NIS2 Compliance & IAM-förstärkning
GreenTyre Recycling AB

Datum: 2026-02-26

Upprättad av: Julian Rieger – IT-säkerhetskonsult

Version: 1.0

1. Projektöversikt

Projektnamn	NIS2 Compliance & IAM-förstärkning – GreenTyre Recycling AB
Beställare	VD, Eva Grönberg GreenTyre Recycling AB
Projektägare	IT-chef, Bosse Däckberg GreenTyre Recycling AB
Projektledare	Julian Rieger – IT-säkerhetskonsult
Startdatum	2026-03-02
Slutdatum	2026-07-17
Budget	400 000 SEK (inkl. extern konsult, licenser och utbildning)
Klassning	GreenTyre Recycling AB – viktig entitet enligt NIS2 (EU 2022/2555)

2. Bakgrund och motiv

GreenTyre Recycling AB (~85 anställda) är ett svenskt däckåtervinningsföretag klassificerat som viktig entitet under NIS2-direktivet (EU 2022/2555). Direktivet ställer bindande krav på riskhantering, styrning, incidentrapportering, tekniska och organisatoriska säkerhetsåtgärder samt leverantörskedjesäkerhet.

En Risk- och sårbarhetsanalys (RSA) genomfördes i februari 2026 (Del 1) och identifierade sju riskområden med konstaterade GAP mot NIS2-kraven:

Risk 1 – Inloggning: avsaknad av MFA och svag lösenordspolicy
Risk 2 – SSO: otillräckligt token-skydd och sessionsövervakning
Risk 3 – Users & SoD: bristande rollseparation och IGDLA-tillämpning
Risk 4 – PIM/PAM: permanent privilegierad åtkomst utan JIT eller auditing
Risk 5 – Ransomware: ingen strukturerad backupstrategi eller testad återställningsplan
Risk 6 – Phishing & säkerhetsmedvetenhet: ingen utbildning eller trygg rapporteringskultur
Risk 7 – Leverantörskedja: externa konsulter och SaaS-tjänster utan formella säkerhetskrav

Detta projektförslag beskriver hur GreenTyre strukturerat ska åtgärda identifierade GAP och uppnå verifierbar NIS2-efterlevnad.

3. Syfte och mål

Övergripande syfte

Att uppnå verifierbar efterlevnad av NIS2-direktivet samt stärka GreenTyres IAM-förmåga och övergripande cybersäkerhetsnivå.

Mål

Åtgärda samtliga GAP identifierade i RSA (Del 1) mot NIS2 och ISO/IEC 27002:2022.
Aktivera MFA på 100 % av konton och implementera Conditional Access i Entra ID.
Implementera Entra ID PIM med just-in-time-åtkomst för alla privilegierade roller.
Etablera strukturerad backupstrategi (daglig/veckovis/månadsvis/halvårsvis) med testad återställningsplan.
Inrätta formell IAM-process för externa konsulter och SaaS-tjänster med NIS2-klausul i avtal.
Genomföra säkerhetsmedvetenhetsutbildning för all personal och etablera trygg rapporteringskultur.
Säkerställa ledningens ansvar och insyn i enlighet med NIS2 Art. 20.
Förbereda organisationen för tillsyn och revision.

4. Omfattning (Scope)

Ingår

GAP-analys mot NIS2 (genomförd i Del 1, fördjupas i Fas 2)
Risk- och sårbarhetsanalys (Del 1 som grund, löpande uppdatering)
IAM-åtgärder: MFA, Conditional Access, PIM, IGDLA, externa konton
Policyer och styrdokument (informationssäkerhetspolicy, IAM-policy, incidentpolicy, leverantörspolicy)
Incident- och rapporteringsprocess (NIS2 Art. 23: 24 h / 72 h / 1 månad)
Backup, återställning och testad rollback-plan
Leverantörs- och tredjepartshantering inkl. NIS2-klausuler i avtal
Utbildning och säkerhetsmedvetenhet för all personal
Loggning, spårbarhet och revision

Ingår inte

OT-säkerhet (hanteras separat i OT-säkerhetsprojektet)
Fysisk säkerhet (utanför projektets scope)
Upphandling av ny ERP eller verksamhetssystem

5. Styrning och roller

Roll	Ansvar
Styrelse / VD	Övergripande ansvar för NIS2-efterlevnad (Art. 20). Godkänner budget och scope.
IT-chef (Projektägare)	Beslut och prioritering. Eskalering vid scope-förändringar. Slutlig godkännare.
Julian Rieger – IT-säkerhetskonsult (Projektledare)	Plan, leverans och koordinering. Upprättar dokumentation och rapporterar till projektägare.

