

MENSHLY PLAYBOOK

# AI Compliance & Regulatory Automation

The complete operating system for building an AI compliance agency that generates \$35,000/month in recurring revenue. 8 modules, 30 procedures, regulatory scanning prompts, client delivery templates, and a 90-day execution timeline.

READING TIME

95 Minutes

PUBLISHED

2026

8

MODULES

30

PROCEDURES

\$35K

MONTHLY TARGET

---

# Table of Contents

|  |           |
|--|-----------|
| <b>MODULE 1: Regulatory Intelligence Foundation</b>                        | <b>3</b>  |
| Procedure 1.1: Build the Master Regulatory Database . . . . .              | 3         |
| Procedure 1.2: Build the Make.com Regulatory Monitoring Pipeline . . . . . | 4         |
| Procedure 1.3: Build the Jurisdiction Applicability Engine . . . . .       | 5         |
| <b>MODULE 2: AI System Inventory &amp; Shadow AI Detection</b>             | <b>6</b>  |
| Procedure 2.1: Create the Client Intake System . . . . .                   | 6         |
| Procedure 2.2: Build the Shadow AI Detection Engine . . . . .              | 7         |
| Procedure 2.3: Build the Risk Classification Engine . . . . .              | 8         |
| <b>MODULE 3: Compliance Gap Analysis &amp; Reporting</b>                   | <b>9</b>  |
| Procedure 3.1: Build the Three-Prompt Gap Analysis Chain . . . . .         | 9         |
| Procedure 3.2: Build the Make.com Gap Analysis Automation . . . . .        | 11        |
| Procedure 3.3: Create the Gap Report Quality Checklist . . . . .           | 11        |
| <b>MODULE 4: Remediation &amp; Automation Build</b>                        | <b>12</b> |
| Procedure 4.1: Build the Audit Trail Automation . . . . .                  | 12        |
| Procedure 4.2: Build the Human Oversight Mechanism Templates . . . . .     | 13        |
| Procedure 4.3: Build the Bias Monitoring Dashboard . . . . .               | 14        |
| <b>MODULE 5: Client Dashboard &amp; Monitoring System</b>                  | <b>14</b> |
| Procedure 5.1: Build the Client Compliance Dashboard . . . . .             | 15        |
| Procedure 5.2: Build the Monthly Monitoring Make.com Scenario . . . . .    | 15        |
| Procedure 5.3: Build the Quarterly Review Package . . . . .                | 16        |
| <b>MODULE 6: Audit Documentation &amp; Preparation</b>                     | <b>17</b> |
| Procedure 6.1: Build the Audit Package Generator . . . . .                 | 17        |
| Procedure 6.2: Build the Audit Readiness Checklist . . . . .               | 17        |
| <b>MODULE 7: Sales, Proposals &amp; Client Acquisition</b>                 | <b>18</b> |
| Procedure 7.1: Build the Prospecting Engine . . . . .                      | 18        |
| Procedure 7.2: Build the Proposal Generator . . . . .                      | 19        |
| Procedure 7.3: Build the Follow-Up Automation . . . . .                    | 20        |
| <b>MODULE 8: Scaling to \$35K/Month</b>                                    | <b>21</b> |

---

|   |     |
|---|-----|
| <b>Procedure 8.1: Revenue Math</b>              | .21 |
| <b>Procedure 8.2: Hiring Roadmap</b>            | .21 |
| <b>Procedure 8.3: 90-Day Execution Timeline</b> | .21 |

---

This is not a blog post condensed into a PDF. This is an operating system for building an AI compliance and regulatory automation agency that generates \$35,000 per month in recurring revenue. Every module contains executable procedures with exact prompts, configurations, templates, and checklists. If you follow every procedure in order, you will have a fully operational compliance agency with automated delivery pipelines and your first paying client within 90 days.

The AI compliance market is growing at 41% annually. The EU AI Act is fully enforceable. US state-level AI laws are multiplying. And 78% of companies deploying AI have zero compliance infrastructure. This playbook turns that gap into your revenue.

---

## MODULE 1: Regulatory Intelligence Foundation

Your agency's competitive moat is the depth and currency of your regulatory knowledge. This module builds the intelligence infrastructure that powers every client deliverable.

You will build a structured regulatory database covering 15+ jurisdictions, automate regulatory monitoring across 50+ sources, and create a classification engine that instantly determines which regulations apply to any AI system. This module takes 3-5 days to complete and becomes your most valuable internal asset.

