Functie	Categorie	Subcategorie
IDENTIFICATIE	**Asset Management:** De gegevens, het personeel, de apparatuur, de systemen en de faciliteiten die de organisatie in staat stellen haar bedrijfsdoelstellingen te bereiken, worden geïdentificeerd en beheerd in overeenstemming met hun relatieve belang voor de organisatiedoelstellingen en de risicostrategie van de organisatie.	Fysieke apparaten en systemen binnen de organisatie worden geïnventariseerd
		Software platforms en applicaties binnen de organisatie worden geinventariseerd
		Organisatorische communicatie en gegevensstromen worden in kaart gebracht
		Externe informatiesystemen worden gecatalogiseerd
		Middelen (bv. hardware, apparatuur, gegevens, tijd, personeel en software) krijgen prioriteit op basis van hun classificatie, kriticiteit en bedrijfswaarde
		Cyberbeveiligingsrollen en -verantwoordelijkheden voor het voltallige personeel en externe belanghebbenden (bv. leveranciers, klanten, partners) worden vastgesteld
	Zakelijke omgeving: De missie, doelstellingen, belanghebbenden en activiteiten van de organisatie worden begrepen en geprioriteerd; deze informatie wordt gebruikt om de rollen, verantwoordelijkheden en beslissingen inzake risicobeheer op het gebied van cyberbeveiliging te onderbouwen.	De rol van de organisatie in de toeleveringsketen wordt geïdentificeerd en gecommuniceerd
		De plaats van de organisatie in de kritieke infrastructuur en de bedrijfssector wordt geïdentificeerd en meegedeeld
		Prioriteiten voor de missie, doelstellingen en activiteiten van de organisatie worden vastgesteld en meegedeeld
		De afhankelijkheden en kritieke functies voor de levering van kritieke diensten zijn vastgesteld
		Voor alle operationele fasen (bv. onder dwang/aanval, tijdens herstel, tijdens normale operaties) worden veerkrachtvereisten vastgesteld om de levering van kritieke diensten te ondersteunen
	Bestuur: het beleid, de procedures en processen voor het beheer en de bewaking van de regelgevings-, juridische, risico-, milieu- en operationele vereisten van de organisatie worden begrepen en het beheer van het cyberbeveiligingsrisico daarop wordt afgestemd.	Het cyberbeveiligingsbeleid van de organisatie wordt vastgesteld en gecommuniceerd
		De taken en verantwoordelijkheden op het gebied van cyberbeveiliging worden gecoördineerd en afgestemd op interne taken en externe partners
		de wettelijke en bestuursrechtelijke voorschriften inzake cyberbeveiliging, met inbegrip van de verplichtingen inzake privacy en burgerlijke vrijheden, worden begrepen en beheerd
		Governance- en risicobeheerprocessen pakken cyberbeveiligingsrisico's aan
	Risico bepaling: De organisatie is zich bewust van het cyberbeveiligingsrisico voor organisatorische operaties (inclusief missie, functies, imago of reputatie), organisatorische activa en personen.	Kwetsbaarheden van activa worden geïdentificeerd en gedocumenteerd
		Informatie over cyberdreigingen wordt ontvangen van informatie-uitwisselingsfora en -bronnen
		Bedreigingen, zowel interne als externe, worden geïdentificeerd en gedocumenteerd
		Mogelijke gevolgen en waarschijnlijkheden voor het bedrijf worden vastgesteld
		Bedreigingen, kwetsbaarheden, waarschijnlijkheden en gevolgen worden gebruikt om risico's te bepalen
		Risicomaatregelen worden geïdentificeerd en geprioriteerd
	Risico Management Strategie: De prioriteiten, beperkingen, risicotoleranties en aannames van de organisatie worden vastgesteld en gebruikt ter ondersteuning van operationele risicobeslissingen.	Risicobeheerprocessen worden vastgesteld, beheerd en goedgekeurd door belanghebbenden in de organisatie
		De risicotolerantie van de organisatie is vastgesteld en duidelijk uitgedrukt
		De bepaling van de risicotolerantie van de organisatie is gebaseerd op haar rol in de analyse van kritieke infrastructuur en sectorspecifieke risico's
	Risicobeheer van de toeleveringsketen: De prioriteiten, beperkingen, risicotoleranties en veronderstellingen van de organisatie worden vastgesteld en gebruikt ter ondersteuning van risicobeslissingen in verband met het beheer van de risico's van de toeleveringsketen. De organisatie heeft de processen ingesteld en geïmplementeerd om de risico's van de toeleveringsketen te identificeren, te beoordelen en te beheren	Risicobeheerprocessen met betrekking tot de cyber-toeleveringsketen worden geïdentificeerd, vastgesteld, beoordeeld, beheerd en overeengekomen door belanghebbenden van de organisatie
		Leveranciers en derden-partners van informatiesystemen, componenten en diensten worden geïdentificeerd, geprioriteerd en beoordeeld aan de hand van een risicobeoordelingsproces voor de cybertoeleveringsketen
		Contracten met leveranciers en derden-partners worden gebruikt om passende maatregelen te implementeren die zijn ontworpen om te voldoen aan de doelstellingen van het cyberbeveiligingsprogramma en het Cyber Supply Chain Risk Management Plan van een organisatie.
		Leveranciers en externe partners worden routinematig beoordeeld aan de hand van audits, testresultaten of andere vormen van evaluaties om te bevestigen dat zij aan hun contractuele verplichtingen voldoen.