Systemadministratör AD/Entra	Teknisk implementation av IAM-åtgärder i AD DS och Microsoft Entra ID.
HR-chef	Roller och rollprofiler, utbildningsplanering, uppdatering vid personalförändringar.
Inköpsansvarig / Juridik	NIS2-klausuler i leverantörsavtal, leverantörsutvärdering.
Leverantörer / Externa konsulter	Genomförande av tekniska åtgärder enligt avtalade säkerhetskrav.

6. Projektfaser

Fas 1 – Initiering

Period: 2026-03-02 – 2026-03-06

Aktiviteter

- Fastställa projektscope och avgränsningar
- Förankra projektet hos ledning och VD (NIS2 Art. 20)
- Identifiera kritiska tjänster och beroenden
- Upprätta projektplan och kommunikationsplan

Leverans: Godkänd projektplan, förankrad hos ledning

Fas 2 – GAP-analys (NIS2)

Period: 2026-03-09 – 2026-03-27

Aktiviteter

- Fördjupad nulägesanalys baserad på RSA (Del 1)
- GAP per NIS2-artikel och ISO 27002:2022-kontroll
- Riskklassning och prioritering av åtgärder

Leverans: GAP-rapport + prioriterad åtgärdslista

Fas 3 – Riskhantering

Period: 2026-03-30 – 2026-04-10

Aktiviteter

- Uppdatera RSA med nya fynd från GAP-analysen
- Koppling till BIA (Business Impact Analysis)
- Upprätta riskregister med ägare och åtgärdstatus

Leverans: Uppdaterad RSA + riskregister

Fas 4 – Styrning & Policy

Period: 2026-04-13 – 2026-04-24

Aktiviteter

- Informationssäkerhetspolicy (NIS2 Art. 21)
- IAM- och åtkomstkontrollpolicy (IGDLA, minsta privilegium)
- Incidentresponspolicy (NIS2 Art. 23)
- Leverantörspolicy med NIS2-klausul
- Logg- och retention-policy

Leverans: Godkänt policypaket (signerat av VD)

Fas 5 – Tekniska åtgärder

Period: 2026-04-27 – 2026-06-05

Aktiviteter

- MFA på 100 % av konton via Entra ID (Authenticator/FIDO2)
- Conditional Access-policyer (riskbaserad inloggning)
- Entra ID PIM – just-in-time-åtkomst för privilegierade roller
- IGDLA-struktur i AD DS, access reviews
- Microsoft LAPS + gMSA för tjänstekonton
- Backup-implementation: daglig/veckovis/månadsvis/halvårsvis + immutable storage
- Testad rollback- och återställningsplan (protokollfört)
- Entra ID External Identities för externa konsulter
- Microsoft Defender for Endpoint (EDR) + Defender for Identity

Leverans: Implementerade och testade tekniska kontroller

Fas 6 – Incident & rapportering

Period: 2026-06-08 – 2026-06-19

Aktiviteter

- Upprätta incidenthanteringsprocess (24 h / 72 h / 1 månad per NIS2 Art. 23)
- Definiera roller, eskalering och kommunikationsvägar
- Genomföra table-top-övning (simulerat ransomware-scenario)
- Dokumentera och godkänn testad process

Leverans: Testad och dokumenterad incidentprocess

Fas 7 – Leverantörskedja

Period: 2026-06-22 – 2026-07-03

Aktiviteter

- Inventering av externa konsulter och SaaS-tjänster
- Klassificering av leverantörer efter risknivå
- Inför NIS2-klausul i alla leverantörsavtal
- Implementera IAM-process för externa konton (tidsbegränsning, avprovisionering)
- Genomför första leverantörsutvärderingen

