

Babak Bandpey

Senior Freelance Software Engineer / Security & GRC Specialist

bb@cocode.dk +45 27 82 30 77 <https://cocode.dk> LinkedIn GitHub

Summary

I design and build systems that remove manual work and make security and compliance work in real organizations. I genuinely love what I do and I take pride in building things that actually hold up in practice.

I built FITS after watching skilled colleagues work late every day producing the same compliance outputs again and again. Surveys were corrected by hand. Hundreds of pages were reviewed manually. The work was slow, error-prone, and exhausting. It was clear to me that this was not a people problem but a system failure, so I automated it. The results were faster, more consistent, and strong enough that others wanted to invest in what I had built.

I see system design and automation as a craft. It takes patience, resilience, and intelligence to turn messy reality into something reliable. Today I help organizations operationalize security, compliance, and AI into production-grade systems that deliver measurable results. I am known as the person who works until the job is done and actually delivers.

I constantly study new technology and push my own limits with one goal: to build solutions that stand on their own and free clients from manual processes and long-term expert dependency. I want people to understand, use, and trust the systems I leave behind.

A product matters if it survives contact with reality.

Experience

Senior Freelance Software Engineer / Security & GRC Specialist

cocode.dk

Copenhagen, Denmark 2025-01 - Present

Independent consultancy providing senior software engineering and security expertise. Focus on outcome-driven delivery with heavy personal ownership.

FITS - AI-Driven GRC Platform

Production-grade GRC / security program management platform used by real organizations. Functions as GRC automation engine, CMDB-like system, and assessment/reporting factory.

Python, Django, PostgreSQL, Neo4j, Redis, TypeScript, React, Tailwind, pgvector, OpenAI / Azure AI, Atlassian Confluence, Jira

- AI-generated security questionnaires
- Policy-aware evaluation of answers
- Automated scoring and assessments
- KPI-rich reporting for CISOs, auditors, and executives
- Reduced assessment turnaround from ~3 weeks to < 48 hours
- Reduced manual review effort by ~75%
- Multi-tenant architecture, operated as single-tenant per customer
- Strong data isolation and compliance alignment

Archer at Nuuday A/S <https://nuuday.dk>

RSA Archer - Nuuday Worked with RSA Archer as the core GRC platform at Nuuday to manage risk, control frameworks, and compliance assessments.

Focused on operationalizing ISO 27001-aligned requirements, running structured assessments, tracking remediation, and producing management and audit-ready reporting, ensuring Archer reflected real operational risk and security status rather than static compliance documentation.

Python, Django, PostgreSQL, Neo4j, Redis, REST APIs, JSON, SQL, React, TypeScript, Tailwind CSS, OpenAI/Azure AI integrations, Jira, Confluence, RSA Archer, ISO 27001 frameworks, CIS Controls frameworks, CMDB principles, risk assessment tooling, policy & control libraries, audit reporting tools

- Planned and executed large-scale gap assessments across business-critical applications
- Conducted structured interviews with system owners, product owners, and technical stakeholders
- Interpreted policies, standards, and regulatory requirements into assessable control questions
- Evaluated control design and operating effectiveness, not just documentation presence
- Identified gaps, weaknesses, and systemic patterns across applications and domains
- Documented findings with clear severity, rationale, and remediation guidance
- Created management-ready assessment reports for security, risk, and executive audiences
- Designed and maintained KPI frameworks covering compliance level, control health, and progress
- Built dashboards tracking assessment completion, remediation status, and maturity trends
- Enabled longitudinal tracking of improvement instead of one-off assessments
- Fed assessment results directly into automated remediation and follow-up workflows
- Reduced manual coordination by enforcing ownership, deadlines, and traceability
- Acted as the bridge between policy intent, technical reality, and management decisions

Archer at Nuuday A/S <https://nuuday.dk>

RSA Archer - Nuuday Worked with RSA Archer as the core GRC platform at Nuuday to manage risk, control frameworks, and compliance assessments. Focused on operationalizing ISO 27001-aligned requirements, running structured assessments, tracking remediation, and producing management and audit-ready reporting, ensuring Archer reflected real operational risk and security status across business-critical systems.

Python, Django, PostgreSQL, Neo4j, Redis, REST APIs, JSON, SQL, React, TypeScript, Tailwind CSS, OpenAI/Azure AI integrations, Jira, Confluence, RSA Archer, ISO 27001 frameworks, CIS Controls frameworks, CMDB principles, risk assessment tooling, policy & control libraries, audit reporting tools

- Centralized management of enterprise risks, controls, and compliance obligations
- Strong support for ISO 27001-aligned risk and control frameworks
- Structured assessment workflows with traceable findings and ownership
- Built-in remediation and issue tracking for audit follow-up
- Audit-ready reporting and dashboards for management and regulators
- Clear traceability from policy → risk → control → finding → remediation

System Developer

Others

Copenhagen Denmark 2000-12 - 2018-12

20 years of experience with the LAMP stack, specializing in web applications and high-traffic sites. Skilled in PHP frameworks, backend logic, database design, and system integration. Created webshops in high-availability environments, transitioning to modern Python-based and AI-driven platforms.

Skills

AI/ML

AI Evaluation & Scoring Logic AI-assisted Assessment Generation

Embedding & Retrieval (RAG) LLM Integration (OpenAI / Azure AI)

Policy-aware AI Workflows Prompt & System Design

Android app development

Kotlin

Architecture

Closed-circuit / Local Deployments Data-driven KPI Systems

End-to-end System Architecture Scalable Compliance Platforms

Security-by-design Architecture

Backend

Backend Architecture Business Logic Modeling Django Flask

Multi-tenant Systems REST API Design Single-tenant Secure Deployments

Workflow Automation

Consulting

Client Advisory (CISO / Security Teams) Independent Delivery & Accountability

Product Vision & Roadmap Ownership Requirements Translation (Business → System)

Technical Leadership

Databases

Graph-based Data Modeling Neo4j (Graph DB) pgvector / Vector Search

PostgreSQL Redis Relational Data Modeling

DevOps

CI/CD

DevOps/Cloud

CI/CD Pipelines DigitalOcean Infrastructure as Code Secure System Deployment

Single-tenant Isolation Strategies

Frontend

React Tailwind CSS Vite Vue.js

Integrations

Atlassian Confluence (Automation & Publishing) Excel-based Reporting Automation

Jira Integration Microsoft / Azure Ecosystem

PHP Framework

Laravel Symfony Yii

Programming Languages

C# JavaScript Node.js PHP Python ReactJS SQL TypeScript

Security/GRC

Audit Support & Reporting CIS Controls / CIS18 Operationalization

CMDB & Asset Dependency Modeling Gap Analysis GRC Process Automation

ISO 27001 / ISMS Implementation Risk Modeling & Assessment

Vulnerability Triage & Mitigation Coordination

Software Development

Debugging

Testing

Integration Test Unit Test

Testing and QA

Code Rabbit

Vibe Coding

Claude CLI Codex

Vide Coding

Cursor