### Procedure 1.1: Build the Master Regulatory Database

Open Notion and create a database called "Master Regulatory Database" with these properties:

| Property         | Type         | Description   |
|------------------|--------------|---|
| Regulation Name  | Title        | Official name of regulation   |
| Jurisdiction     | Select       | EU, US-Federal, US-State, UK, Brazil, Canada, Japan, Australia, India, South Korea, Singapore |
| Status           | Select       | Enacted, Proposed, Draft, Under Review, Repealed  |
| Effective Date   | Date         | Compliance deadline   |
| Risk Framework   | Multi-select | Risk-tiered, Risk-based, Sector-specific, Principles-based                                    |
| Affected Sectors | Multi-select | Healthcare, Finance, HR, Legal, Marketing, Education, Government, General                     |
| Key Obligations  | Text         | Summary of compliance requirements  |
| Penalty Maximum  | Text         | Maximum fine or penalty   |
| Source URL       | URL          | Link to official text   |
| Last Verified    | Date         | When you last confirmed accuracy  |
| Impact Score     | Number       | 1-10 scale based on companies affected x severity   |

Populate with these 15 minimum entries:

| #  | Regulation                              | Jurisdiction | Status    | Impact |
|----|---|--------------|-----------|--------|
| 1  | EU AI Act (Regulation 2024/1689)        | EU           | Enacted   | 10     |
| 2  | US Executive Order 14110                | US-Federal   | Enacted   | 8      |
| 3  | Colorado AI Act (SB 24-205)             | US-State     | Enacted   | 6      |
| 4  | NIST AI RMF 1.0                         | US-Federal   | Voluntary | 7      |
| 5  | UK AI Regulation Framework              | UK           | Enacted   | 7      |
| 6  | Brazil AI Regulation (PL 2338/2023)     | Brazil       | Proposed  | 6      |
| 7  | Canada AIDA (Part 3 of C-27)            | Canada       | Proposed  | 5      |
| 8  | Japan AI Guidelines for Business        | Japan        | Enacted   | 4      |
| 9  | South Korea AI Act                      | South Korea  | Proposed  | 5      |
| 10 | Singapore Model AI Governance Framework | Singapore    | Enacted   | 4      |
| 11 | HIPAA AI Provisions                     | US-Federal   | Enacted   | 9      |
| 12 | Fair Lending / ECOA AI Guidance         | US-Federal   | Enacted   | 8      |
| 13 | EEOC AI Hiring Guidance                 | US-Federal   | Enacted   | 7      |
| 14 | Illinois AI Video Interview Act         | US-State     | Enacted   | 5      |
| 15 | NYC Local Law 144 (Bias Audits)         | US-State     | Enacted   | 6      |

### HACK:

When prospecting clients, check their industry against your Impact Score column. Companies in high-impact sectors (healthcare, finance, HR) are 5x more likely to sign compliance retainers because their regulatory exposure is existential. Lead with impact, not features.

## Procedure 1.2: Build the Make.com Regulatory Monitoring Pipeline

Create a Make.com scenario called "Regulatory Intelligence Pipeline" with these modules:

### Module 1: Scheduler Every 6 Hours

```
Cron: 0 */6 * * *
```

### Module 2: HTTP Multi-Feed Fetcher

Configure separate HTTP requests for each regulatory source: EU Official Journal AI section, Federal Register (search: "artificial intelligence"), NIST publications feed, UK ICO guidance updates, State legislature AI bill trackers (via LegiScan API), ICO, CNIL, BfDI enforcement actions

### Module 3: OpenAI Regulatory Update Classifier

```
Model: gpt-4o | System Prompt: "You are an AI regulatory intelligence analyst. For each update, classify as: NEW_REGULATION, AMENDMENT, GUIDANCE, ENFORCEMENT_ACTION, PROPOSED_RULE, or IRRELEVANT. Extract: jurisdiction, affected_sectors, urgency (CRITICAL/HIGH/MEDIUM/LOW), one_sentence_impact, and key_obligation_changes. Return JSON." | Temperature: 0.1
```

### Module 4: Filter Remove Irrelevant Items

```
Condition: classification != "IRRELEVANT"
```

### Module 5: Iterator Process Each Relevant Update

### Module 6: Notion Create/Update Database Entry

```
Database: Master Regulatory Database | Map all extracted fields to database properties
```

### Module 7: Slack Send Alert

```
Channel: #regulatory-alerts | Message: "[{{urgency}}] {{classification}} | {{jurisdiction}} | {{one_sentence_impact}}" | Color: Red for CRITICAL, Orange for HIGH, Yellow for MEDIUM
```

### Module 8: Google Sheets Log to Audit Trail

```
Spreadsheet: Regulatory Change Log | Columns: timestamp, classification, jurisdiction, urgency, source, action_taken
```

## Procedure 1.3: Build the Jurisdiction Applicability Engine

When a client tells you where they operate, you need to instantly know which regulations apply. Build this as a ChatGPT prompt that you reuse for every client:

```
You are an AI regulatory compliance analyst. Given the following company profile, identify ALL applicable AI regulations and their compliance obligations.
```

```
Company Profile:
```

- Headquarters: [country]
- Operations: [list of countries where they have users or employees]
- Industry: [industry]
- AI Systems: [list of AI systems and their purposes]
- Data Types Processed: [personal data, health data, financial data, biometric, etc.]
- Employee Count: [number]
- Annual Revenue: [range]

```
For each applicable regulation, specify:
```

1. Why it applies (nexus analysis)
2. Which AI systems it covers
3. Risk classification for each covered system
4. Specific compliance obligations
5. Compliance deadline
6. Penalty for non-compliance

Organize by priority: regulations with the nearest deadline and highest penalties first.

