**COMPLIANCE AS A COMPETITIVE ADVANTAGE**

*AI Governance Resource Pack*

*Practical tools and references for regulated organizations navigating AI adoption*

**What's Inside This Pack**

* Tool #1 — AI Use Case Risk Tiering Template
* Tool #2 — AI Vendor Security Assessment Checklist
* Tool #3 — Green Lane AI Tool Evaluation Scorecard
* Tool #4 — 5-Rule AI Policy Starter Template
* Tool #5 — 30-Day Sprint Action Card
* Resource Guide — Frameworks, Reading & Platforms

|  |
| --- |
| **🛠 TOOL #1: AI USE CASE RISK TIERING TEMPLATE** |

**Purpose**

Use this template to assess and classify AI use cases before deployment. Triage by data sensitivity, automation level, and regulatory exposure to determine the appropriate level of review and approval required.

|  |  |  |  |
| --- | --- | --- | --- |
| **RISK TIER** | **CRITERIA** | **EXAMPLES** | **APPROVAL REQUIRED** |
| **🟢 LOW** | No sensitive data Fully human-reviewed No regulatory scope | Email drafting Non-confidential meeting summaries Public research | Manager acknowledgement Self-service from Green Lane |
| **🟡 MEDIUM** | Internal data only Partial automation Limited regulatory touch | Internal report drafting Data analysis (non-PII) Customer FAQs | Department head + IT review Vendor checklist required |
| **🟠 HIGH** | Confidential/PII data Significant automation Direct regulatory impact | Clinical documentation Financial forecasting HR decision support | Legal + Compliance + CISO Full vendor security audit DPIA may be required |
| **🔴 CRITICAL** | Regulated data (PHI, PII) Autonomous decisions High legal liability | Autonomous clinical triage Credit decisioning Legal contract execution | Executive sign-off Board awareness Full risk assessment + audit trail |

**How to Use This Template**

* Step 1: List every AI use case currently in use or being considered
* Step 2: Score each against the criteria above — when in doubt, go one tier higher
* Step 3: Apply the appropriate approval process before the tool goes live
* Step 4: Re-assess annually or when the use case, data scope, or tool changes
* Tip: Build this into your IT/software request process so it becomes automatic

**An Excel version of this document is also available for use. *(See ‘04\_data\_tier\_worksheet.xlsx’)***

|  |
| --- |
| **🛠 TOOL #2: AI VENDOR SECURITY ASSESSMENT CHECKLIST** |

**Purpose**

Use this checklist before signing any contract or enabling any AI tool that will touch organizational data. Ask these questions of every vendor — their answers (or inability to answer) tell you everything.

**DATA HANDLING**

|  |  |  |
| --- | --- | --- |
| **QUESTION** | **IDEAL ANSWER / RED FLAGS** | **✓** |
| Does this tool use our data to train its AI models? | *Must be NO or clearly opt-out confirmed in writing* | ☐ |
| Where is our data stored geographically? | *Must align with your data residency requirements* | ☐ |
| How long is our data retained after processing? | *Should align with your retention policy — shorter is better* | ☐ |
| Is data encrypted in transit and at rest? | *Minimum: TLS 1.2 in transit, AES-256 at rest* | ☐ |
| Do employees of the vendor have access to our data? | *If yes: under what conditions? With what controls?* | ☐ |

**SECURITY & COMPLIANCE**

|  |  |  |
| --- | --- | --- |
| **QUESTION** | **IDEAL ANSWER / RED FLAGS** | **✓** |
| Is the vendor SOC 2 Type II certified? | *Request the report — not just a badge* | ☐ |
| ISO 27001 certified? | *Good indicator of mature security management* | ☐ |
| Do they have a published AI ethics / responsible AI policy? | *Look for specifics, not marketing language* | ☐ |
| Have they undergone a third-party AI security audit? | *Emerging best practice — flag if not done* | ☐ |
| What is their vulnerability disclosure / patch process? | *Should have a clear, documented process* | ☐ |

**BREACH & INCIDENT**

|  |  |  |
| --- | --- | --- |
| **QUESTION** | **IDEAL ANSWER / RED FLAGS** | **✓** |
| What is their breach notification timeline? | *Your jurisdiction may require 72 hours — vendor must match* | ☐ |
| Have they experienced any data breaches in the past 3 years? | *If yes: what happened and what changed?* | ☐ |
| Do they carry cyber liability insurance? | *Ask for coverage limits* | ☐ |

