate GenAI tools 26

4.4. Step 4: Implementation and training 27

4.5. Step 5: Continuous review and improvement 30

Annexes 32

List of Contributors 48

1. Introduction

1.1. Purpose

1 The Ministry of Law ("**MinLaw**") is publishing this Guide for Using Generative AI in the Legal Sector ("**Guide**"), which will be updated as necessary, to set out general principles and good practices to encourage responsible, ethical, and effective use of generative artificial intelligence ("**GenAI**") in Singapore's legal services sector. The Guide aims to support the legal services sector in harnessing the potential of GenAI, while being mindful of professional obligations in the delivery of legal services.

2 This Guide builds on the Model AI Governance Framework for GenAI,[1] released by the Infocomm Media Development Authority ("**IMDA**") and the AI Verify Foundation, and complements the Singapore Courts' Guide on the Use of Generative Artificial Intelligence by Court Users.[2] It is also aligned with the National AI Strategy 2.0, which calls for sector-specific interventions that address distinct risks and considerations across use cases.[3]

1.2. Scope and Applicability

3 This Guide is intended for use by anyone handling legal work in Singapore, including legal professionals (i.e. lawyers in private practice, and in-house counsel), allied legal professionals (i.e. paralegals, legal secretaries, legal technologists, and legal project managers in private practice and in-house legal teams), alternative legal service providers, law students, and anyone providing GenAI tools for the legal sector, among others.

4 This Guide is non-binding. It serves as a reference for (a) the deployment and use of GenAI in carrying out legal work, and (b) the development of GenAI tools for legal work, whether for own use or for use by others. Where product names are specified, they are strictly for illustrative purposes and **do not** constitute any endorsement of said products, or the organisations which own or have developed them.

---

[1] Infocomm Media Development Authority ("**IMDA**"), "Model AI Governance Framework for Generative AI, Fostering a Trusted Ecosystem" (30 May 2024)

[2] Supreme Court of the Republic of Singapore, Registrar's Circular No. 1 of 2024, "Issue of the Guide on the Use of Generative Artificial Intelligence Tools by Court Users" (23 September 2024); State Courts of the Republic of Singapore, Registrar's Circular No. 9 of 2024, "Issue of the Guide on the Use of Generative Artificial Intelligence Tools by Court Users" (23 September 2024); and Family Justice Courts of the Republic of Singapore, Registrar's Circular No. 1 of 2024, "Issue of the Guide on the Use of Generative Artificial Intelligence Tools by Court Users" (23 September 2024)

[3] Ministry of Communications and Information and Smart Nation Singapore, "National AI Strategy 2.0: Singapore National AI Strategy" (4 December 2023) at Action 13

1.3. Definition and Core Concepts

What is AI?

5 The Organisation for Economic Co-operation and Development ("**OECD**") defines an Artificial Intelligence ("**AI**") system as:

> "a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment."[4]

6 In simple terms, AI systems process input (such as data, text, or images) to produce useful output. Early AI systems were rule-based, following pre-programmed instructions to perform specific tasks. The advent of machine learning enabled systems to learn patterns from historical data and apply them to new information to make predictions and decisions. Deep learning advanced this further through sophisticated neural networks that mimic aspects of the human brain, achieving breakthroughs in complex tasks like image recognition and natural language processing.

7 **GenAI** marks a new frontier. Unlike traditional AI, which classifies data and recognises patterns to make predictions or decisions, GenAI systems create entirely new content. These systems are trained on extensive datasets, known as **training data**, which can include various forms such as text, images, audio, and video. By identifying and applying patterns learned from this data, GenAI generates original outputs such as text, images, audio, video, and even code, in response to user prompts (or "**input**") [5]. Generally, traditional AI systems are deterministic (same input, same output), while GenAI systems are probabilistic, often generating different outputs in response to the same input. User input may also be used to further train and refine the GenAI model.

8 Large Language Models ("**LLMs**") are a prominent type of GenAI specialising in text generation. Trained on vast textual datasets, LLMs predict and generate text responses based on the given context. While their output can appear coherent and persuasive, LLMs

[4] Organisation for Economic Co-operation and Development's (OECD) definition of an "AI System" as of 3 May 2024.
[5] IMDA, "Generative AI: Implications for Trust and Governance" (2023)

do not in fact understand the meaning of the words they use or generate. Instead, they rely on statistical patterns to produce likely word sequences. As a result, outputs may be inaccurate, fictitious, or misleading (such as when errors are interspersed with factual information). Such errors are broadly referred to as "**hallucination**".[6] Nonetheless, with continual technology advancement, the capabilities, limitations, and risk profiles of GenAI tools, including LLMs, are likely to evolve and improve over time.

2. Evolution of AI in Legal Practice and the Rise of GenAI

9 AI is already transforming the way legal professionals work, and will continue to do so. Globally, many law practices and in-house counsel teams are increasingly adopting legal technology ("**legaltech**") tools.[7] These tools, alongside general technologies such as word processing, communication platforms and collaboration workspaces, support functions like practice management, document and knowledge management, legal research, document review, and contract review and analysis (see Section 2.1).

10 Advancements in machine learning, increased computational power, and access to vast datasets have propelled legaltech beyond basic rule-based applications, such as voice-to-text transcription, to sophisticated GenAI-powered systems capable of analysing and creating new content. Modern GenAI systems can now analyse complex documents, respond to natural language queries, synthesise information from multiple sources into clear summaries, and draft documents across different formats.

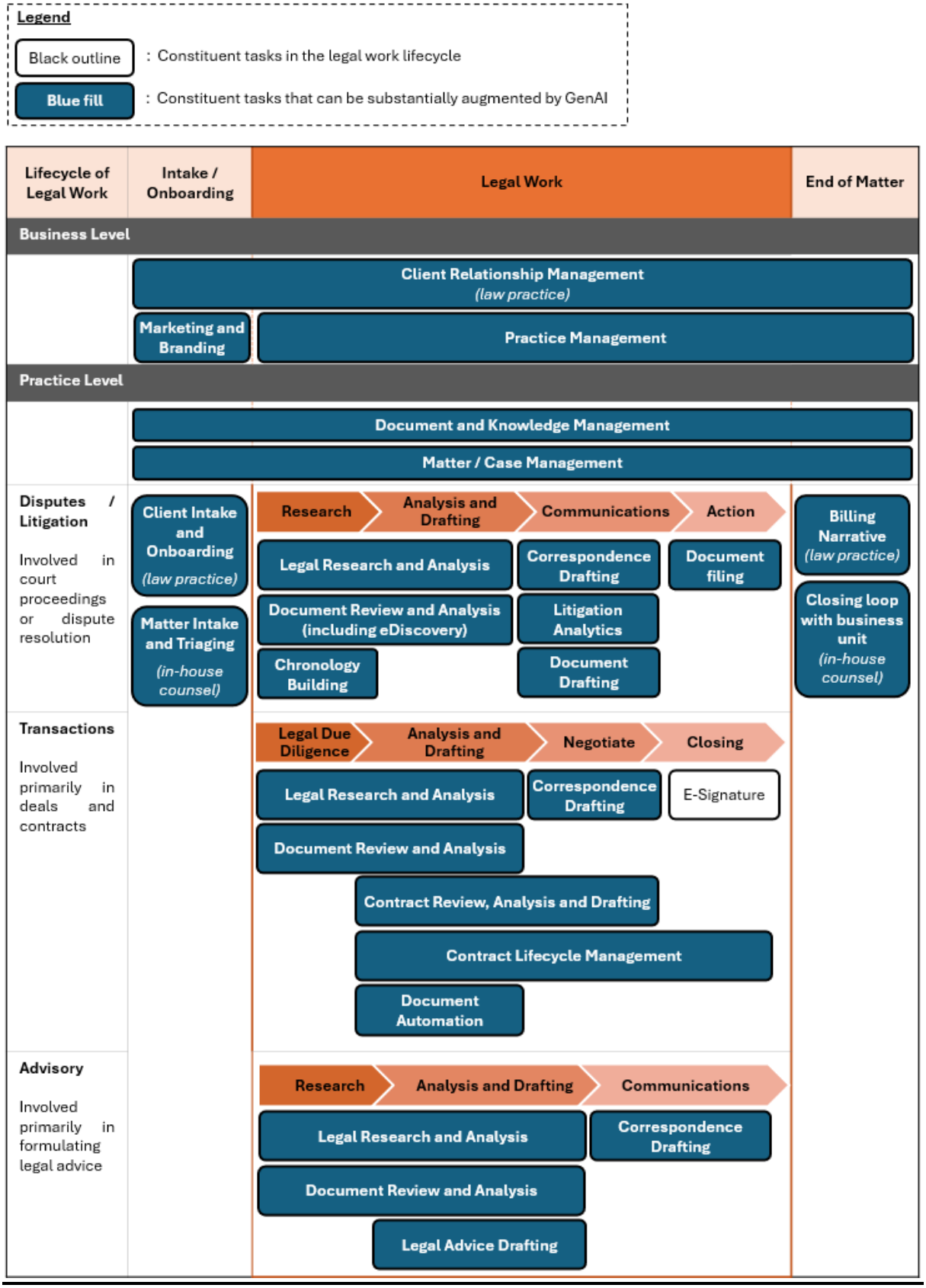
11 This evolution is transforming core legal work processes, from document review and drafting to legal research and client communication. **Diagram 1** illustrates the typical legal work lifecycle across practice areas. GenAI can augment most, if not all, essential tasks, ranging from routine tasks, such as preparing first drafts for client responses and summarising lengthy documents, to supporting more complex tasks like legal research and contract review. This enables legal professionals to devote more time to strategic analysis, advisory work, and other tasks requiring human judgement and expertise.

