kapaciti

COMPLIANCE

Kapaciti Master Compliance Roadmap

Hederlig genomgång av allt vi måste, bör och kan certifieras mot. Sorterat efter tvång.

KAPACITI AB
SKELLEFTEÅ · STOCKHOLM · GÖTEBORG
KAPACITI.SE · ALEX@KAPACITI.SE

2026-05-13

INNEHÅLL

Kapaciti Master Compliance Roadmap

Hederlig genomgång av allt vi måste, bör och kan certifieras mot. Sorterat efter tvång.

Datum: 2026-05-12

TL;DR

Det finns tre tier av compliance-krav:

Tier 1 (lagkrav eller deal-blocking i 95% av RFPs): EU AI Act, GDPR, ISO 27001, ISO 42001
Tier 2 (sektor-blocking eller internationellt-blocking): DORA, SOC 2, AML5/6
Tier 3 (signal-värdig, ej blocking): NIST AI RMF, ISAE 3402, CSA STAR

Vi har **0 av 10** klart idag. Vi behöver minst Tier 1 (4 stycken) inom 18 månader för att vara enterprise-säljbara.

TIER 1: Måste-ha. Antingen lag eller deal-blocking.

1. EU AI Act

Status: Lagkrav, inte certifikat. Compliance krävs för high-risk AI-system från 2026-08-02 (möjligen 2027-12-02 om Digital Omnibus passerar).

Vad det är: Sex obligationer för high-risk AI: risk management, data governance, technical documentation, automatic logging, transparency, human oversight. Plus artikel 50 transparency för limited-risk.

Påverkar Kapaciti:

- Modul `credit-scoring` är direkt high-risk (Annex III 5b)
- Övriga moduler limited eller minimal, context-beroende
- Vi som leverantör måste själv-certifiera enligt Annex VI eller Annex VII

Vad vi har: Audit-chain (artikel 12) live i kod. EU AI Act mapping-research klar (5862 ord). 22-punkts checklista finns som lead-magnet.

Kvarstår: Self-certification per modul, CE-märkning för high-risk, conformity assessment, post-market monitoring (artikel 72), serious incident reporting (artikel 73), FRIA-template (artikel 27).

Tidsplan: Self-cert klart Q3 2026. CE-mark för credit-scoring Q4 2026. Löpande monitoring från Q3 2026.

Kostnad: Internt arbete + extern AI Act-jurist SEK 200-400K under 2026.

Sanktion vid brott: EUR 15 miljoner eller 3% av global omsättning, whichever is higher.

2. GDPR

Status: Lagkrav. I kraft sedan 2018. Inte certifikat.

Vad det är: EU-förordning om personlig data. Förbjuder hantering utan rättslig grund, kräver transparens, ger registrerade rättigheter (åtkomst, radering, dataportabilitet).

Påverkar Kapaciti:

- All kund-data vi hanterar (även B2B-bolag har personal personlig data)
- Modul `gdpr-response` är direkt GDPR-leverantör
- Privacy by design krävs

Vad vi har: Lead-capture API har grundläggande consent. Cal.com-integration har egen GDPR-mapping.

Kvarstår: Formell privacy policy publicerad. DPIA per modul. DPO eller motsvarande utses. DPA (data processing agreement) som mall för kunder. Subprocessor-lista publik. Data deletion-procedur dokumenterad. Cross-border transfer-bedömning (Vercel = USA, Anthropic = USA, etc).

Tidsplan: Privacy policy + DPA-mall Q3 2026. DPIA per modul Q4 2026.

Kostnad: Jurist SEK 100-200K. Internt arbete.

Sanktion vid brott: EUR 20 miljoner eller 4% av global omsättning, whichever is higher.

3. ISO 27001

Status: Frivillig certifiering, men deal-blocking i 95% av enterprise-RFPs.

Vad det är: International standard för information security management system (ISMS). 93 kontroller i Annex A. Audit av extern body.

Påverkar Kapaciti:

- Varje bank, försäkringsbolag, kommun i sin upphandling kräver det
- Utan det blir vi screened-out i RFP-skedet, oavsett produkt-fit
- ISO 27001 är inträdesbiljett, inte särskiljare

Vad vi har: Audit-chain. On-prem-arkitektur (täcker delvis A.13 Communications security, A.14 System acquisition). Self-funded utan dirty term sheets (delvis A.7 Human resources). On-prem-compliance-doc utkast.