### Check-In: Module 1 Complete

- Master Regulatory Database created with 15+ entries
- All Impact Scores calculated and verified
- Make.com Regulatory Intelligence Pipeline running every 6 hours
- At least 5 regulatory alerts successfully processed and logged
- Jurisdiction Applicability Engine prompt tested with 3 different company profiles
- Audit trail log in Google Sheets capturing all regulatory changes

## MODULE 2: AI System Inventory & Shadow AI Detection

You cannot assess compliance for AI systems your client does not know about. This module builds the tools to conduct comprehensive AI inventories, detect shadow AI, and classify every system by risk tier. Your inventory deliverable becomes the foundation for all downstream compliance work.

### Procedure 2.1: Create the Client Intake System

Build a Tally.so form called "AI Compliance Intake - [Client Name]" with these sections:

#### Section 1: Organization Profile

| Question                  | Type         | Purpose                                 |
|---------------------------|--------------|---|
| Company legal name        | Short text   | Contract and report generation          |
| Industry                  | Dropdown     | Determines applicable regulations       |
| Headquarters country      | Dropdown     | Determines primary jurisdiction         |
| Countries of operation    | Multi-select | Determines all applicable jurisdictions |
| Number of employees       | Number       | Determines regulatory thresholds        |
| Annual revenue range      | Dropdown     | Determines penalty exposure             |
| Existing compliance team? | Yes/No       | Determines engagement scope             |

#### Section 2: Known AI Systems

| Question                    | Type       | Purpose                     |
|-----------------------------|------------|-----------------------------|
| List all AI/ML tools used   | Long text  | Baseline inventory          |
| Purpose of each tool        | Long text  | Risk classification input   |
| Vendor name for each        | Long text  | Third-party risk assessment |
| Who approved the purchase?  | Short text | Governance maturity signal  |
| How is each tool monitored? | Long text  | Current oversight level     |

### Section 3: Data Processing

| Question                                    | Type         | Purpose                                  |
|---|--------------|--|
| Types of data processed by AI               | Multi-select | Data protection regulation applicability |
| Is personal data of EU residents processed? | Yes/No       | GDPR + EU AI Act nexus                   |
| Is health/medical data processed?           | Yes/No       | HIPAA applicability                      |
| Are automated decisions made about people?  | Yes/No       | High-risk classification trigger         |
| Are there human review processes?           | Yes/No       | Human oversight requirement assessment   |

### Section 4: Current Compliance Posture

| Question  | Type   | Purpose                            |
|---|--------|------------------------------------|
| Has any AI risk assessment been conducted?            | Yes/No | Scope of initial assessment needed |
| Are there documented AI policies?                     | Yes/No | Policy gap analysis                |
| Has the company received regulatory inquiries?        | Yes/No | Urgency indicator                  |
| Are there data processing agreements with AI vendors? | Yes/No | Third-party compliance gaps        |

## Procedure 2.2: Build the Shadow AI Detection Engine

Create a Make.com scenario called "Shadow AI Detector":

### Module 1: Webhook - Receive Client Profile

```
Method: POST
Expected data: { "industry": "string", "employee_count": number, "known_tools": ["array"], "departments": ["array"] }
```

## Module 2: OpenAI - Predict Shadow AI

```
Model: gpt-4o
System Prompt: "You are an AI governance consultant specializing in shadow AI detection. Based on the company's industry, size, known tools, and departments, predict the 10-15 most likely shadow AI tools that employees are using without IT approval. For each prediction, provide: tool_name, category (content_generation, data_analysis, communication, productivity, image_generation), likelihood (HIGH/MEDIUM/LOW), risk_tier under EU AI Act, and reasoning. Return as JSON array."
Temperature: 0.3
```

## Module 3: Notion - Create Shadow AI Assessment

```
Database: Client Name / Shadow AI Assessment
Map: tool_name, category, likelihood, risk_tier, reasoning, verification_status
(default: "PENDING")
```

## Procedure 2.3: Build the Risk Classification Engine

For every AI system in the inventory (known + shadow), classify it under the EU AI Act four-tier framework:

```
You are an EU AI Act classification specialist. Classify the following AI system according to the EU AI Act's four-tier risk model.

AI System: [system_name]
Purpose: [purpose]
Sector: [sector]
Data Processed: [data_types]
Decision Autonomy: [fully_automated / human_in_loop / decision_support / advisory]
Impact on Individuals: [describe how AI output affects people]
Scale: [how many people are affected]

Classification Framework:
- UNACCEPTABLE (Article 5): Social scoring by governments, real-time remote biometric identification in public spaces (with exceptions), manipulation of vulnerable groups
- HIGH-RISK (Articles 6-7): AI used in critical infrastructure, education access, employment/HR, essential services, law enforcement, migration/asylum, justice/democratic processes
- LIMITED (Article 52): Chatbots, emotion recognition, biometric categorization, deepfake generators
- MINIMAL: All other AI systems

Provide:
1. Classification: [tier]
2. Applicable Articles: [list]
3. Reasoning: [3-5 sentences]
4. Compliance Obligations Summary: [bullet list]
5. Similar Classified Examples: [2-3 examples]
6. Uncertainty Flags: [any ambiguous classification issues]
```

**HACK:**

Always present risk classifications to clients with a "confidence level" (High/Medium/Low). This protects you from liability if a regulator later classifies a system differently. Document your reasoning in the audit trail. Clients respect transparency about uncertainty more than false certainty.