Note: *Diagram 1 provides a general overview and is not intended to be exhaustive in depicting how GenAI capabilities can augment legal practice.*

[6] Ibid.

[7] Legal technology ("Legaltech") tools refer to technology solutions designed to support or augment traditional methods of delivering legal services

Diagram 1: Mapping of GenAI use cases in a lifecycle of legal work



2.1. Examples of AI (including GenAI) in the Legal Sector: Use Cases, Key Considerations, and Practical Safeguards

12 This section provides practical examples of how AI, including GenAI, is applied in legal practice. **Table 1** illustrates common AI use cases in the legal sector. **Table 2** highlights key considerations that apply across all AI tools used for legal work, and the corresponding practical safeguards to ensure safe and responsible adoption. These are not intended to be exhaustive, and additional considerations may apply depending on specific circumstances.

Table 1: Examples of AI and GenAI Use Cases in the Legal Sector

Type of tool	Common features	Use cases
Practice management, and matter / case management	• Auto-scheduling and calendar reminders • Time tracking for time spent on tasks and matters • Dashboards for client/matter data • Automated billing and reporting • Workflow automation for routine administrative processes	**Law practice** • Organise client information, coordinate schedules, and monitor deadlines • Generate billing narrative, billing statements, and reports on client activities • Create matter overviews and client updates • Automate routine administrative tasks (e.g. opening new matters, sending client updates, etc.) **In-house counsel** • Track and prioritise legal requests and deadlines across multiple business units • Manage intake and triage legal requests from business units,

		assign tasks, monitor progress and track follow-up with business units
Contract lifecycle management	• Centralised repository for storing and managing contracts • Automated contract drafting using templates and clause libraries • Workflow automation for approvals and execution • Tracking of key dates, obligations, and renewal deadlines • Integration with e-signature platforms	**In-house counsel** • Manage end-to-end contract processes from drafting to execution • Ensure compliance with organisational policies and regulatory requirements • Track obligations and renewal dates across multiple business units • Generate reports for management on contract performance and risk exposure
Legal research (cases, statutes, changes in regulations)	• Plain-language search of legal databases • Jurisdiction or topic filter to find relevant cases, statutes, and legal materials • Interactive chatbot to refine research parameters • Summarisation of lengthy legal texts and synthesise information from multiple sources	**Law practice** • Identify and synthesise relevant case precedents, statutes, and trends to prepare case strategy • Draft research memos and litigation brief **In-house counsel** • Advise business units on regulatory changes affecting operations • Scan horizon, monitor and summarise global legal developments for business units for their operations, transactions and compliance
Document review	• Bulk ingestion and sorting of documents	**Law practice**

	• Extraction of key information and organise into structured formats (e.g. table, lists) • Timeline of events from document data • Prediction and flagging of important and relevant documents based on legal issues, including explanation of why documents were flagged • Generate summary reports of key findings	• Conduct e-discovery for litigation • Conduct forensic report analysis for criminal proceedings • Conduct due diligence for transactions • Build case chronology **In-house counsel** • Review internal records, flag discrepancies and identify material facts, e.g. in internal investigation cases • Review cases or documents against company policies • Flag and escalate potential compliance breaches • Summarise findings for reporting
Contract analysis and review	• Contract review against standard templates and company playbooks[8] to highlight deviations • Search and compare across contract libraries (clause library mining) • Track contract deadlines and obligations • Flag potential risks based on customisable risk preferences	**Law practice** • Support negotiations by quickly identifying non-standard clauses and suggesting fallback positions • Review high-volume contracts for merger and acquisition or financing deals • Advise clients on risk exposure in complex agreements • Ensure consistency across multiple inter-linked contracts, e.g.

[8] A manual that describes a company's policies, workflows, and procedures.

	• Suggest edits and generate tracked changes (redlines) • Answers specific queries on contract terms, with references • Explains complex contract language in simple terms	in a complex transaction **In-house counsel** • Ensure consistency and compliance in vendor / customer contracts across business units • Identify clauses that need to be reviewed or amended in light of new regulation or company policies • Support business negotiations (negotiation assistants tied to playbooks) • Track renewal dates and obligations, sending automated reminders • Support in responding to business queries about contract terms and risk implications
Document drafting	• Clause libraries and precedents • Auto-populate standard templates with details of the client, business unit or matter and allow customisation • Checks legal formatting standards, grammar, and cross-references • Drafts documents based on specific requirements in user prompts • Adjusts tone and writing style to fit the context • Suggests improvements and alternative phrasing	**Law practice** • Generate first drafts of pleadings tailored to jurisdiction, case type and client profile • Customise contracts for international transactions, ensuring local compliance • Suggest alternative clauses for negotiation and risk mitigation **In-house counsel** • Draft internal policies and board papers • Draft documents for business units, such as Master Services Agreements, non-disclosure agreements, employment

	• Learns and applies preferred drafting conventions from precedents • Supports drafting and translating in multiple languages	contracts, etc. • Translate documents in multiple languages for cross-border matters

Table 2: Key Considerations and Practical Safeguards

Key Consideration	Most relevant use cases	Practical safeguards
System integration and compatibility: Seamless integration with existing platforms (e.g. calendar, billing systems, and document processing) can reduce workflow disruptions and/or data inconsistencies.	• Practice management • Matter / case management • Contract lifecycle management	• Assess system compatibility before deployment. • Establish clear workflows and conduct staff training on proper use. • Regularly monitor automated processes to maintain system performance and reliability.
Data governance and confidentiality: AI tools may process confidential or sensitive information (e.g. individual / company data, financial records, proprietary content). If stored or used for model training, data could be leaked or reproduced in future GenAI output to unintended persons.	All use cases	• Review provider's terms of use, privacy, and data handling policies to ensure sufficient safeguards for confidentiality. ***For example,*** ensure the GenAI tool provider (a) offers opt-out options, or (b) provides legally binding commitments, that they will not log, store, nor retain input and output data for any purpose, including content monitoring or model improvement. • Implement data access controls and apply sensitivity labels, restricting GenAI access to use only the information each user is authorised to view based on their role and responsibilities. ***For example,*** when using Microsoft 365 Copilot, block search

		indexing on sensitive SharePoint sites, apply sensitivity labels like "Confidential" to restrict document access, and use Microsoft's Restricted SharePoint Search to block access to sites with confidential client information. • Train staff on usage protocols, including anonymising data and removing confidential or sensitive information before input, especially when using free-to-use GenAI tools.
Accuracy and reliability: Consider the degree of accuracy and ability to detect hallucination in legal content, including incorrect legal principles, unsupported conclusions, or made-up legal authorities.	• Legal research • Document drafting • Contract review and analysis	• Ensure appropriate human verification by personnel with requisite expertise. • Verify that sources are authoritative, and cases remain good law in the relevant jurisdiction. • Use GenAI tools that provide source citations or include instructions in prompts for generated output to include source citations, if possible, to facilitate fact- and source-checking. • Check completeness of analysis, i.e. whether it comprehensively covers all aspects, including complex contractual nuances, unusual clauses, or jurisdiction-specific requirements. • Craft precise prompts, including specifications on jurisdiction, time-period and source requirements. • Develop prompting capabilities by training staff in prompt engineering and creating internal prompt libraries for common legal tasks. This promotes consistency and improves output quality, which is often dependent on prompt quality.

Auditability and transparency: Maintaining version histories and approval trails ensures compliance and accountability during internal and external audits.	• Contract lifecycle management	• Configure systems to maintain version histories and approval logs. • Implement structured workflows for contract creation and approval. • Conduct regular audits to verify completeness and compliance.
Intellectual property and copyright: Consider copyright implications arising from the use of GenAI, such as potential infringement of third-party intellectual property, lack of copyright protection or ownership of AI-generated work. [9]	• Legal research • Document drafting	• Do not prompt GenAI tools to reproduce third-party content. • Consider using a plagiarism detection tool for written content, or reverse image search for visual content, to check if third-party content has been reproduced whether in part or in entirety. • Review terms of use to (a) confirm permitted uses, and whether users are indemnified against potential infringement (including conditions for indemnification); and (b) ensure that copyright of GenAI output is not owned by the provider.

[9] See also the explainers on AI and Copyright issued by IPOS under "Other resources: Artificial Intelligence" at ipos.gov.sg/about-ip/copyright/copyright-resources

3. Key Principles for Use of GenAI in Legal Work

13 As illustrated in **Table 1**, GenAI offers significant opportunities to enhance legal workflows. At the same time, legal professionals must uphold their professional duties and standards, being mindful of the key considerations when using GenAI and implement appropriate safeguards. This section sets out the key principles and practical steps legal professionals should take when using GenAI in legal work.

3.1. Professional Ethics

Why is this important?