Kvarstår: ISMS-policy, risk-register, dokumenterade procedures, incident response, business continuity, supplier assessment, internal audit, management review, stage 1 + stage 2 audit.

Tidsplan: Kickoff Q3 2026. Stage 1 Q1 2027. Stage 2 Q3 2027. Certifierad end Q3 2027.

Kostnad: SEK 200-500K för förstgångs-certifiering (intern arbete + auditor-fee). Sveriges auditorer: BSI Sverige, DNV Sverige, Intertek Sverige, SGS Sverige.

Sanktion vid brott: Ingen lagsanktion. Bara deal-loss.

4. ISO 42001

Status: Frivillig certifiering, blir kund-krav i växande takt. 40% av EU enterprise AI RFPs frågar redan.

Vad det är: International standard för AI management system. Publicerad december 2023. 38 controls i Annex A. Integrerar EU AI Act och NIST AI RMF.

Påverkar Kapaciti:

- Som AI-bolag är detta vår analog till ISO 27001
- Inte harmoniserad under EU AI Act ännu (förväntat 2027)
- Om harmoniserad: certifierade får presumption of conformity för AI Act artikel 17

Vad vi har: Tekniska byggblocken (audit-chain, voice-validator, on-prem). Inget managementsystem.

Kvarstår: AI policy. AI risk register. AI system impact assessment per modul. Change management. Procedures för utveckling, deployment, monitoring. Stage 1 + Stage 2 audit.

Tidsplan: Kickoff Q3 2026 (parallellt med 27001). Stage 1 Q2 2027. Stage 2 Q3 2027. Certifierad end Q3 2027.

Kostnad: SEK 400-750K standalone. SEK 250-350K besparing om integrated audit med 27001. Sveriges auditorer: SGS, TÜV SÜD, Intertek, LRQA.

Sanktion vid brott: Ingen lagsanktion. Deal-loss + svagare AI Act-compliance-position.

TIER 2: Sektor-blocking. Måste för bank-deals eller internationellt.

5. DORA (Digital Operational Resilience Act)

Status: Lagkrav för finansiella entiteter sedan januari 2025. Vi är inte själva en finansiell entitet, men vi BLIR ICT third-party provider när vi säljer till bank.

Vad det är: EU-förordning som kräver att finansiella entiteter har resilient ICT-system. Tredjepartsleverantörer registreras hos Finansinspektionen och kan klassificeras som CTPP (critical third-party provider).

Påverkar Kapaciti:

- Bank-kunder kommer kräva DORA third-party assessment
- Vi måste registreras hos FI
- Om vi blir CTPP är vi under direkt EU-tillsyn

Vad vi har: DORA third-party assessment-utkast (04-dora-third-party-assessment.md) klar. On-prem-arkitektur som gör oss icke-CTPP initialt.

Kvarstår: Formell DPA-mall med bank, exit-strategi-dokumentation, sub-contractor-lista (Vercel, Anthropic, OpenAI, Resend, Supabase), audit-rights-klausul, register-rapportering till bankens FI-koordinator.

Tidsplan: Klart innan första bank-kund.

Kostnad: Bankjurist SEK 50-150K.

Sanktion vid brott: Banken kan inte använda oss. Inte direkt-sanktion mot oss.

6. SOC 2 Type II

Status: Frivillig, men deal-blocking för internationella kunder och vissa svenska enterprise.

Vad det är: Amerikansk audit-standard från AICPA. Fem trust criteria: security, availability, processing integrity, confidentiality, privacy. Type II innebär audit över 6-12 månader, inte bara point-in-time.

Påverkar Kapaciti:

- Inte deal-blocking i Sverige (27001 räcker oftast)
- Deal-blocking för USA, UK, finanssektor internationellt
- Lägre prio än 27001 + 42001 för vår nordiska target-marknad

Vad vi har: Inget. Tekniska byggblocken delvis (audit-chain, on-prem) men inget formellt.

Kvarstår: Allt. SOC 2 är mer kontinuerligt än ISO. Kräver 6-månaders observationsperiod.

Tidsplan: Inte prio 2026. Q2 2028 om vi går mot UK/USA-marknad.

Kostnad: SEK 400-800K första audit.

Alternativ: ISAE 3402 (svensk/europeisk variant av SOC 2 för outsourcing) är ofta accepterat istället. Mer attainable för nordiskt bolag.