Leverans: Leverantörsregister + uppdaterade avtal med NIS2-krav

Fas 8 – Utbildning & medvetenhet

Period: 2026-07-06 – 2026-07-10

Aktiviteter

- Ledningsutbildning: NIS2-ansvar (Art. 20) och rapporteringsskyldighet
- IT-personalutbildning: tekniska kontroller och incidenthantering
- Slutanvändarutbildning: phishing, social ingenjörskonst, trygg rapportering
- Lansera rapporteringskanal och kommunicera öppen rapporteringskultur

Leverans: Genomförd utbildning med deltagarlistor

Fas 9 – Revision & avslut

Period: 2026-07-13 – 2026-07-17

Aktiviteter

- Intern revision mot NIS2-krav och policypaket
- Dokumentera kvarstående avvikelser med åtgärdsplan
- Sammanställ compliance-paket för eventuell tillsyn
- Överlämning till förvaltning (IT-chef som processägare)

Leverans: Compliance-paket + förvaltningsplan

7. Tidsplan

Fas	Period	Veckor	Ansvarig
Fas 1 – Initiering	2026-03-02 – 2026-03-06	1	Projektledare
Fas 2 – GAP-analys	2026-03-09 – 2026-03-27	3	Projektledare + IT-chef
Fas 3 – Riskhantering	2026-03-30 – 2026-04-10	2	Projektledare
Fas 4 – Styrning & Policy	2026-04-13 – 2026-04-24	2	Projektledare + Juridik
Fas 5 – Tekniska åtgärder	2026-04-27 – 2026-06-05	6	Systemadministratör + IT
Fas 6 – Incident & rapportering	2026-06-08 – 2026-06-19	2	Projektledare + IT-chef
Fas 7 – Leverantörskedja	2026-06-22 – 2026-07-03	2	Inköp + Juridik
Fas 8 – Utbildning	2026-07-06 – 2026-07-10	1	HR + Projektledare
Fas 9 – Revision & avslut	2026-07-13 – 2026-07-17	1	Projektledare + IT-chef

8. Risker i projektet

Projektrisk	Sannolikhet / Konsekvens	Hantering
Otydligt ledningsansvar (NIS2 Art. 20)	Medel / Hög	Förankra mandat hos VD i Fas 1. Skriftligt beslut krävs.
Resursbrist – IT-personal hinner inte med daglig drift och projekt parallellt	Hög / Medel	Planera fas-övergångar med buffert. Extern konsult avlastar vid behov.
Leverantörsberoenden – externa parter levererar sent	Medel / Medel	Identifiera beroenden tidigt i Fas 1. Inför klausuler om leveranstider.
Underskattad förändringsledning – motstånd mot nya rutiner	Medel / Medel	Kommunikationsplan från Fas 1. Ledningens stöd synligt för all personal.
Scope-kryp – nya krav tillkommer under projektets gång	Medel / Låg	Formell ändringshantering. Alla scope-förändringar godkänns av projektägare.

9. Mätetal (KPI)

KPI	Nuläge	Målvärde (vid projektslut)
% uppfyllda NIS2-krav (Art. 21)	~30 %	100 %
MFA-täckning (% av konton)	< 50 %	100 %
Antal privilegierade konton utan JIT	Alla	0
Andel externa konsulter med	0 %	100 %

tidsbegr. konto		
Andel granskade leverantörer med NIS2-krav	0 %	100 %
Testad återställningsplan (backup)	Nej	Ja (halvårsvis)
Personal som genomgått säkerhetsutbildning	0 %	100 %

10. Beslutspunkter

Beslutspunkt	Datum	Beslutsfattare
Godkänd projektplan och budget	2026-03-06	VD / IT-chef
Godkänd GAP-rapport och åtgärdslista	2026-03-27	IT-chef
Godkänt policypaket (signerat av VD)	2026-04-24	VD
Godkänd teknisk implementation	2026-06-05	IT-chef
Godkänd och testad incidentprocess	2026-06-19	IT-chef / VD
Godkänt compliance-paket (projektavslut)	2026-07-17	VD / IT-chef