14 Professionals and organisations are ultimately responsible for the quality and integrity of their work product, and for compliance with applicable professional and ethical duties. While enterprise technology providers are responsible for offering solutions with security features, data privacy protections, and foundational integrity, users bear the ultimate responsibility of exercising sound judgement in selecting appropriate tools that align with their requirements and support compliance with their obligations.[10]

15 Under the Legal Profession Act 1966 ("**LPA**"), lawyers are responsible for their work product, and must have the requisite knowledge, skill and experience to provide competent advice and representation. While GenAI offers powerful capabilities to assist legal work, it comes with inherent limitations, and the professional responsibility must appropriately rest with lawyers who can apply their expertise to guide and validate GenAI outputs. GenAI should therefore be used in ways that uphold and strengthen professional competency, keeping core legal skills and independent judgment central to legal practice. Legal professionals should use these tools thoughtfully to enhance the quality of legal practice and support the development of junior lawyers as competent practitioners.

16 **Hallucinations** are a key issue with GenAI systems.[11] Although GenAI systems may appear capable of analysis and reasoning, they do not truly "think", or understand meaning. Instead, output is generated by predicting word sequences based on statistical patterns.

---

[10] See also Google Cloud, "Shared responsibilities and shared fate on Google Cloud" (21 Aug 2023) for a useful example of the shared responsibilities between the provider and user. While the framework addresses cloud solutions, the underlying principles are applicable to GenAI solutions

[11] See also IMDA, "Starter Kit for Safety Testing of LLM-Based Applications: Building a Trusted Secure and Reliable AI Ecosystem, Draft for Public Consultation (28 May to 25 Jun 2025)" (2025) at p 32. Broadly, hallucination refers to output that is incorrect, which can manifest in different forms, primarily through factual inaccuracy, lack of grounding or incompleteness.

Hallucination cannot be completely eliminated, but its **likelihood** can be significantly **minimised** through practical techniques such as grounding, which includes providing sample documents as part of user prompts, or more systematic approaches like retrieval-augmented generation (known as RAG).[12,13]

17 **Bias** is another inherent consideration in GenAI tools, as with other AI systems, requiring careful human oversight in legal practice. Bias can arise from factors, such as:

(a) Training data that reflect historical prejudices or unrepresentative samples (e.g. case law or precedent that disproportionately disadvantage or favour certain groups);

(b) Algorithmic design choices (e.g. reliance on non-causal relationships where variables are correlated but not causally linked) may skew legal reasoning or recommendations; and

(c) Feedback loops where biased outputs influence future training, potentially reinforcing discriminatory patterns in legal analysis or client profiling.

These factors can compound, resulting in GenAI systems that perpetuate discrimination or systematically disadvantage specific client groups, case types or legal scenarios.

What should legal professionals do?

18 Rule 5 of the Legal Profession (Professional Conduct) Rules 2015 ("**PCR**") imposes fundamental duties of honesty, competence, and diligence on lawyers. At the same time, the Singapore Corporate Counsel Association's ("**SCCA**") Code of Ethics and Standards of Professional Conduct for In-House Counsel ("**SCCA Code of Ethics**") sets out duties to exercise due skill, care, integrity, and diligence.[14]

---

[12] See also IMDA, *supra* n 1, at p 13 and p 46 which provides testing guidance for RAG. Briefly, RAG is a technique that enhances AI models' responses by connecting them to external knowledge bases. While LLMs rely on their training data to generate responses, RAG supplements this by retrieving information from trusted external sources, allowing the model to provide more accurate and contextual outputs without requiring retraining.

[13] In practice, RAG is the mechanism used to "ground" a model's response on specified, authoritative sources of information (e.g. a firm's internal knowledge base or specific legal databases). This grounding capability is what enables the development of further trust-building features, such as: (a) direct citations - pinpointing the exact source of information within the provided documents for every part of the generated output, and (b) confidence scores - indicating the model's level of certainty for a given statement.

[14] SCCA's Code of Ethics sets out ethical behaviour and standards of professional conduct, and illustrates the ethical duties and responsibilities expected from the in-house community, which may assist SCCA Members and the In-House Counsel Profession in general.

19 Legal professionals in law practices and in-house legal teams are expected to exercise proper supervision over staff working under them. This includes paralegals, legal secretaries and other support staff. Legal professionals should ensure that they, and the staff under their supervision, possess the requisite AI literacy, and receive training on the key principles and best practices for ethical use of GenAI tools.

20 When using GenAI tools, legal professionals should consider the following approaches to uphold professional standards:

(a) **Develop AI literacy**. Legal professionals using GenAI should understand (i) how AI tools function and their limitations, (ii) when AI tools are likely to generate reliable output and when they are not, (iii) basic prompting techniques to reduce hallucination and bias, (iv) that AI competency varies across legal tasks, and (v) when and by whom additional scrutiny should be exercised when reviewing GenAI output.

(b) **Take ultimate responsibility for all work product.** Regardless of whether GenAI is used, legal professionals remain ultimately accountable for all work product as part of their professional duties owed to clients or business units they serve.[15] Additionally, the Singapore Courts' Guide on the Use of GenAI by Court Users emphasises that all court users are responsible for ensuring any information provided to the Court is independently verified, accurate, true and appropriate.[16] The use of GenAI tools does not delegate or diminish these obligations.

(c) **Apply necessary and proportionate human oversight.** Before using any GenAI-generated output in legal work, legal professionals must ensure that the output is correct, factually accurate, and fit for purpose. Legal professionals should apply a level of oversight that is sufficient for the nature and risk level of the task. See **Diagram 2** (Section 3.1) for a suggested risk-based approach. Enterprise-level tools may provide trust-building features such as **auditability** (e.g. traceable log of input and output) and **explainability** (e.g. confidence scores, source citations, reasoning), which can make review faster and more effective.

---

[15] See also Singapore Academy of Law and Microsoft Corporation, "Prompt Engineering for Lawyers" (2024) at p 6 on "Professionalism".

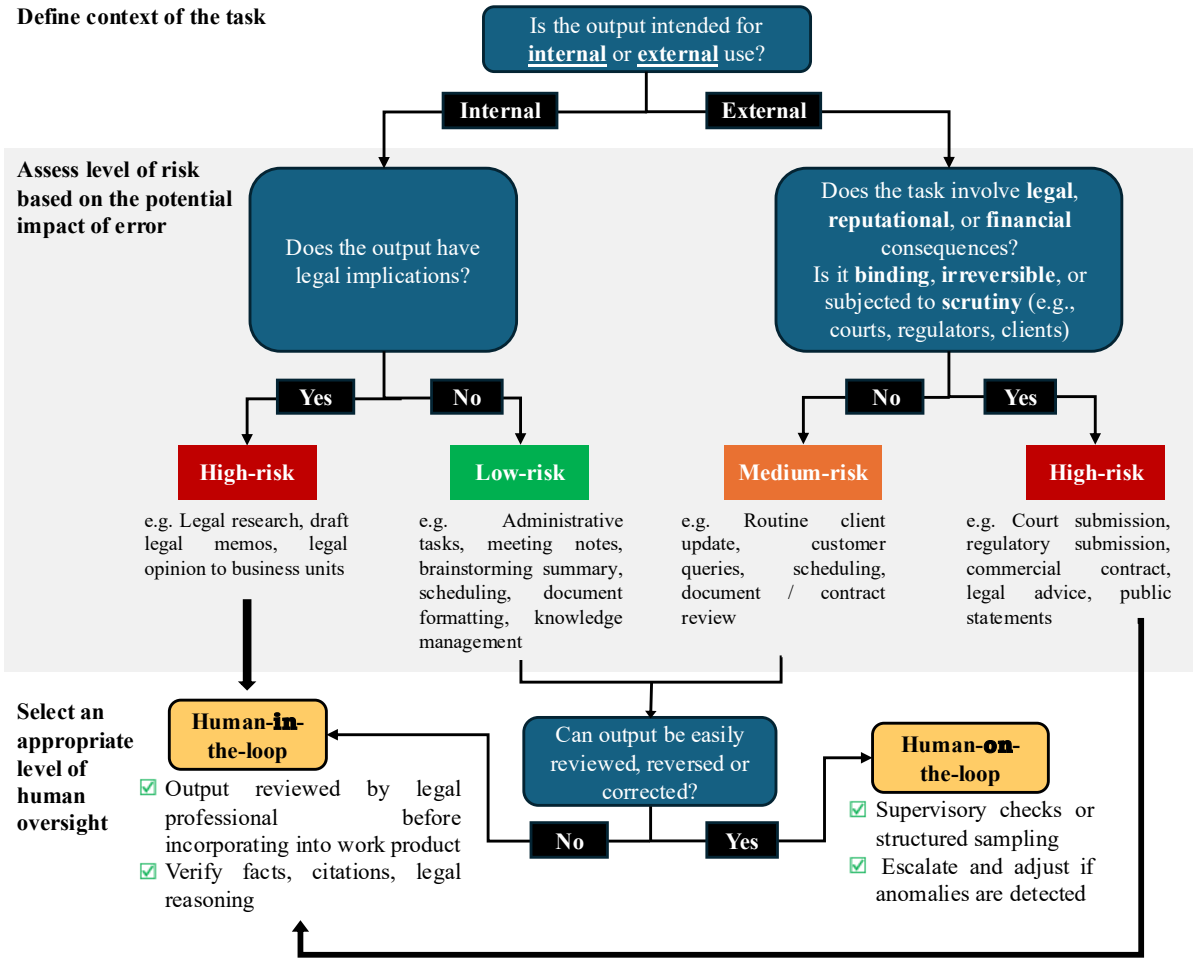
[16] Supreme Court of the Republic of Singapore, Registrar's Circular No. 1 of 2024, "Issue of the Guide on the Use of Generative Artificial Intelligence Tools by Court Users" (23 September 2024); State Courts of the Republic of Singapore, Registrar's Circular No. 9 of 2024, "Issue of the Guide on the Use of Generative Artificial Intelligence Tools by Court Users" (23 September 2024); and Family Justice Courts of the Republic of Singapore, Registrar's Circular No. 1 of 2024, "Issue of the Guide on the Use of Generative Artificial Intelligence Tools by Court Users" (23 September 2024)