7. AML5 och AML6

Status: Lagkrav. AML5 i kraft. AML6 implementeras 2026-2027.

Vad det är: EU-direktiv om penningtvätt och terrorfinansiering. Kräver kundkännedom, transaktionsövervakning, suspicious activity reporting.

Påverkar Kapaciti:

- Vi är inte själva finansiell entitet, men vi BYGGER aml-screening-modul som ska användas av finansiella entiteter
- Vår produkt måste stödja bankens AML-compliance
- Inte ett certifikat, mer produkt-kapabilitet

Vad vi har: aml-screening är planerad modul, inte byggd. Mapping-research nämner den.

Kvarstår: Bygg aml-screening-modulen. Validera mot EBA-guidance. Dokumentera EBA fraud-undantag för limited-risk-klassificering.

Tidsplan: Modul klar Q4 2026 om bank-pilot kräver det.

Kostnad: Utvecklingsarbete + AML-konsult SEK 100-200K för validering.

TIER 3: Signal-värdig. Inte blocking, men stärker position.

8. NIST AI RMF (AI Risk Management Framework)

Status: Frivillig referens-framework från USA. Inte certifikat.

Vad det är: AI risk management framework från US National Institute of Standards and Technology. Bra grund för att strukturera AI-risk-arbete.

Påverkar Kapaciti:

- Refererad i ISO 42001
- US-kunder uppskattar
- Hjälper strukturera vårt eget AI-risk-arbete

Vad vi har: Inget formellt, men EU AI Act mapping-research följer liknande logik.

Kvarstår: Adoptera som intern referens. Inte audit-bart.

Tidsplan: Q3 2026 parallellt med ISO 42001-arbete.

Kostnad: Internt arbete, ingen audit.

9. ISAE 3402

Status: Frivillig audit-standard för outsourcing-tjänster. Europeisk alternativ till SOC 2.

Vad det är: International Standard on Assurance Engagements för outsourcing. Type I (point-in-time) eller Type II (kontinuerligt).

Påverkar Kapaciti:

- Accepteras av svenska banker istället för SOC 2
- Mindre känd internationellt än SOC 2
- Lättare att uppnå än SOC 2 om vi har ISO 27001

Vad vi har: Inget.

Kvarstår: Som SOC 2 men billigare och snabbare.

Tidsplan: Q4 2027 om bank-kund kräver.

Kostnad: SEK 200-400K första audit.

10. CSA STAR (Cloud Security Alliance Security Trust Assurance and Risk)

Status: Frivillig certifiering för cloud-leverantörer. Tre nivåer: Self-Assessment, Third-Party Certification, Continuous Monitoring.

Vad det är: Cloud-specifik säkerhetscertifiering byggd ovanpå ISO 27001 plus extra cloud-controls.

Påverkar Kapaciti:

- Vi kör delvis cloud (Vercel, Supabase), delvis on-prem hos kund
- Mer relevant om vi går full cloud-stack
- Idag på-tum nedprio eftersom on-prem är vår positionering

Vad vi har: Inget.

Tidsplan: Inte i 18-månaders-fönster.

Kostnad: SEK 100-300K.

TIER 4: Sektor-specifika. Bara relevant om vi går djupt i specifik vertikal.

MDR (Medical Device Regulation)

Om Kapaciti någonsin används som diagnos-stöd i vården, kan moduler klassas som medical device class IIa eller IIb. Då krävs MDR-CE-märkning, vilket är 12-18 månaders process. **Idag inte relevant** för våra vård-moduler eftersom de är dokumentations/triage-AI, inte diagnostik.

HIPAA

Endast relevant om vi säljer till USA-vård. **Inte i scope** för vår nordiska expansion.