### Check-In: Module 2 Complete

- Tally intake form created and tested with sample data
- Shadow AI Detector scenario producing predictions for test profiles
- Risk Classification Engine prompt tested with 10+ different AI system types
- Classification results include all 6 required output fields
- Notion client workspace template includes inventory and shadow AI databases

## MODULE 3: Compliance Gap Analysis & Reporting

The gap analysis is your primary client deliverable and your biggest revenue generator. This module builds the automated engine that takes an AI inventory and produces a professional, audit-ready compliance gap report in under 2 hours instead of the industry standard 40-60 hours.

### Procedure 3.1: Build the Three-Prompt Gap Analysis Chain

#### Prompt A - Risk Classification (per system):

```
Classify [system_name] under the EU AI Act and identify all applicable regulations.
```

```
System details:
```

- Name: [system\_name]
- Purpose: [purpose]
- Sector: [sector]
- Data processed: [data\_types]
- Decision type: [decision\_autonomy]
- User impact: [impact\_description]
- Operating jurisdictions: [jurisdictions]

```
Output:
```

1. EU AI Act risk tier with article references
2. All applicable regulations (beyond EU AI Act)
3. Risk classification under each applicable regulation
4. Confidence level and uncertainty flags

#### Prompt B - Obligation Mapping (per system):

```
For [system_name], classified as [risk_tier] under the EU AI Act, map ALL compliance obligations across applicable regulations:
```

1. EU AI Act obligations:

- [List obligations specific to the risk tier with article references]

2. [Additional regulation] obligations:

- [List obligations with section references]

For each obligation, specify:

- Obligation text (what must be done)
- Current status: COMPLIANT, PARTIALLY\_COMPLIANT, NON-COMPLIANT, or UNKNOWN
- Gap description: [specifically what is missing]
- Gap severity: CRITICAL, HIGH, MEDIUM, LOW
- Remediation approach: [2-3 sentence description]
- Estimated remediation effort: [hours/days]
- Evidence required for compliance: [what documentation is needed]

### **Prompt C - Report Synthesis:**

Synthesize the following compliance analysis into a professional gap report for [client\_name].

**EXECUTIVE SUMMARY:**

Write 3-5 paragraphs for C-suite readers. Cover: overall compliance posture, highest-priority risks, potential penalty exposure, and recommended investment in remediation. Be specific with numbers.

**RISK HEAT MAP:**

Categorize all identified gaps into a priority matrix:

- CRITICAL + URGENT: Gaps that could result in enforcement action within 90 days
- CRITICAL + NOT URGENT: Gaps that are serious but have longer compliance timelines
- HIGH: Significant compliance gaps requiring remediation within 6 months
- MEDIUM: Gaps that should be addressed within 12 months
- LOW: Best practice improvements with no immediate regulatory risk

**DETAILED FINDINGS:**

For each AI system, present:

- System overview
- Risk classification
- Compliance obligations
- Identified gaps
- Recommended remediation

**PRIORITIZED REMEDIATION ROADMAP:**

Organize by quarter:

- Q1: Critical and urgent gaps
- Q2: High-priority gaps
- Q3: Medium-priority gaps
- Q4: Low-priority and best-practice improvements

**ESTIMATED COSTS:**

Provide a table with:

| Category | Internal Cost | External Cost | Total |

Include rows for: Technology, Personnel, Legal Review, Training, Ongoing Monitoring

Analysis data: [paste all Prompt A and B outputs]

Write for a non-technical executive audience. Use specific numbers. Be direct about

risks.

## Procedure 3.2: Build the Make.com Gap Analysis Automation

Create a scenario called "Compliance Gap Analysis Engine":

### Module 1: Google Sheets Read AI Inventory

Spreadsheet: Client Name / AI System Inventory | Range: All rows

### Module 2: Iterator Process Each System

### Module 3: OpenAI Run Prompt A (Risk Classification)

Model: gpt-4o | Temperature: 0.1 | Max tokens: 1000

### Module 4: OpenAI Run Prompt B (Obligation Mapping)

Model: gpt-4o | Temperature: 0.1 | Max tokens: 2000 | Input: Module 3 classification + Module 1 inventory data

### Module 5: Text Aggregator Combine All System Analyses

Source: All Module 4 outputs | Separator: "\n\n---\n\n"

### Module 6: OpenAI Run Prompt C (Report Synthesis)

Model: gpt-4o | Temperature: 0.2 | Max tokens: 5000 | Input: Module 5 aggregated analysis