(d) **Exercise greater scrutiny on areas outside of expertise.** GenAI can generate convincing, but inaccurate and/or biased responses. When using GenAI tools in areas outside their subject matter expertise, legal professionals should exercise greater scrutiny to identify potential hallucinations and biases, and take additional steps to verify output against authoritative sources and reference materials.[17]

(e) **Mitigate potential biases.** Legal professionals should actively identify and address potential biases by applying appropriate human oversight of GenAI output (see para 20(c) above). Consider also (i) testing GenAI outputs using different case types and client groups, (ii) asking GenAI to explain the reasoning or logic behind its recommendations, and/or (iii) choosing GenAI vendors who demonstrate bias testing and mitigation measures.

[17] See also Singapore Academy of Law and Microsoft Corporation, "Prompt Engineering for Lawyers" (2024) at p 6 on "Copilot, not autopilot".

Diagram 2: Suggested risk-based approach



Trust-building features

- ✓ **Auditability:** Does the tool provide audit trails (i.e. activity logs so that prompts and outputs can be traced for accountability)?
- ✓ **Explainability:** Does the tool offer confidence scores, indicators of reliability, source citations and/or provide reasoning for outputs?

Final check: Can you explain how GenAI output was verified, if asked?

→ If **NO**, review level of oversight and/or use tools with trust-building features.

Two levels of human oversight:

Human-in-the-loop

Human is actively involved in reviewing, approving, or making key decisions before the AI output is finalised or acted upon

- ☑ Human makes the final call before action is taken
- ☑ AI assists, but the legal professional is directly "in the loop"

→ Use when task requires legal judgement and accountability

Human-on-the-loop

Human oversees and monitors the AI system, but does not directly intervene in every decision unless errors or anomalies arise.

- ☑ Human provides oversight and can step in if needed
- ☑ The AI operates autonomously most of the time, but under human supervision

→ Can be applied for lower-risk or operational tasks where outputs are reversible or easily corrected

3.2. Confidentiality

Why is this important?

21 Rule 6 of the PCR imposes a fundamental duty on lawyers to maintain the confidentiality of any information acquired during professional work. This rule is principle-based and, akin to its application to other forms of technology (e.g. email or cloud computing), does not prohibit the use of GenAI provided that appropriate safeguards are implemented. Similarly, under the SCCA Code of Ethics, in-house counsel must protect the confidentiality of all information concerning the business and affairs of their organisation.

22 When using GenAI tools, legal professionals must remain vigilant and take proactive measures to protect confidential data, especially when client information is processed through third-party systems. Key risks, among others, include (a) unauthorised use of data for AI model training, (b) unauthorised third-party access (including employees within the same organisation without proper authorisation), and (c) malicious attack on models to extract sensitive information (e.g. prompt injection).

What should legal professionals do?

23 Legal professionals should take steps to uphold confidentiality when procuring and using GenAI tools. The following should be considered:

(a) Establish clear organisational rules for handling confidential client or business information, including data classification, data handling practices, and system access controls. See *Annex C - Sample Internal GenAI Governance Policy* under *Use-case classification* for an example.

(b) Select GenAI tools based on confidentiality needs. Tools offer varying degrees of protection, generally in this increasing order: free-to-use tools, enterprise-level commercial-off-the-shelf (known as "**COTS**") tools with safety features, and in-house developed GenAI systems. For confidential client or business data, prefer enterprise-level GenAI tools that provide the requisite level of assurances for data confidentiality and security.

(c) Review the GenAI provider's terms of service carefully to understand how input and output data is handled, i.e. whether it is retained or used for model training, and data privacy and security commitments. This will inform what type of data can be safely processed.

(d) When using free-to-use GenAI tools:

i) Disable data retention and use for model training; verify settings regularly as updates may reset configurations [**Note**: Data may be temporarily retained even with privacy settings enabled]; and

ii) Avoid using confidential or commercially sensitive information; if necessary, (i) anonymise data by replacing identifiers and sensitive information with generic placeholders (e.g. [Party A], [Company B], [Amount X]); (ii) frame queries as hypothetical scenarios; and (iii) use isolated clauses instead of full documents where possible. [**Note**: Anonymised content may still be identifiable with sufficient context. Consider documenting placeholders used for transparency, consistency, and traceability].

(e) For COTS solutions deployed at enterprise-level for use with confidential client data:

i) Review the GenAI provider's data protection, privacy, usage, and security policies and product features, where relevant. This includes but is not limited to:

a. How input, output, and system-generated data are collected, processed, stored, and deleted;

b. Whether firm data is used for model training or shared with third parties;

c. Availability of enterprise-grade privacy and security controls (e.g. encryption, audit logs, access control); and

d. Whether data processing agreements and confidentiality commitments meet client expectations.

ii) Verify that the GenAI provider's terms of service (or equivalent contractual agreement) explicitly prohibit use of input and output data for model training; and/or adjust data control settings to opt out of using input and output data for AI model training;

iii) Consider data residency requirements of clients or organisation, e.g. whether input and output data can be transferred, processed and stored outside of Singapore, and

ensure these requirements are met by the GenAI provider;[18]

iv) Prefer tools that (a) disclose their training data sources and methods, and (b) offer audit capabilities to verify that user data is not used for model training, and allow deletion of client data upon request or at the conclusion of engagement; and

v) Assess the robustness of GenAI provider's privacy and cybersecurity measures, including:

a. Privacy controls (e.g. encryption, audit logs, access control mechanism, and administrative-privilege restrictions);

b. Independent security certifications and documentation (e.g. SOC 2 Type II, ISO/IEC 27001);

c. Identity-management features (e.g. SSO, MFA); and

d. Integration and operational safeguards, including API security, model-isolation controls, logging, monitoring, and incident response processes.

(f) When developing proprietary GenAI systems, law practices and in-house legal teams should conduct a thorough review of the entire AI model development process, including how the model is designed and trained. This review should specifically address how input data is stored, processed, and whether it is employed for model training, ensuring that client confidentiality is not compromised.[19] Any proprietary training data containing client information should be anonymised before use.

24 See **Annex A** for examples of steps that law practices and in-house counsel teams have taken to ensure confidentiality when using GenAI tools.

---

[18] When GenAI systems store inputs or outputs that contain client information, such data may reside on servers outside Singapore. This could conflict with clients' data residency requirements, which restrict the geographical location their data can be stored or processed in for regulatory, compliance, or security reasons. Therefore, it is crucial to understand service providers' server locations and data storage practices before using client information in GenAI tools. For cloud-based GenAI solutions, please refer to The Law Society's Guidance Note 3.4.1 on "Cloud Computing" for further guidance on client data stored in overseas servers.

[19] This includes conducting relevant tests for data disclosure. See IMDA, *supra* n 1, from p 65.

3.3. Transparency

Why is this important?

25 Rule 5 of the PCR imposes a duty, among others, on lawyers to be honest in all dealings with clients and to inform them of any information that may reasonably affect their interests. Similarly, the SCCA Code of Ethics obliges in-house counsel to act in a fair, honest, and transparent manner when discharging their duties.

26 Legal professionals should assess whether their use of GenAI tools could reasonably impact the interests of their clients or organisations, and whether disclosure is necessary. This is particularly important when the use of GenAI is integral to the legal workflow.

27 Legal professionals should consider disclosing to clients or business units the use of GenAI, especially in the following three situations:[20]

(a) When GenAI is used substantially in producing work product, e.g. reviewing contracts, preparing litigation strategies, evaluating litigation outcomes, or generating documents that clients or business units will rely on;

(b) When GenAI impacts the cost of legal services. For example, where legal practitioners intend to incorporate the cost of GenAI tool(s) into client fees beyond traditional billable hours, it may be reasonable to inform clients and agree on the approach; or

(c) When data handling practices of the GenAI tool(s) may potentially conflict with client-specific preferences or data residency requirements.

28 Clear communication about the use of GenAI in legal work creates an opportunity to build trust with clients or business units by offering assurance, explaining safeguards for responsible and ethical use, and addressing concerns proactively. When legal professionals help stakeholders understand both the benefits and measures in place to ensure safe AI innovation, they demonstrate that technology can enhance efficiency and service quality while upholding their professional obligations and ethical standards.