**CONTRACTUAL PROTECTIONS**

|  |  |  |
| --- | --- | --- |
| **QUESTION** | **IDEAL ANSWER / RED FLAGS** | **✓** |
| Is a Data Processing Agreement (DPA) available? | *Non-negotiable for GDPR/HIPAA covered data* | ☐ |
| Are there data deletion rights on contract termination? | *You must be able to retrieve and delete your data* | ☐ |
| What are their sub-processor disclosure obligations? | *You should know who else touches your data* | ☐ |

**⚠ Red Flag Summary**

* 🚩 Vendor cannot confirm whether your data is used for model training
* 🚩 No SOC 2 report available (not just a badge — the actual report)
* 🚩 No DPA available for regulated data
* 🚩 Breach notification timeline exceeds your regulatory requirement
* 🚩 Vague or evasive answers to any of the above — this is itself a red flag

|  |
| --- |
| **🛠 TOOL #3: GREEN LANE AI TOOL EVALUATION SCORECARD** |

**Purpose**

The Green Lane is your pre-approved AI tool list. Use this scorecard when evaluating any new AI tool for inclusion. Tools that pass go on the Green Lane — employees can adopt them without a lengthy approval process every time.

|  |  |  |  |
| --- | --- | --- | --- |
| **CATEGORY** | **CRITERION** | **MAX POINTS** | **SCORE (0–Max)** |
| Data Handling | Does NOT train on org data | 3 |  |
| Data Handling | Data stored in compliant jurisdiction | 3 |  |
| Data Handling | Clear data retention & deletion policy | 2 |  |
| Security | SOC 2 Type II certified | 3 |  |
| Security | Data encrypted in transit and at rest | 3 |  |
| Security | MFA / SSO integration available | 2 |  |
| Compliance | DPA available and signed | 3 |  |
| Compliance | No outstanding regulatory actions | 2 |  |
| Compliance | Aligns with internal data classification policy | 3 |  |
| Usability & Control | Admin controls and audit logs available | 2 |  |
| Usability & Control | Usage monitoring / DLP integration possible | 2 |  |
| Usability & Control | Clear off-boarding / data export process | 1 |  |

**Scoring Guide**

|  |  |
| --- | --- |
| **29–29 points (max)** | Green Lane Approved — add to approved tool list |
| **22–28 points** | Conditional Approval — address gaps with compensating controls |
| **15–21 points** | Further Review Required — escalate to IT/Compliance |
| **Below 15 points** | Do Not Approve — do not deploy in regulated environments |

*Maximum possible score: 29 points | Recommended Green Lane threshold: 22+*

|  |
| --- |
| **🛠 TOOL #4: 5-RULE AI POLICY STARTER TEMPLATE** |

**Purpose**

This is a plain-language starting point — not a finished policy. Adapt language, add your organization's specific requirements, and have Legal/Compliance review before publishing. The goal is a one-page policy every employee can read and apply in under 5 minutes.

**[ORGANIZATION NAME] — AI USE POLICY**

*Version 1.0 | Effective Date: [DATE] | Owner: [ROLE/DEPARTMENT]*

|  |
| --- |
| **Rule 1: USE APPROVED TOOLS ONLY** |

Only use AI tools that appear on our approved Green Lane list. If you want to use a tool that isn't listed, submit a request to [CONTACT/PROCESS] before using it. Do not use personal AI accounts for work tasks.

*📌 Why: Unapproved tools may use your data to train AI models or store it in unsecured environments.*

|  |
| --- |
| **Rule 2: NEVER INPUT REGULATED OR CONFIDENTIAL DATA** |

Do not enter personally identifiable information (PII), protected health information (PHI), financial records, legal documents, client contracts, or any Tier 3/4 classified data into any AI tool — even approved ones — without explicit authorisation from [ROLE].

*📌 Why: Even compliant tools have risk at the data level. Classify first, then decide.*

|  |
| --- |
| **Rule 3: REVIEW EVERYTHING AI GENERATES** |

AI output is a starting point, not a final answer. You are responsible for verifying accuracy, appropriateness, and compliance of any content before it is used, shared, or acted upon.