### Module 7: Google Docs Create Gap Report

Title: "[Client Name] - AI Compliance Gap Report - [Date]" | Content: Module 6 output, formatted with proper headings

### Module 8: Google Drive Move to Client Folder

Destination: Client Name / Deliverables / Gap Analysis/

### Module 9: Notion Update Client Dashboard

Update: compliance\_score, last\_assessment\_date

### Module 10: Slack Notify Team

Channel: #client-[name] | Message: "Gap analysis complete for [client\_name]. [X] critical gaps identified. Report: [link]"

## Procedure 3.3: Create the Gap Report Quality Checklist

Before delivering any automated report to a client, verify:

---

**Classification Accuracy:** Are risk tiers correctly assigned? Cross-check high-risk classifications against EU AI Act Annex III

**Obligation Completeness:** Did the AI miss any applicable regulations? Check against your Jurisdiction Applicability Engine output

**Gap Severity Calibration:** Are severity ratings consistent? A missing human oversight mechanism for a high-risk system must be CRITICAL, not HIGH

**Remediation Feasibility:** Can the recommended remediation actually be implemented in the suggested timeline?

**Executive Readability:** Would a non-technical CEO understand the risk and the business case for remediation?

**No False Positives:** Are there gaps flagged that are not actually gaps? Over-reporting damages credibility

**No False Negatives:** Are there gaps the AI missed? Under-reporting creates liability

**HACK:**

Always add a "Compliance Officer's Note" at the beginning of every gap report that says: "This analysis was generated using AI-assisted compliance scanning tools and reviewed by [your name], AI Compliance Specialist. While comprehensive, this report does not constitute legal advice and should be reviewed by qualified legal counsel before making compliance decisions." This disclaimer is essential for liability protection.

**Check-In: Module 3 Complete**

- Three-prompt chain tested with 5+ different AI systems
- Make.com Gap Analysis Engine running end-to-end
- Google Docs reports generating with proper formatting
- Quality checklist applied to at least 3 test reports
- Compliance Officer's Note added to report template
- Average report generation time under 2 hours

---

## **MODULE 4: Remediation & Automation Build**

Identifying gaps is only half the job. This module builds the remediation delivery system - the Make.com workflows, documentation templates, and implementation procedures that actually close compliance gaps and create the recurring monitoring infrastructure clients pay retainers for.

### **Procedure 4.1: Build the Audit Trail Automation**

Every compliance action must be documented. Create a Make.com scenario called "Audit Trail Generator":

#### **Module 1: Webhook - Receive Audit Event**

```
Method: POST
```

```
Data: { "client": "string", "system": "string", "action": "string", "user": "string",  
"evidence_url": "string" }
```

## Module 2: Notion - Create Audit Log Entry

```
Database: Client Name / Audit Trail
```

```
Properties: timestamp (now), client, system, action, user, evidence_url,  
verification_status ("PENDING")
```

## Module 3: Google Sheets - Append to Compliance Log

```
Spreadsheet: Client Name / Compliance Log
```

```
Row: [timestamp, system, action, status, evidence_link]
```

# Procedure 4.2: Build the Human Oversight Mechanism Templates

For high-risk AI systems, the EU AI Act requires documented human oversight. Create these templates:

## Human Oversight Protocol Template:

```
HUMAN OVERSIGHT PROTOCOL
```

```
System: [system_name]
```

```
Risk Tier: HIGH-RISK
```

```
Regulation: EU AI Act, Article 14
```

### 1. DESIGNATED OVERSEERS

- Primary: [Name, Title]
- Secondary: [Name, Title]
- Qualifications: [Training required for overseers]

### 2. MONITORING SCHEDULE

- Real-time monitoring: [Yes/No, for what decisions]
- Daily review: [What outputs to review]
- Weekly assessment: [Performance metrics to check]
- Monthly audit: [Full system review]

### 3. OVERRIDE PROCEDURES

- When to override: [Specific conditions]
- Override process: [Step-by-step]
- Documentation required: [What to record]
- Escalation path: [Who to notify]

### 4. INTERVENTION TRIGGERS

- Accuracy drops below [threshold]
- Bias metrics exceed [threshold]
- System generates unexpected outputs
- Stakeholder complaints received
- Regulatory changes affect classification

### 5. RECORD-KEEPING

- All override actions logged in: [Audit trail system]
- Monthly oversight reports due: [Date]
- Annual oversight review: [Date]

---

## Procedure 4.3: Build the Bias Monitoring Dashboard

Create a Notion dashboard that tracks bias metrics for high-risk AI systems:

### Dashboard Properties:

| Property        | Type    | Purpose   |
|-----------------|---------|---|
| System Name     | Title   | AI system identifier  |
| Metric          | Select  | Demographic parity, equalized odds, disparate impact, calibration |
| Protected Class | Select  | Race, Gender, Age, Disability, Religion, National Origin          |
| Current Value   | Number  | Latest measurement  |
| Threshold       | Number  | Acceptable limit  |
| Status          | Formula | GREEN (within threshold), YELLOW (approaching), RED (exceeded)    |
| Last Measured   | Date    | Most recent assessment  |
| Next Assessment | Date    | Scheduled follow-up   |
| Remediation     | Text    | Action if threshold exceeded                                      |

#### **HACK:**

For clients in NYC, NYC Local Law 144 requires annual bias audits for automated employment decision tools. Build this as a standalone service (\$2,500-\$5,000 per audit) that serves as a low-cost entry point to upsell your full compliance retainer.