29 Additionally, the Supreme Court's Guide on the Use of GenAI by Court Users requires all court users, including legal professionals, to be prepared to identify GenAI use in court

[20] See also Singapore Academy of Law and Microsoft Corporation, "Prompt Engineering for Lawyers" (2024) at p 6 on "Disclosure".

documents and explain how the output was verified, if asked.[21]

What should legal professionals do?

30 When disclosing to clients and business units on the use of GenAI, legal professionals should:

(a) Choose appropriate disclosure channels, such as client engagement letters, law practice's website or in correspondences with business units;

(b) Where relevant, explain how GenAI is used in their provision of legal service. For example, which tools are used, at what stage of the legal workflow, by whom, and how the output is verified. This may be important in the following contexts:

i) For legal practices, clients may maintain a whitelist of preferred or approved GenAI tools for use by their service providers, and seek assurance that their legal service provider has performed appropriate risk assessment and due diligence on the GenAI tools used.

ii) For in-house counsel, organisations may require all software used, including those used by in-house legal teams, to comply with enterprise-wide IT policies;

(c) Clarify that while GenAI tools may be used, legal professionals retain full responsibility for the work product;

(d) Provide clients with information on safeguards implemented to ensure data privacy and confidentiality;

(e) Provide contact channels for clients to reach out regarding their questions or concerns; and

(f) Offer clients the option to opt out of GenAI being applied in connection with their matters[22].

---

[21] Supreme Court of the Republic of Singapore, Registrar's Circular No. 1 of 2024, "Guide on the Use of Generative Artificial Intelligence Tools by Court Users" (2024) at p 5, Section 5 para (4).

[22] Where clients choose to opt out, it is important to explain how this may impact the delivery of legal services. For example, certain efficiencies or capabilities enabled by GenAI may not be available, and traditional processes may be used instead, resulting in slower turnaround time, and potentially higher costs. This ensures clients can make informed decisions about their preferences.

See **Annex A** for examples of how law firms have communicated and disclosed their use of GenAI tools to clients. Refer to **Annex C -** *(III) Sample Clauses for Letter of Engagement* for a sample clause that can be included in letters of engagement.

4. Implementing GenAI in Legal Practice or Team

31 This section provides a framework for implementing GenAI, drawing on industry experiences and emerging best practices. Each step in this section is mapped to three progressive adoption stages (see para 32). When developing an implementation strategy, law practices or teams should first determine their current stage of GenAI adoption and consider the relevant steps, bearing in mind the key principles in Section 3.

32 To determine which GenAI adoption stage applies, a quick guide is as follows:

(a) **Stage 1:** Starting with basic GenAI tools (e.g. Microsoft Copilot, LawNet AI) to support routine tasks.

(b) **Stage 2**: Building on Stage 1 by expanding to commercial-off-the-shelf legal GenAI tools (e.g. Harvey AI, CoCounsel, Robin AI, Legora) for core legal tasks.

(c) **Stage 3:** Building on Stage 2 by implementing commercial-off-the-shelf legal GenAI tools, and developing customised legal GenAI solutions tailored to the specific needs of the law practice or team.

After identifying the applicable adoption stage, refer to the steps marked for that stage throughout this section. For practical examples, refer to **Annex B,** which provides illustrations of how law practices and in-house teams have implemented GenAI in their organisations.

4.1. Step 1: Develop an AI adoption framework

33 A clear framework sets clear expectations, supports compliance, and build trusts – both within your team, and with clients or internal stakeholders. A comprehensive AI adoption framework includes both internal and external facing policies.

(a) **Internal policies** guide responsible GenAI usage, compliance with professional standards and operational requirements, including development of AI literacy.

(b) **External policies** communicate your GenAI practices and safeguards to clients, business units, and stakeholders. These policies should clarify how GenAI is used, how data is protected, and how clients, business units and stakeholders can raise concerns or opt out (see Section 3.3 of this document on transparency).

34 These policies establish the foundation for effective governance and responsible implementation, addressing professional obligations and operational requirements that will guide the selection and deployment of GenAI tools within your law practice or team.

35 The following key elements may be considered:

- **Governance structure:** Appoint an AI lead (for small practices / teams), or committee (for large practices / teams) for oversight, policy implementation, updates, and training.
- **Usage protocols:** Define approved GenAI tools, permissible data or information for prompts, and required level of human oversight (e.g. human-in-the-loop or human-on-the-loop), bearing in mind the key principles in Section 3.
- **Data classification:** Categorise information according to confidentiality levels (e.g., public, internal, confidential, highly confidential) and specify which GenAI tools can be used for each category.
- **Procurement requirements:** Establish clear criteria and due diligence processes for selecting GenAI vendors and tools (see Step 3 below).

Practical tip

Refer to the sample clauses for internal GenAI governance policy, employee handbook, and letter of engagement in **Annex C**, and adapt them to your needs.

For Stage 3

Implement more specific governance policies tailored to your firm's needs, and consider including additional terms to address data privacy, intellectual property considerations in greater detail.

- **Disclosure and client communication protocols:** Establish clear procedures for communicating to clients, business units, or stakeholders about how GenAI is used in legal work, including safeguards for confidentiality and data protection.
- **Incident reporting:** Set out procedures for reporting and managing misuse, errors, or data breaches involving GenAI tools.

i) Establish an AI incident-response protocol that can be activated upon triggers such as detection of unreliable citations, unexpected content, or exposure of sensitive

data. The protocol can include triage procedures, rollback plans, mitigation actions, client notification protocols, and vendor escalation steps**.** The Cyber Security Agency's Singapore Cyber Emergency Response Team (SingCERT) provides reference materials (e.g. checklist, playbooks, reporting forms) at https://www.csa/gov.sg/resources/singcert which legal professionals can refer to when formulating this protocol.

ii) Ensure these procedures are aligned with PDPC breach-notification obligations and your organisation's internal escalation paths.

- **Training and capability building:** Require regular training to improve AI literacy, including prompt engineering, risk management, and updates on policies, best practices and/or regulatory developments.

4.2. Step 2: Diagnose and analyse needs

36 Identifying where GenAI can deliver the greatest value begins with a clear understanding of your organisation's current workflows, challenges, and strategic priorities. Deploying GenAI may require substantial workflow and process redesign to achieve its full potential.

37 Use this checklist to identify potential GenAI use cases and assess risk and feasibility of adoption:

Step 2: Diagnose and analyse needs	Stage 1	Stage 2	Stage 3
Set objectives for GenAI adoption and identify potential use case(s):			
☐ General productivity tasks (e.g. document summarisation, language modification, legal research)	✓	✓	✓
☐ Core legal tasks (e.g. contract review, advanced legal research, e-discovery)		✓	✓
☐ Specialised legal task (e.g. complex transaction analysis, regulatory compliance, due diligence)			✓
Assess risk and feasibility of GenAI use cases *(see Annex D for sample evaluation questions):*			
☐ Level of confidentiality of the data used	✓	✓	✓
☐ Risk level of the task and corresponding human oversight required	✓	✓	✓
☐ Cost-benefit analysis for adopting GenAI solution	✓	✓	✓

☐ Readiness for change (e.g. availability of resources, required skillsets, training)	✓	✓	✓

38 For Stage 3 of implementation, **Annex D** offers a structured approach, along with sample evaluation questions, to guide the identification and prioritisation of GenAI use cases.

4.3. Step 3: Identify and evaluate GenAI tools

39 Selecting the right tool requires proper and thorough due diligence to ensure that the tool is secure, reliable, and suitable for legal work. Law firms and in-house teams should ensure that the chosen solution offers robust safeguards to support professional and ethical duties, protects client and/or business information, provides technical capabilities suited for the identified use case(s), and is provided by credible, trustworthy vendors. As a user of the solution, remember you have the right to ask the vendor to demonstrate how they offer such safeguards and protection, and their track record before subscribing to their solutions.

40 Use this checklist to guide evaluation of GenAI tools:

Step 3: Identify and evaluate GenAI tools	**Stage 1**	**Stage 2**	**Stage 3**
Assess data security and confidentiality measures *(See also Section 3.2)*			
☐ Vendor policies on usage of data inputs for model training	✓	✓	✓
☐ Retention of data inputs and prompts	✓	✓	✓
☐ Data storage location and jurisdiction (whether cloud or on-premises)	✓	✓	✓
☐ Access controls and security measures	✓	✓	✓
Evaluate technical capabilities and system requirements			
☐ Suitability for identified use case	✓	✓	✓
☐ Compatibility with existing systems		✓	✓
☐ Scalability and customisation options		✓	✓
☐ Update and maintenance protocols		✓	✓
☐ Support and training resources		✓	✓
Assess model performance and output quality			
☐ Define benchmarks for acceptable performance (e.g. level of accuracy and quality of output) for the identified use case		✓	✓

☐ Review vendor-reported performance metrics and testing results, where available	✓	✓	✓
☐ Evaluate model performance test results against defined benchmarks	✓	✓	✓
☐ Assess availability of trust-building features (e.g. explainability and auditability, see Section 3.1)	✓	✓	✓
Vendor due diligence – credentials and track record			
☐ Compliance with relevant regulations	✓	✓	✓
☐ Vendor's public commitment to responsible AI development and AI principles	✓	✓	✓
☐ Experience in legal sector deployment		✓	✓
☐ Client references and testimonials		✓	✓
☐ Financial stability and long-term viability		✓	✓

41 Refer to **Annex E: Sample Vendor Checklist** to guide vendor assessment. For further guidance on assessing and mitigating AI-related security risks, please refer to the ***Guidelines* and *Companion Guide on Securing AI Systems*** published by the Cyber Security Agency.