*📌 Why: AI tools hallucinate, make errors, and lack contextual judgment. Human oversight is non-negotiable.*

|  |
| --- |
| **Rule 4: DISCLOSE AI USE WHERE REQUIRED** |

Where our professional obligations, client contracts, or regulatory requirements require disclosure of AI use (e.g., in legal filings, regulated reports, or client deliverables), you must disclose it. When in doubt, ask [ROLE] before submitting.

*📌 Why: Undisclosed AI use in regulated contexts can create legal and reputational liability.*

|  |
| --- |
| **Rule 5: REPORT CONCERNS PROMPTLY** |

If you believe an AI tool has handled data incorrectly, produced harmful output, or behaved in an unexpected way, report it immediately to [CONTACT]. If you receive a suspected phishing or AI-generated social engineering attempt, report it to [SECURITY CONTACT].

*📌 Why: Early reporting limits damage. There is no penalty for reporting in good faith.*

*QUESTIONS? Contact [AI POLICY OWNER] at [EMAIL/CHANNEL]  
This policy will be reviewed [ANNUALLY/QUARTERLY]. Last reviewed: [DATE]*

|  |
| --- |
| **🚀 TOOL #5: YOUR 30-DAY COMPLIANCE CONFIDENCE SPRINT** |

*Pick the tier that matches where your organization is today. Assign an owner to each action before you leave the room.*

**🟡 IF YOU'RE STARTING FROM SCRATCH**

|  |  |  |  |
| --- | --- | --- | --- |
| **ACTION** | **TIMING** | **NOTES** | **OWNER** |
| Conduct an AI Inventory Audit | Week 1 | Surveying all department leads — what AI tools are in use? |  |
| Identify your 1 highest-risk use case | Week 1–2 | Where is AI currently closest to regulated data? |  |
| Assign an AI Policy Owner | Week 1 | Someone accountable for governance — even in a small org |  |
| Draft your 5-Rule AI Policy | Week 2–3 | Use Tool #4 as your starting point |  |
| Publish your policy internally | Week 4 | Even a draft version creates clarity and accountability |  |

**🟠 IF YOU HAVE A FOUNDATION TO BUILD ON**

|  |  |  |  |
| --- | --- | --- | --- |
| **ACTION** | **TIMING** | **NOTES** | **OWNER** |
| Publish your AI policy org-wide | Week 1 | Ensure every employee has access and acknowledges it |  |
| Complete vendor security audits (Tool #2) | Week 1–2 | Prioritise any tool touching regulated data |  |
| Build your Green Lane approved tool list | Week 2–3 | Use Tool #3 to score and approve tools |  |
| Run a data classification workshop | Week 3 | Ensure staff can identify Tier 3/4 data on sight |  |
| Review and close your Governance Gap | Week 4 | Revisit the gap diagram — where are you now? |  |

**🔴 IF YOU'RE SCALING GOVERNANCE**

|  |  |  |  |
| --- | --- | --- | --- |
| **ACTION** | **TIMING** | **NOTES** | **OWNER** |
| Launch your AI Champions Program | Week 1–2 | Identify and onboard champions in each department |  |
| Build continuous AI monitoring | Week 2 | Audit logs, usage tracking, anomaly detection |  |
| Align to NIST AI RMF or ISO 42001 | Week 2–4 | Map your current controls against the framework |  |
| Pursue formal AI governance certification | Week 4+ | Begin gap assessment for ISO 42001 or equivalent |  |
| Track and report AI ROI + compliance metrics | Week 4 | What's compliance enabling — in revenue and risk avoided? |  |

**An Excel version of this is also available for use. (See ‘05\_90day\_roadmap.xlsx)**

|  |
| --- |
| **📚 RESOURCE GUIDE: FRAMEWORKS, READING & PLATFORMS** |

*Curated resources to support your AI governance journey — from first steps to advanced compliance.*

**FRAMEWORKS & STANDARDS**

**▶ NIST AI Risk Management Framework (AI RMF 1.0)**

*🔗 nist.gov/artificial-intelligence*

The US gold standard for AI risk governance. Surprisingly readable. Start with the Govern function.

**💰 Free PDF**

**▶ ISO/IEC 42001 — AI Management System Standard**

*🔗 iso.org/standard/81230.html*

The 'ISO 27001 for AI.' If your org is already ISO 27001 certified, this is a natural extension. Begin with a gap assessment.

**💰 Paid standard — summaries freely available**

**▶ EU AI Act**

*🔗 artificialintelligenceact.eu*

Even for non-EU organizations, this shapes global AI regulation. Understand the risk tier definitions — they're influencing frameworks worldwide.

