Bijlage 1: Overzicht status opvolging van de BIT-maatregelen door programma ERTMS

Id.	Korte omschrijving van de actie	Invloed op aanbesteding	Getoetst	Tijdpad
1.1	Systems engineering aanpak (werkwijze op hoofdlijnen) uitwerken naar aanleiding van het BIT.	Ja	Ja	Afgerond
1.2	Systems engineering sturingstafel operationeel.	Ja	Ja	Afgerond
1.3	Team systems engineering operationeel.	Deels	Ja	Afgerond
1.4	Documentatie (Verificatie PvE (Pass-Fail) en Apportionering PvE) afronden.	Ja	Ja	Afgerond
1.5	Apportionering tot op bestelniveau gereed voor aanbestedingen.	Deels	Ja	Afgerond
1.6	Additionele middelen (tooling en processsen) ten behoeve van systems engineering definiëren en implementeren.	Deels	Ja	2020
1.7	Verantwoordelijkheid voor de kwaliteit en de systeemintegratie van alle systeemobjecten en hun interfaces expliciteren.	Ja	Ja	Afgerond
1.8	Overzicht opstellen van alle relevante PvE's in hun onderlinge relaties.	Deels	Ja	Afgerond
2.1	Kwaliteitsbeheersingsmethode opnemen in aanbestedingsdossiers.	Ja	Ja	Afgerond
2.2	Configuratiemanagement aanpak operationeel.	Deels	Ja	Afgerond
2.3	Audits uitvoeren door Programmadirectie en Implementerende organisaties op kwaliteitsbeheersing. op componenten.	Deels	Ja	Afgerond
3.1	Aanvullende expertise cybersecurity verwerven.	Nee	Nee	Afgerond
3.2	Document "Rules & regulations" opstellen, daarbij aansluiten bij beleid cybersecuritysector-partijen.	Deels	Ja	2021
3.3	Het inrichten van een centrale organisatie voor cybersecurity aansluitend op centrale organisaties bij sectorpartijen en IenW.	Nee	Nee	2021
3.4	Tooling implementeren bij sectorpartijen en de centrale organisatie ten behoeve van detectie van cyberincidenten.	Nee	Nee	2021
3.5	Actieplan Cybersecurity uit 2017 actualiseren op basis van nieuwe inzichten.	Nee	Nee	Afgerond
3.6	Dreigingsanalyse ERTMS jaarlijks actualiseren en n.a.v. beheersmaatregelen doorvoeren.	Nee	Nee	Afgerond
3.7	Aandringen op het opnemen van eisen voor het gebruik van cryptografische hardware in de Europese specificaties en parallel daaraan leveranciers vragen, waar mogelijk al gebruik te maken van cryptografische hardware. Mocht dit niet mogelijk zijn dan zal het programma andere beveiligingsmaatregelen laten toepassen.	Deels	Ja	2020
3.8	Strenge eisen stellen ten aanzien van fysieke beveiliging van en toegang tot de apparatuur waarin de sleutels worden opgeslagen (spoorvoertuig, RBC, KMC).	Deels	Ja	2020
4.1	Projectteam ketenbeheer instellen met kennishouders huidige beheer ERTMS.	Nee	Nee	Afgerond
4.2	Geplande migratietafel ketenbeheer versneld starten met verantwoordelijken uit de lijn van de implementerende organisaties.	Nee	Nee	Afgerond
4.3	Definitie en inrichting van ketenbeheer opstellen op basis van ITIL. (migratiestap 1)	Nee	Nee	Afgerond
4.4	Stappenplan opstellen voor de invoering van ketenbeheer waarin duidelijk is welke taken centraal en welke decentraal worden uitgevoerd. (migratiestap 1)	Deels	Ja	Afgerond