42 At **Stage 2** or **Stage 3**, law practices or teams may work with cybersecurity specialists to review security features and confirm that the provider's safeguards meet organisational requirements and support intended use cases.[23]

4.4. Step 4: Implementation and training

43 After selecting the tools, establish a structured approach to deployment and training to ensure effective adoption while maintaining professional standards. A well-planned implementation strategy supports user adoption and risk management.

[23] For cybersecurity expertise, organisations may consider the Cyber Security Agency's CISO-as-a-Service (CISOaaS) programme, which provides access to qualified consultants to develop a Cybersecurity Health Plan and strengthen security posture. Details are available at https://www.csa.gov.sg/our-programmes/support-for-enterprises/sg-cyber-safe-programme/cybersecurity-certification-for-organisations/ciso-as-a-service-to-develop-cybersecurity-health-plan/

44 Consider the following steps:

Step 4: Implementation and training	Stage 1	Stage 2	Stage 3
Develop an implementation strategy			
☐ Define scope of pilot project	✓	✓	✓
☐ Identify an AI lead to champion the project	✓	✓	✓
☐ Plan staged deployment timeline and establish clear success metrics	✓	✓	✓
☐ Set up communication channels with vendor for coordination and support		✓	✓
☐ Coordinate with vendor for product onboarding and secure data migration		✓	✓
☐ Develop feedback and troubleshooting mechanisms for users		✓	✓
Conduct user acceptance test			
☐ Document best practices to guide users in crafting more effective prompts	✓	✓	✓
☐ Assess quality and effectiveness of generated output based on user requirements and established standards (including defined benchmarks for acceptable performance in Step 3)		✓	✓
☐ Refine prompts to introduce clearer constraints, contextual details, and instructions to improve model responses and achieve higher quality output			✓
☐ Consider pre-generating prompts for common use cases			✓
Monitor and evaluate usage			
☐ Identify areas for improvement and update training or protocols as needed	✓	✓	✓
☐ Track usage patterns and adoption rates [**Note**: This may require vendors to provide the required permissions and data logs (e.g. logins, number of queries, types of queries, etc.)]		✓	✓
☐ Assess performance against objectives		✓	✓
☐ Review outcomes and impact on work quality, efficiency, and user satisfaction		✓	✓
Safeguards and training			

☐ Ensure all users receive training on GenAI tool functionality, prompt engineering, risk management, and incident-response protocols.	✓	✓	✓
☐ Check if guardrails such as PII/secret detectors and content filters can be implemented to prevent data leakage and inappropriate outputs		✓	✓
☐ Check if vendor can conduct adversarial testing to identify vulnerabilities (e.g., prompt-injection, jailbreak) before deployment		✓	✓

45 Training programmes should reinforce that GenAI is intended to augment, not replace, foundational legal competencies. For junior lawyers especially, the goal is not simply to teach them how to use AI tools, but to develop them holistically into competent legal professionals. This includes cultivating the ability to assess, challenge, and refine GenAI output, ensuring that AI use strengthens, rather than weakens, their development of core legal skills.

4.5. Step 5: Continuous review and improvement

46 Regular review ensures GenAI remains effective and complies with professional standards. Establish systematic review processes to evaluate performance and update practices based on experience and changing requirements.

47 Consider the following areas for continuous review and improvement:

Areas for review and improvement	Stage 1	Stage 2	Stage 3
☐ Evaluate implementation outcomes against original objectives	✓	✓	✓
☐ Review and strengthen usage protocols and risk management framework	✓	✓	✓
☐ Identify new opportunities to enhance existing workflows	✓	✓	✓
☐ Assess return on investment using defined metrics		✓	✓

48 Stay current with emerging GenAI technologies and industry developments through the following best practices:

- Active participation in events such as TechLaw.Fest and Legaltech GoWhere events organised by MinLaw and SAL, legaltech fairs by LawSoc, and relevant professional development programmes.

- Attend cybersecurity health clinics run by the Cyber Security Agency to strengthen understanding of cybersecurity risks and protective measures relevant to legaltech implementation, including GenAI.

- Engage in knowledge sharing, monitor regulatory requirements and professional conduct rules, and continuously explore new opportunities to optimise workflows and expand legaltech applications, including GenAI, across teams and practice areas.

Annex A: Illustrations of Key Principles for Use of GenAI in Legal Work

This annex provides practical examples of how law practices and in-house counsel teams have demonstrated the key principles in Section 3 when using GenAI.

Principle	Law Practice / Company	Example(s)
Confidentiality	OC Queen Street LLC	• Established an internal policy that permits its lawyers to use LLMs, with strict adherence to its internal guidelines and industry best practices. • When using publicly available LLMs, the policy requires data control settings to be adjusted to prevent input data from being used for AI model training.
Confidentiality	Rajah & Tann Singapore LLP	• Maintains strict control over GenAI usage by limiting access to enterprise versions of tools such as Microsoft Co-pilot and Harvey AI. • Selects enterprise solutions only after securing commitment from solution providers that the firm's data, including client data, is not used for foundation model training, and the assurance of information security and data privacy.
Confidentiality	WongPartnership	• Requires specific contractual commitments from its legaltech vendors, including data encryption, data deletion, and prohibition of access to and use of input data for model training. • These safeguards are reinforced by data minimisation protocols when using GenAI tools. For example, users must consider the sensitivity of data and take measures to input only necessary data, and remove or anonymise confidential details used in inputs whenever possible.
Confidentiality	GenZero[24] (in-house legal team)	• Even when using enterprise versions of GenAI tools, additional safeguards are taken when handling sensitive information. For example, when transcribing minutes of

[24] GenZero is global investment firm incorporated and headquartered in Singapore.

		meetings with sensitive company information, safeguards such as limiting access and ensuring files were immediately downloaded and deleted, were put in place to ensure confidentiality.
Transparency	KEL LLC	• Discloses the use of GenAI to its clients by including the following clause in its terms of engagement: "We may employ AI to improve our productivity and efficiency. You agree that we can utilise AI in connection with this engagement."
Transparency	Rajah & Tann Singapore LLP	• Notifies all existing clients about their GenAI adoption and strategy, and incorporates this information in their engagement letters for prospective clients. The firm also publishes their AI strategy on its website,[25] and has established dedicated contact channels for clients to address their GenAI-related queries.
Transparency	Clifford Chance	• Openly communicates with its clients how GenAI is integrated into its workflows, the safeguards in place, and the principles guiding its use. The firm has also published their AI principles on its website.[26]
Transparency	WongPartnership	• Tailors their communication with clients on the use (or restriction) of GenAI based on their understanding of each client's needs, recognising that clients have varying requirements and concerns about GenAI usage on their matters depending on where they are at on their own technology journey and their business context.

[25] See https://sg.rajahtannasia.com/ai-strategy/

[26] See https://www.cliffordchance.com/about_us/who-we-are-and-how-we-work/policies/AI-Principles.html

Annex B: Illustrations of GenAI Implementation in Legal Practice

Step	Law Practice / Company	Example(s)
Step 1: Develop an AI adoption framework	Dentons Rodyk	• Established comprehensive policy guidelines, guided by an internal AI Committee, which aim to balance between innovation with ethical considerations. • Takes a facilitative and platform-agnostic approach, with a focus on internal education. • Deploys tools like Microsoft Copilot to enhance internal productivity, granting access only after employees complete in-house training. • These sessions cover foundational AI knowledge, ethical use, risk management, and practical skills such as prompt engineering to help users generate more accurate and valuable outputs.
	Rajah & Tann Singapore LLP	• Formed an AI Core Team comprising subject-matter experts across various domains: o **Technology adoption specialist** to analyse product standards, oversee procurement, and implementation; o **Cybersecurity specialist** to review security features and solution provider's safeguards; o **Knowledge management** to curate and manage data for AI / Gen AI use, implement adoption of AI / GenAI, drive cultural change and innovate to use AI / Gen AI to streamline and facilitate lawyers' workflow; o **Innovation lead** to assess relevance from innovation standpoint; and o **Regional management counsel** and an **Executive Committee for Technology** to lead the firm's AI strategy, and set direction on AI adoption with an aim to improving operational efficiency, enriching the work environment and delivering better service.