HDS (Hébergement de Données de Santé)

Franskt krav för hosting av hälsodata. Endast relevant om vi expanderar till Frankrike och tar vård-kunder där. **Inte 2026-2027.**

PCI DSS

Endast relevant om vi hanterar betalningskortsdata. Vi gör inte det idag. Stripe är vår payment-provider, de hanterar PCI scope. **Inte aktuellt.**

NIS2 (Network and Information Security Directive 2)

EU-direktiv för cybersecurity hos essential entities. Kan komma att omfatta oss om vi blir critical supplier till banking. **Bevaka under 2026-2027.**

Konsoliderad prio-ordning för Kapaciti 2026-2028

PRIO	KRAV	STATUS IDAG	KLART TILL
P0	GDPR	Delvis	Q3 2026 (privacy policy + DPA + DPIA)
P0	EU AI Act self-cert	Research klar	Q3 2026
P0	ISO 27001	Inte startat	Q3 2027 (certifierad)
P0	ISO 42001	Inte startat	Q3 2027 (parallellt med 27001)
P1	DORA assessment	Utkast klart	Innan första bank-kund
P1	AML5/6 produkt-kapabilitet	Modul planerad	Q4 2026 om bank-pilot
P2	NIST AI RMF	Intern referens	Löpande från Q3 2026
P2	ISAE 3402	Inte startat	Q4 2027 om bank-kund kräver
P3	SOC 2 Type II	Inte startat	Q2 2028 om USA/UK-marknad
P3	CSA STAR	Inte startat	Bara om vi går cloud-only
Bevaka	NIS2	Inte aktuellt än	Bevaka under 2026-2027

Total kostnad för Tier 1 första 18 månader

POST	KOSTNAD SEK
EU AI Act self-cert (jurist + intern)	200 000-400 000
GDPR (jurist + DPIA + dokumentation)	100 000-200 000
ISO 27001 förstgångs-certifiering	200 000-500 000
ISO 42001 (integrated med 27001)	200 000-400 000
Summa Tier 1	**700 000-1 500 000**

Pre-seed Use of Funds har 5% legal/compliance = SEK 825 000. **Det räcker exakt för Tier 1 om vi exekverar disciplinerat** (väljer mid-range estimat och integrated 27001+42001-audit).
Tier 2 (DORA-bilagor, AML-konsult) ryms inom samma post om vi prioriterar.

Tier 3 är post-Series A eller väntar tills vi har konkret kund som kräver det.

Vad detta betyder för Wellstreet-mötet

Säg:

- Vi har en strukturerad 18-månadersplan för Tier 1 compliance (GDPR, EU AI Act, ISO 27001, ISO 42001)
- Audit-chain och on-prem-arkitektur ger oss huvud-start på 27001 och AI Act artikel 12
- Pre-seed Use of Funds har dedikerad allokering för compliance-arbetet (5% = SEK 825K)
- Integrerad 27001+42001-audit Q3 2027 är planen

Säg INTE:

- "Vi är 27001-certifierade" (osant)
- "Vi är 42001-certifierade" (osant)
- "Vi är AI Act-compliant" (delvis, ej validerat)
- "Vi har CE-mark" (osant)
- "Vi har DORA-godkännande från FI" (osant, FI godkänner inte vendorer)

Förbered svar på:

- "Vad är er kompletthetsgrad för 27001?" → Cirka 15% baserat på interna byggblock. 12 månader till certifierad om vi startar Q3 2026.
- "Hur ser ni på 42001 vs 27001 i ordning?" → Vi gör dem parallellt för att utnyttja gemensam ISMS-struktur. Spar SEK 250-350K vs sekventiellt.
- "Vilka av era moduler är high-risk under AI Act?" → Bara credit-scoring direkt. Övriga limited eller minimal, context-beroende. Vi har skriftlig research.
- "Hur DORA-säker är ni för banker?" → Icke-CTPP-klassad. On-prem-default eliminerar de flesta tredjepartsproblemen. Vi har utkast till bank-bilaga.

Konkret nästa steg

Om vi sätter compliance-spåret igång efter pre-seed-close:

Vecka 1-2 efter close: Quote-requests från BSI, DNV, Intertek, SGS, TÜV SÜD, LRQA för integrated 27001+42001-audit. Välj body.

Vecka 3-4: Engagera jurist för EU AI Act self-cert + DORA-mall. Tre kandidater: Mannheimer Swartling, Setterwalls, Hammarskiöld.

Månad 2-3: Skriva ISMS-policy + AI-policy. CEO godkänner. Distribuera för signature.

Månad 4-6: Implementera procedures, risk-register, supplier assessment. Bygg internal audit-program.

Månad 7-9: Internal audit. Management review. Stage 1-prep.

Månad 10-12: Stage 1 audit. Åtgärda findings. Stage 2 audit.

Månad 13-14: Certifierings-beslut. Marknadsföring av certifikat.

Detta är aggressivt men möjligt om vi har dedikerad person på det från månad 2.