### Check-In: Module 4 Complete

- Audit Trail Generator scenario operational
- Human Oversight Protocol template created and customizable per system
- Bias Monitoring Dashboard template built in Notion
- At least 3 test audit events logged successfully
- Override procedure template reviewed for legal adequacy

---

## MODULE 5: Client Dashboard & Monitoring System

---

Your retainer clients need ongoing visibility into their compliance status. This module builds the client-facing dashboard and the automated monitoring workflows that justify monthly retainers of \$2,000-\$8,000.

## Procedure 5.1: Build the Client Compliance Dashboard

Create a Notion template for client dashboards with these components:

### Section 1: Compliance Score Card

COMPLIANCE SCORE: [X]%

Breakdown:

- Technical Documentation: [X]% complete
- Human Oversight: [X]% implemented
- Bias Monitoring: [X]% active
- Regulatory Tracking: [X]% current
- Audit Readiness: [X]% prepared

Last Updated: [Date]

Next Review: [Date]

### Section 2: AI Systems Registry

A database view with columns: System Name, Risk Tier, Compliance Status (GREEN/YELLOW/RED), Owner, Last Assessment, Next Review

### Section 3: Obligations Tracker

A database of all compliance obligations with columns: Obligation, Regulation, Deadline, Status (Complete/In Progress/Not Started/Overdue), Evidence Link, Notes

### Section 4: Regulatory Alerts Feed

Auto-populated by Make.com - shows the latest regulatory changes that affect the client's AI systems

### Section 5: Audit Trail

Chronological log of all compliance actions, auto-populated by the Audit Trail Generator

## Procedure 5.2: Build the Monthly Monitoring Make.com Scenario

Create a scenario called "Monthly Compliance Monitor":

### Module 1: Schedule First Monday of Every Month

```
Cron: 0 9 1-7 * 1
```

### Module 2: Notion Query All Client Obligations

```
Database: [Client Name] / Obligations Tracker
Filter: Deadline < now() + 30 days AND Status != "Complete"
```

### Module 3: Notion Calculate Compliance Score

```
Query: All obligations for client
Calculate: (Complete / Total) x 100
Update: Dashboard compliance score
```

### Module 4: OpenAI Generate Monthly Summary

```
Model: gpt-4o
System: "Generate a professional monthly compliance summary for [client_name]. Include:
compliance score trend, upcoming deadlines, new regulatory alerts, and recommended
actions. Be specific and actionable. Write for an executive audience."
User: "[Compliance score data from Module 3] + [Upcoming deadlines from Module 2] +
[Recent regulatory alerts]"
Temperature: 0.2
```

### Module 5: Google Docs Create Monthly Report

```
Title: "[Client Name] - Monthly Compliance Summary - [Month Year]"
Content: Module 4 output
```

### Module 6: Slack Send to Client Channel

```
Channel: #client-[name]
Message: "Monthly compliance summary ready. Score: [X]%. [Y] deadlines this month.
Report: [link]"
```

## Procedure 5.3: Build the Quarterly Review Package

Every quarter, retainer clients receive a comprehensive compliance review. Build this as an automated deliverable:

1. Updated compliance score with trend analysis
2. New regulatory changes and their impact on client AI systems
3. Risk reassessment for any new AI systems deployed since last review
4. Updated gap analysis (re-run Gap Analysis Engine with current data)
5. Updated remediation roadmap with progress tracking
6. Audit readiness assessment (how prepared is the client for a regulatory inspection?)
7. Recommendations for the next quarter

Use the Make.com Gap Analysis Engine from Module 3 to re-run analyses quarterly, comparing current results against the previous quarter to show progress.

### Check-In: Module 5 Complete

- Client dashboard template built in Notion with all 5 sections
- Monthly Compliance Monitor scenario running on schedule

- ☐ Monthly summary reports generating automatically
- ☐ Quarterly review package template created
- ☐ Compliance score calculation verified manually against sample data

## MODULE 6: Audit Documentation & Preparation

When regulators arrive, your clients need organized, comprehensive documentation. This module builds the system that generates audit-ready documentation packages on demand - a premium service that clients pay extra for and that dramatically increases retention rates.