Step	Law Practice / Company	Example(s)
	WongPartnership	• Implemented a firm-wide framework for AI safety. The framework and its accompanying policies are communicated to all members of the firm to ensure clarity around expectations, procedures, and rationale. This minimises the risk of inconsistent practices and addresses responsible GenAI use. Examples of matters addressed under the framework include: o Protocols for data uploads, including restrictions on the use of sensitive data o Risk assessment procedure in relation to the use of data on GenAI platforms based on data classifications o Approval mechanisms to facilitate oversight on the use of data in relation to GenAI platforms
	GenZero (in-house legal team)	• Established an AI adoption framework, in collaboration with their IT and Risk department, before fully implementing GenAI tools. The framework includes data classification and management procedures, a cybersecurity framework, and cyber-crisis plans and toolkits. • Implemented training to raise awareness of cyber risks and to ensure proper handling of information at different sensitivity levels, with particular attention to GenAI use.
Step 2: Diagnose and analyse needs	Clifford Chance	• Segment their GenAI adoption across different levels of complexity and specialisation: o At the first foundational tier, firms can implement everyday AI tools that enhance general productivity across the organisation. These include widely accessible solutions like Microsoft Copilot, which effectively assists in general drafting, modifying tone and language, and summarising content. o The second tier focuses on AI tools designed for core legal capabilities, targeting specific functions such as contract review and e-discovery. These specialised tools require more focused deployment and training but can significantly enhance efficiency in

Step	Law Practice / Company	Example(s)
		defined areas of practice. o The third and highest tier represents AI solutions designed to address complex, firm-specific needs that are not met by off-the-shelf solutions. These solutions are customised or self-built.
	Allen & Gledhill LLP	• Partnered with Singapore GenAI startup Pand.ai in 2024, with support from IMDA, to develop and implement an in-house and on-premises LLM. • Consolidated over 100 use cases across various practice areas, and built its LLM around the use cases with the greatest impact and highest likelihood of success. • Deploys the LLM to optimise the quality and speed of research, drafting and advise, especially in relation to specific aspects of complex matters.
Step 3: Identify and evaluate GenAI tools	Rajah & Tann Singapore LLP	• Begins its GenAI tool evaluation by identifying the specific challenges the firm aims to address through the adoption or implementation. This informs their market research to identify tools that may be suitable for those needs. Once potential solutions are identified, the firm shortlists and evaluates them using a structured checklist. • A sample of checklist includes, among other things: o Whether the firm's and client's data are used to train the AI / GenAI model; o Whether the tools deal with hallucinations and bias; o Whether the tools cite sources for their output; o Information security and data privacy safeguards and standards; o Whether the tools put in place access controls that observe the firm's information barriers arrangements and client confidentiality requirements;

Step	Law Practice / Company	Example(s)
		○ Data / prompt retention manner (cloud or on-premises server) and jurisdiction; ○ The firm's budget; ○ Functionalities and usability of the tools; and ○ Training support provided by the AI / GenAI solution providers.
	Google (Legal department)	• Leverages Google's foundation AI, including the Gemini family of models, to enable a two-track strategy for GenAI adoption: ○ Centralised solutions: The department centrally builds and deploys AI solutions for common, high-volume legal needs to ensure consistency and scale. ○ Empowering individual lawyers: Individual lawyers are empowered to become "builders" themselves, using intuitive, approved platforms like Vertex AI and NotebookLM. These platforms allow lawyers to create custom tools tailored for niche, specialised workflows. • For example, to support complex commercial negotiations, the team developed an AI Negotiations Assistant using Vertex AI. This specialised agent is grounded on a secure, curated dataset of agreement documents and negotiation guidance. The Assistant is powered by a Gemini model to generate draft clauses, summarize standard positions, and create first drafts of internal advice notes, all with citations to original source documents. • Additionally, the team uses a custom-built Gemini Gem to analyse negotiated agreements, highlight deviations from commercial practice guides, and provide tailored recommendations based on specified risk tolerance levels.
Step 4: Implementation and training	Clifford Chance	• Set up an Innovation Board to monitor AI usage firm-wide, supported by steering groups that test and provide feedback on the effectiveness of the tools
	Rajah & Tann Singapore LLP	• Engages subject-matter experts within the firm to identify the challenges the firm is aiming to

Step	Law Practice / Company	Example(s)
		address through the adoption of AI / GenAI tools and gather user requirements • Implements controlled testing with small, targeted user groups • Gathers test users' feedback on and assessment of the products and provide survey reports and analysis to Executive Committee for Technology for decision making • Conducts structured proof-of-concept exercises with vendors
	WongPartnership	• When piloting GenAI tools with vendors, each practice area is represented by a small group, led by a designated team lead to support focused discussions. • Participants receive onboarding training and attend regular touch-point sessions to facilitate feedback, address challenges, and discuss best practices. • During the pilot, team members systematically document their use cases, outcomes, and assessment of tool functionality and issues. Such documentation supports thorough reviews and helps inform decisions about product refinement and adoption. • At the end of the pilot, a custom survey is distributed to measure satisfaction and collect quantitative performance metrics. This process helps evaluate the practical utility, accuracy, and efficiency of Gen AI tools within each practice area and at an enterprise level.
Step 5: Continuous review and improvement	WongPartnership	• Places particular emphasis on the ongoing assessment of its GenAI tools to ensure sustained effectiveness and alignment with compliance requirements and operational objectives when using GenAI in legal services. • Engages in regular discussions with vendors after deployment of GenAI tools to remain abreast of the latest developments and updates to the tools. This facilitates timely alignment of internal policies and procedures in response to

Step	Law Practice / Company	Example(s)
		emerging technological advancements or potential risks. • Conducts annual post-deployment surveys to track usage, evaluate utility, and collect user feedback.

Annex C: Sample Templates and Clauses for GenAI Usage Policy

(I) Sample Internal GenAI Governance Policy

---

1. Objective

To guide the responsible, ethical and secure use of GenAI tools in the practice of law, in alignment with Singapore's legal, professional responsibility and data protection standards.

2. Scope

This policy applies to all employees, contractors and interns using GenAI tools for legal, administrative, or client-related tasks.

3. Responsible Use of GenAI

(a) Confidentiality

i) Do not input client names, case details or sensitive data into public GenAI platforms.

ii) Use only secure GenAI tools approved by the firm / company for handling confidential information.

(b) Accuracy

i) GenAI-generated content must be reviewed and verified before use. Where necessary, such review and verification must be by a qualified lawyer.

(c) Transparency

i) Inform clients, business units and stakeholders when GenAI tools are used in their matters, such as drafting or research.

(d) Accountability

i) Employees, contractors and interns remain fully responsible for all outputs, regardless of GenAI involvement.

4. Use-case Classifications

Classification	Description	Elaboration/ Examples	Implication
Public	Intended for public use	Material authorised for publication	Can use public GenAI platforms
Internal	Proprietary information intended for internal use or authorised external use.	All internal matters except for information designated as "Confidential" or "Highly confidential". Examples include: • automating administrative tasks (e.g. scheduling); and • core legal tasks (e.g. legal research, summarising case law or legal texts)	Can use public GenAI platforms
Confidential	Client / business confidentiality – on a need-to-know basis	All client / business unit information except those under "Highly confidential". Examples include: • drafting initial versions of legal documents, • contract review, • policy review, • document summarisation, • language modification. Internal financial information or internal information designated as confidential	Use only firm/company-approved secure GenAI tools
Highly confidential	Authorised users only – data marked as highly confidential	Any data that falls within the following categories: • Official Secrets Act • Bank customer information • Personally identifiable information • MAS for corporate finance • Designated as secret or highly confidential by the client	Use only firm/company-approved secure GenAI tools Requires express approval by client, business unit and/or relevant committee
Prohibited	Use cases that are prohibited	Examples include • providing legal advice without human review	

Classification	Description	Elaboration/ Examples	Implication
		• predicting case outcomes without context • handling sensitive data in non-approved GenAI tools	

5. Training and Oversight

All staff must complete basic GenAI training annually. The firm / company will review issues arising from GenAI usage quarterly.

6. Incident Reporting

Any misuse, error or data breaches involving GenAI tools must be reported immediately to the relevant head of department. Reports should include the nature of the incident, the tool used and any affected data.

(II) Sample Clauses for Employee Handbook

Misuse or unauthorised use

Employees may intentionally or inadvertently misuse authorised GenAI tools, such as by attempting to manipulate outputs (e.g., through prompt injection) or using GenAI tools beyond their intended and authorised scope. Such actions can compromise data security, produce unreliable results, or expose the firm to legal and reputational risks.

Sample clause
Unauthorised use, modification, or tampering with GenAI tools, including but not limited to prompt injection or any attempt to manipulate AI outputs, is strictly prohibited. Employees must only use GenAI tools and upload authorised information as expressly authorised, classified as appropriate for use with these tools, and in accordance with the Firm's / Company's policies and procedures. Any suspected misuse or unauthorised activity must be reported immediately to *[reporting channel]* and may result in disciplinary action, up to and including dismissal.

Data privacy and security

The use of GenAI may involve the processing of sensitive personal or business data, increasing the risk of unauthorised access, data breaches, or non-compliance with data protection laws. Failure to safeguard such data could expose the firm to regulatory penalties and reputational harm.

Sample clause
Employees must comply with all applicable data protection and security policies, including obligations under the Personal Data Protection Act 2012 ("**PDPA**"), when using GenAI. No confidential, personal, or sensitive information may be uploaded or inputted into any GenAI tools without prior written authorisation from the Data Protection Officer or designated authority. Employees must ensure that any use of GenAI tools complies with the PDPA's data protection obligations, including consent, purpose limitation, and transfer limitation requirements where applicable. Any suspected or actual data breach involving GenAI must be reported immediately in accordance with the Firm's / Company's incident response procedures and, where required, to the Personal Data Protection Commission.