**💰 Free summary site**

**▶ CISA AI Cybersecurity Guidelines**

*🔗 cisa.gov/ai*

Free, practical, government-backed guidelines specifically for AI cybersecurity. Excellent for defence/critical infrastructure sectors.

**💰 Free**

**THREAT INTELLIGENCE**

**▶ MITRE ATLAS**

*🔗 atlas.mitre.org*

The adversarial threat landscape for AI systems. Like ATT&CK but for AI-specific attacks. Essential for security-minded leaders.

**💰 Free**

**▶ OWASP Top 10 for LLM Applications**

*🔗 owasp.org/www-project-top-10-for-large-language-model-applications/*

The definitive list of AI/LLM security vulnerabilities. Practical and actionable for technical and non-technical leaders.

**💰 Free**

**PRIVACY & SECTOR-SPECIFIC**

**▶ Future of Privacy Forum — AI Resources**

*🔗 fpf.org/focus-area/artificial-intelligence/*

Especially valuable for healthcare and financial services. Strong on privacy-by-design in AI contexts.

**💰 Free**

**▶ HHS Office for Civil Rights — HIPAA & AI**

*🔗 hhs.gov/hipaa*

For healthcare leaders: official HHS guidance on AI use in HIPAA-regulated contexts.

**💰 Free**

**▶ FINRA — AI in Financial Services**

*🔗 finra.org/rules-guidance/key-topics/technology/artificial-intelligence*

Guidance specific to broker-dealers and financial firms on responsible AI adoption.

**💰 Free**

**ANNUAL REPORTS & BENCHMARKING**

**▶ Stanford HAI — AI Index Report (Annual)**

*🔗 aiindex.stanford.edu*

The most comprehensive annual report on the state of AI. Full of quotable statistics and trend data. Free to download.

**💰 Free PDF annually**

**▶ McKinsey — State of AI Report (Annual)**

*🔗 mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai*

Excellent benchmarking data on enterprise AI adoption, ROI, and governance maturity. Use for internal business cases.

**💰 Free with registration**

**▶ Gartner AI Governance Research**

*🔗 gartner.com*

Search 'AI governance' on Gartner for frameworks and maturity models. Some free, some require subscription.

**💰 Mixed — some free**

**PLATFORMS & TOOLS TO KNOW**

**▶ Microsoft Purview**

*🔗 microsoft.com/purview*

Data governance and compliance for Microsoft 365/Azure environments. Integrates with Copilot governance. Essential for Microsoft shops.

**💰 Commercial — included in some M365 plans**

**▶ Nightfall AI**

*🔗 nightfall.ai*

Data loss prevention specifically designed for AI tools and cloud environments. Detects sensitive data in AI interactions.

**💰 Commercial**

**▶ Securiti AI**

*🔗 securiti.ai*

Unified data + AI governance platform. Strong in regulated industries. Covers consent, privacy, and AI risk in one platform.

**💰 Commercial**

**▶ OneTrust — AI Governance Module**

*🔗 onetrust.com/solutions/ai-governance/*

Popular in compliance-heavy organizations. Integrates with existing GRC workflows. Good for those already using OneTrust.

**💰 Commercial**

**QUICK READS (UNDER 15 MINUTES)**

**▶ 'Responsible AI Principles' — Microsoft**

*🔗 microsoft.com/en-us/ai/responsible-ai*

A practical, enterprise-focused view of responsible AI principles. Useful as a benchmark for your own policy language.

**💰 Free**

**▶ Google DeepMind — AI Safety Resources**

*🔗 deepmind.google/safety*

For those wanting to understand the technical safety landscape behind the tools your org may be using.

**💰 Free**

**▶ 'Shadow AI: Risks and Mitigations' — various authors**

*🔗 Search: 'Shadow AI enterprise risk 2024'*

Multiple recent articles from Gartner, Forrester, and SANS on shadow AI. Search for the most current version.

**💰 Free — multiple sources**

**A FINAL THOUGHT**

*"The organizations that will win in regulated industries aren't the ones who waited until AI was perfectly safe. They're the ones who built the infrastructure to adopt it responsibly — while everyone else was still debating whether to try."*

Compliance is not your cage. It is your competitive moat.  
  
Use these tools. Adapt them to your context. Start this week.