### Procedure 6.1: Build the Audit Package Generator

Create a Make.com scenario called "Audit Documentation Generator":

#### Module 1: Webhook Trigger Generation

```
Data: { "client": "string", "system": "string", "regulation": "string" }
```

#### Module 2: Notion Fetch All System Data

Databases to query:

- AI Systems Registry (system details, risk classification)
- Obligations Tracker (compliance status per obligation)
- Audit Trail (all logged compliance actions)
- Bias Monitoring Dashboard (latest metrics)

#### Module 3: OpenAI Generate Documentation Package

```
Model: gpt-4o  
System Prompt: "Generate a complete audit documentation package for [system_name] under [regulation]. Include: System Description, Technical Documentation, Risk Management Documentation, Quality Management Documentation, Human Oversight Documentation, Transparency Documentation, Post-Market Monitoring Plan. Use all available data to make the documentation specific and evidence-based."  
Temperature: 0.1  
Max tokens: 8000
```

#### Module 4: Google Docs Create Audit Package

```
Title: "[System Name] - Compliance Documentation Package - [Date]"  
Apply formatting: Professional document styles, table of contents, page numbers
```

#### Module 5: Google Drive File in Client Folder

```
Destination: Client Name / Audit Documentation / [System Name] / [Date]/
```

### Procedure 6.2: Build the Audit Readiness Checklist

For each client, maintain an audit readiness score based on:

| Category                    | Weight | Criteria  |
|-----------------------------|--------|---|
| Technical Documentation     | 20%    | Complete for all high-risk systems                |
| Human Oversight Records     | 15%    | Documented for all high-risk systems              |
| Bias Monitoring Active      | 15%    | Regular assessments for all high-risk systems     |
| Regulatory Tracking Current | 15%    | All applicable regulations identified and tracked |
| Audit Trail Complete        | 15%    | All compliance actions logged with evidence       |
| Training Records            | 10%    | All overseers trained and documented              |
| Incident Response Plan      | 10%    | Documented and tested                             |

Generate the readiness score automatically in the client dashboard using a Notion formula that weights each category.

### Check-In: Module 6 Complete

- Audit Documentation Generator scenario producing complete packages
- Generated packages reviewed for completeness against EU AI Act requirements
- Audit readiness checklist implemented in client dashboard
- Readiness score auto-calculating correctly
- Test package generated for a sample high-risk AI system

## MODULE 7: Sales, Proposals & Client Acquisition

The best compliance infrastructure in the world is worthless without clients. This module builds your sales system - from prospecting to proposal to close - with automated tools that reduce your sales cycle from months to weeks.

### Procedure 7.1: Build the Prospecting Engine

Create a Make.com scenario called "Compliance Prospecting Engine":

#### Module 1: HTTP - Scrape Job Postings

```
URL: LinkedIn Jobs search for "AI compliance" OR "AI governance" OR "AI risk"  
Purpose: Companies hiring these roles are investing in compliance - prime prospects
```

## Module 2: OpenAI - Score and Categorize Prospects

```
Model: gpt-4o
System: "Score this company as a compliance agency prospect. Consider: industry risk (healthcare/finance/HR = high), company size (100-2000 employees = ideal), AI tool usage indicators, geographic exposure (EU operations = urgent). Return: prospect_score (1-10), primary_risk, recommended_outreach_angle, estimated_deal_value."
Temperature: 0.2
```

## Module 3: Google Sheets - Add to Prospect Pipeline

```
Spreadsheet: Sales Pipeline
Columns: company_name, industry, size, prospect_score, primary_risk, outreach_angle, estimated_value, status, last_contact, next_action
```

## Procedure 7.2: Build the Proposal Generator

Create a Google Docs proposal template with merge fields:

```
[CLIENT_NAME] - AI Compliance & Regulatory Automation Proposal

EXECUTIVE SUMMARY
[Generated per client using OpenAI]

YOUR COMPLIANCE LANDSCAPE
- AI Systems Identified: [estimated_count] (including shadow AI)
- High-Risk Systems: [estimated_count]
- Applicable Regulations: [list]
- Estimated Penalty Exposure: [calculated based on revenue and violations]

RECOMMENDED ENGAGEMENT

Phase 1: Discovery & Inventory - $3,500
- Complete AI system inventory including shadow AI detection
- Risk classification for all identified systems
- Applicable regulation mapping

Phase 2: Gap Analysis & Roadmap - $4,000-$7,500
- Comprehensive compliance gap report
- Prioritized remediation roadmap
- Cost estimates for remediation activities

Phase 3: Remediation & Automation - $5,000-$12,000
- Implementation of compliance automation workflows
- Audit documentation generation
- Human oversight mechanism design
- Bias monitoring setup

Phase 4: Ongoing Monitoring - $2,000-$8,000/month
- Regulatory change monitoring and alerts
- Monthly compliance summaries
- Quarterly compliance reviews
- On-demand advisory support
- Annual audit readiness assessment
```

| Phase            | Investment         | Timeline  |
|------------------|--------------------|-----------|
| Discovery        | \$3,500            | Weeks 1-2 |
| Gap Analysis     | \$4,000-\$7,500    | Weeks 2-3 |
| Remediation      | \$5,000-\$12,000   | Weeks 3-6 |
| Monthly Retainer | \$2,000-\$8,000/mo | Ongoing   |

### HACK:

Always present pricing as an "investment" not a "cost." Frame compliance spending against potential penalties. For a \$50M revenue company, a \$35,000 compliance engagement is 0.07% of revenue - compared to a potential 35M euro fine which is 70% of revenue. That is a 1,000x return on compliance investment. Put this comparison in every proposal.