Intellectual property ("IP")

The use of GenAI tools may create copyright-related legal risks. For instance, GenAI output that incorporates significant portions of third-party copyrighted content may infringe the copyright in that content. The use of GenAI tools may also give rise to questions around whether the work is eligible for copyright protection, and if so, who owns the copyright.

Sample clause
All work products, inventions, or outputs generated by employees in the course of their employment, including those generated with the assistance of approved GenAI tools whether wholly or partially, shall be the exclusive property of the Firm / Company, subject to the terms of the employment contract and applicable intellectual property laws. Employees are prohibited from using unauthorised third-party GenAI tools or incorporating third-party content without prior approval. The Firm / Company makes no representations regarding the intellectual property status of AI-generated content and employees must ensure compliance with third-party terms of service for any approved GenAI tools.

Transparency and accountability

GenAI-driven decisions may lack transparency, making it difficult to explain or justify outcomes to clients, regulators, or other stakeholders. This can undermine trust and hinder the firm's / company's ability to demonstrate compliance or fair practice especially on occasions where unchecked GenAI outputs contain errors or unreliable output.

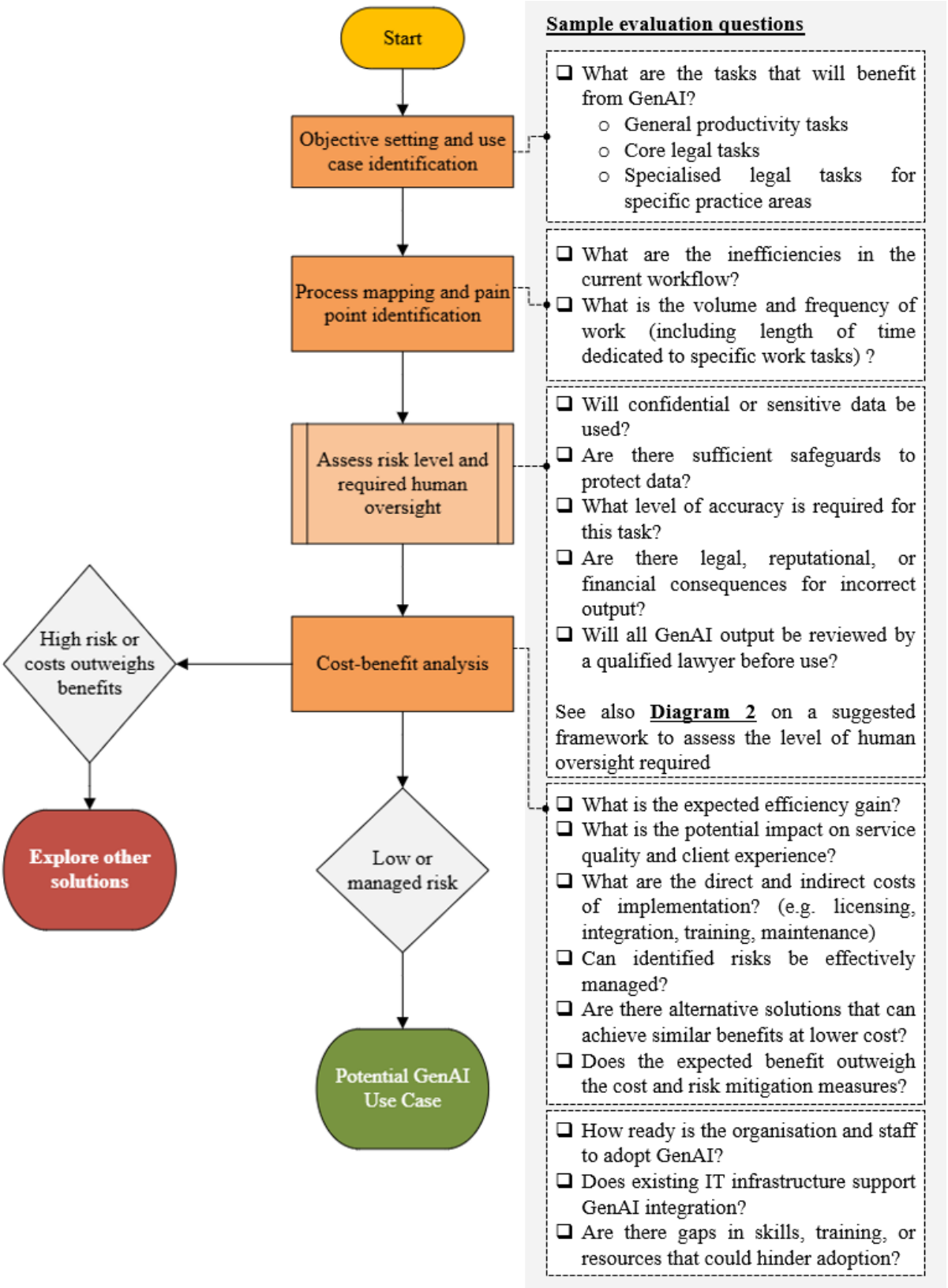
Sample clause
Employees must review and verify all content and responses produced by GenAI tools before incorporating into work products. Employees are personally responsible for ensuring the accuracy, quality, and appropriateness of AI-generated content and must exercise reasonable judgement in doing so. Where the context requires, the responses shall be reviewed by a qualified lawyer in the Firm / Company. Where significant portions of a work product rely on or includes content produced by GenAI tools, employees must keep a record of the input provided to the GenAI tools, e.g. copy of the prompt and list of references or resources provided. These records must be stored in *[designated location/system]* and retained in accordance with the Company's document retention policy [or for a minimum of *[X]* years].

(III) Sample Clauses for Letter of Engagement

The use of AI in business operations introduces risks such as data breaches, intellectual property issues, and reliability concerns, which can lead to legal and reputational consequences. Updating the letter of engagement is necessary to inform clients about AI use, clarify responsibilities, and manage potential liabilities.

Sample clause
The Firm may, from time to time, use advanced generative artificial intelligence ("GenAI") technologies to assist in delivering legal services, including for research, document review, drafting, and analysis. Such technologies are employed under strict protocols to ensure the confidentiality and security of client information. The Firm exercises oversight to ensure that all outputs are reviewed by qualified professionals and that no client-sensitive information is disclosed to external AI systems without the requisite safeguards and your prior consent. By engaging our services, you agree to our responsible use of GenAI in accordance with applicable laws and professional standards and that client information provided to us may be used in conjunction with GenAI.

Annex D: Sample Evaluation Checklist



Annex E: Sample Vendor Checklist

S/N	Question	Answer
Cybersecurity and data protection		
1	Is your solution hosted on a server that is compliant with recognised **cybersecurity standards** (e.g. MTCS SS584:2020, ISO/IEC 21878:2018, SOC-2 audit, or equivalent)?	
2	Is your solution compliant with **personal data protection standards** (e.g. ISO/IEC 27701, Data Protection Trustmark SS 714: 2025, SOC-2 audit, or equivalent)?	
3	Is your solution compliant with **cross border personal data transfers standards** (e.g. Global Cross Border Privacy Rules (CBPR), APEC Cross Border Privacy Rules, Global Privacy Recognition for Processors, APEC Privacy Recognition for Processors, or equivalent)?	
4	Are you compliant with the "Good Practices" of the Law Society of Singapore's Guide to Cybersecurity for Law Practices (30 March 2020)?	
Data handling measures		
5	Does your AI solution permit firms to set custom retention periods for client data?	
6	Can client data be securely deleted upon request or at the conclusion of the engagement, and is this process auditable?	
Available support and training resources		
7	What channels are available for after sales support (e.g., phone, email, live chat)?	
8	What are your standard support hours, and do you offer out-of-hours or emergency support?	
9	What is your guaranteed uptime?	
10	Are training materials and documentation provided, and if so, in which formats?	

List of Contributors

In developing this Guide, the Ministry of Law is grateful for the contributions from:

Asia-Pacific Legal Innovation & Technology Association

AdminLess.ai

Allen & Gledhill LLP

BetterWiser Pte. Ltd.

BillDetail

Center for AI and Digital Policy

Clifford Chance Pte. Ltd.

Cyber Security Agency of Singapore

Drew & Napier LLC

Dentons Rodyk & Davidson LLP

FsLAW LLC

Google

Infocomm Media Development Authority

KEL LLC

Lee Bon Leong & Co.

LegalEASE

Lexplosion Solutions Pte. Ltd.

Luo Ling Ling LLC

Ministry of Digital Development and Information

Microsoft Singapore

Mr Andre Chua

Mr Ang Hou Fu

Mr Chua Teck Leong

National University of Singapore Faculty of Law

OC Queen Street LLC

PwC Singapore

Rajah & Tann Singapore LLP

Ramdas & Wong

Selected Members of the Law Society of Singapore (Council, Information Technology Committee, Social & Welfare Committee, Cybersecurity & Data Protection Committee, Intellectual Property Practice Committee), and the Professional Conduct Council Advisory Committee

Singapore Academy of Law

Singapore Corporate Counsel Association Ltd

Singapore Courts

Singapore Management University, Yong Pung How School of Law, Centre for Digital Law

Stephenson Harwood LLP

Taxise Asia LLC

The App Association

University of Leeds, School of Law, Centre for Business Law and Practice

WongPartnership LLP