## Procedure 7.3: Build the Follow-Up Automation

Create a Make.com scenario for prospect follow-up:

**Module 1: Schedule** Every Monday 9 AM

**Module 2: Google Sheets** Find Prospects Needing Follow-Up

```
Filter: status = "PROPOSAL_SENT" AND last_contact < now() - 7 days
```

**Module 3: OpenAI** Draft Follow-Up Email

```
System: "Write a brief, professional follow-up email for a compliance agency proposal. Reference the prospect's specific compliance risks. No filler. Maximum 150 words. End with a specific call-to-action."
```

**Module 4: Gmail** Send Follow-Up

```
To: [prospect_email]
Subject: "Following up - [Client Name] compliance proposal"
Body: Module 3 output
```

### Check-In: Module 7 Complete

- Prospecting Engine scenario identifying and scoring leads
- Proposal template created with all merge fields
- At least 3 test proposals generated for different company profiles
- Follow-up automation running weekly
- Sales pipeline spreadsheet tracking all prospects

## MODULE 8: Scaling to \$35K/Month

This module maps the exact path from your first client to \$35,000 in monthly recurring revenue. The math is straightforward: you need 8-12 clients on retainers averaging \$3,000-\$4,000/month, plus project revenue from new client onboarding.

### Procedure 8.1: Revenue Math

| Revenue Stream                             | Target             | Monthly Revenue |
|--|--------------------|-----------------|
| Starter Retainer Clients (3 x \$2,000)     | 3 clients          | \$6,000         |
| Growth Retainer Clients (4 x \$4,500)      | 4 clients          | \$18,000        |
| Enterprise Retainer Clients (1 x \$8,000)  | 1 client           | \$8,000         |
| New Client Onboarding Projects (1-2/month) | 1.5 avg            | \$5,250         |
| Audit Documentation Packages (2-3/month)   | 2.5 avg            | \$2,500         |
| <b>TOTAL</b>                               | <b>~10 clients</b> | <b>\$39,750</b> |

### Procedure 8.2: Hiring Roadmap

| Revenue Milestone | Hire                      | Salary                  | Purpose                    |
|-------------------|---------------------------|-------------------------|----------------------------|
| \$10K MRR         | Junior Compliance Analyst | \$50K/year              | Day-to-day client delivery |
| \$20K MRR         | Sales/BD Specialist       | \$60K/year + commission | Client acquisition         |
| \$30K MRR         | Senior Compliance Analyst | \$80K/year              | Enterprise client delivery |
| \$40K MRR         | Technical Lead            | \$90K/year              | SaaS product development   |

### Procedure 8.3: 90-Day Execution Timeline

| Week | Focus | Action   | Outcome                    |
|------|-------|--|----------------------------|
| 1-2  | Build | Complete Modules 1-3 (database, inventory, gap analysis)         | Delivery stack operational |
| 3-4  | Build | Complete Modules 4-6 (remediation, dashboards, audit docs)       | Full service capability    |
| 5-6  | Sell  | Complete Module 7, launch LinkedIn content, send first proposals | 5+ prospects in pipeline   |

|       |         |   |                                    |
|-------|---------|---|------------------------------------|
| 7-8   | Sell    | Follow-up automation, partner outreach, conference applications     | 10+ prospects, 2 proposals out     |
| 9-10  | Deliver | First client onboarded, delivering gap analysis                     | \$3,500-\$7,000 project revenue    |
| 11-12 | Scale   | First retainer active, second client onboarding, analyst job posted | \$5,000+ MRR, hiring pipeline open |
| 13+   | Grow    | Systematic client acquisition, SaaS MVP planning                    | \$10K to \$20K to \$35K MRR        |

### Final Verification: Complete System Checklist

- Master Regulatory Database with 15+ entries, updated every 6 hours
- Regulatory Intelligence Pipeline running automatically
- Client Intake System (Tally form + Shadow AI Detector)
- Risk Classification Engine producing accurate tier assignments
- Gap Analysis Engine generating reports in under 2 hours
- Quality checklist applied to every report before delivery
- Audit Trail Generator logging all compliance actions
- Human Oversight Protocol templates for high-risk systems
- Bias Monitoring Dashboard template
- Client Compliance Dashboard template with auto-updating scores
- Monthly Compliance Monitor scenario running on schedule
- Quarterly Review Package template
- Audit Documentation Generator producing complete packages
- Audit Readiness Score calculating automatically
- Prospecting Engine identifying and scoring leads
- Proposal template with client-specific merge fields
- Follow-up automation running weekly
- Sales pipeline spreadsheet tracking all activity
- Revenue targets mapped with client acquisition goals
- Hiring roadmap documented with salary ranges