	Samen met leveranciers en derden worden respons- en herstelplanning en tests uitgevoerd.

BESCHERMEN	**Identiteitsbeheer, Authenticatie en Toegangscontrole:** De toegang tot fysieke en logische activa en bijbehorende faciliteiten wordt beperkt tot bevoegde gebruikers, processen en apparaten, en wordt beheerd in overeenstemming met het ingeschatte risico van ongeoorloofde toegang tot geautoriseerde activiteiten en transacties.	Identiteiten en legitimatiebewijzen worden uitgegeven, beheerd, geverifieerd, ingetrokken en geaudit voor geautoriseerde apparaten, gebruikers en processen.
		De fysieke toegang tot bedrijfsmiddelen wordt beheerd en beveiligd
		Toegang op afstand wordt beheerd
		Het beheer van toegangsrechten en autorisaties, met inachtneming van de beginselen van minimale privileges en scheiding van taken
		De integriteit van het netwerk wordt beschermd (bijv. door netwerksegregatie, netwerksegmentatie)
		Identiteiten worden aangetoond en gekoppeld aan legitimatiebewijzen en bevestigd in interacties
		Gebruikers, apparaten en andere middelen worden geauthenticeerd (bijv. op basis van enkelvoudige of meervoudige factoren) naar rato van het risico van de transactie (bijv. individuele beveiligings- en privacyrisico's en andere organisatorische risico's)
	Bewustwording en training: Het personeel en de partners van de organisatie krijgen voorlichting over cyberbeveiligingsbewustzijn en worden opgeleid om hun cyberbeveiligingsgerelateerde taken en verantwoordelijkheden uit te voeren in overeenstemming met het desbetreffende beleid, de desbetreffende procedures en overeenkomsten.	Alle gebruikers zijn geïnformeerd en opgeleid
		Bevoegde gebruikers begrijpen hun rol en verantwoordelijkheden
		Externe belanghebbenden (bijv. leveranciers, klanten, partners) begrijpen hun rol en verantwoordelijkheden.
		Leidinggevenden begrijpen hun taken en verantwoordelijkheden
		Fysieke en cyberbeveiligingsmedewerkers hebben inzicht in hun taken en verantwoordelijkheden
	Gegevensbeveiliging: Informatie en records (gegevens) worden beheerd in overeenstemming met de risicostrategie van de organisatie om de vertrouwelijkheid, integriteit en beschikbaarheid van informatie te beschermen.	gegevens in ruste worden beschermd
		Gegevens in doorvoer worden beschermd
		Activa worden gedurende de verwijdering, overdracht en vervreemding formeel beheerd
		Er wordt voldoende capaciteit gehandhaafd om beschikbaarheid te waarborgen
		Er zijn beschermingsmaatregelen getroffen tegen het uitlekken van gegevens
		Er worden mechanismen voor integriteitscontrole gebruikt om de integriteit van programmatuur, firmware en informatie te verifiëren
		De ontwikkelings- en testomgeving(en) zijn gescheiden van de productieomgeving
		Er worden mechanismen voor integriteitscontrole gebruikt om de integriteit van de hardware te verifiëren

	Processen en procedures voor informatiebeveiliging: Er worden beveiligingsbeleidsmaatregelen (die betrekking hebben op het doel, het toepassingsgebied, de taken, de verantwoordelijkheden, de inzet van het management en de coördinatie tussen organisatorische entiteiten), processen en procedures gehandhaafd en gebruikt om de bescherming van informatiesystemen en -middelen te beheren.	Er wordt een basisconfiguratie van informatietechnologie/industriële controlesystemen gemaakt en onderhouden, met inachtneming van de beveiligingsprincipes (b.v. concept van minimale functionaliteit)
		Er wordt een systeemontwikkelingscyclus voor het beheer van systemen geïmplementeerd
		Er zijn processen voor controle op wijzigingen in de configuratie.
		Er worden back-ups van informatie gemaakt, onderhouden en getest
		Er wordt voldaan aan beleid en regelgeving met betrekking tot de fysieke gebruiksomgeving van organisatorische middelen
		Gegevens worden vernietigd conform beleid
		Beveiligingsprocessen worden verbeterd
		De effectiviteit van beschermingstechnieken wordt gedeeld
		Er zijn responsplannen (Incident Response en Business Continuity) en herstelplannen (Incident Recovery en Disaster Recovery) aanwezig en deze worden beheerd
		Response- en herstelplannen worden getest
		Cyberbeveiliging wordt meegenomen in personeelsbeleid (bijv. deprovisionering, personeelsscreening)
		Er wordt een plan voor kwetsbaarheidsbeheer ontwikkeld en uitgevoerd
	Onderhoud: Onderhoud en reparaties van onderdelen van industriële besturings- en informatiesystemen worden uitgevoerd in overeenstemming met het beleid en de procedures.	Onderhoud en reparatie van organisatorische middelen worden uitgevoerd en vastgelegd, met goedgekeurde en gecontroleerde hulpmiddelen
		Onderhoud op afstand van organisatorische middelen wordt goedgekeurd, vastgelegd en uitgevoerd op een wijze die voorkomt dat onbevoegden toegang krijgen
	Beveiligingstechnologie: Technische beveiligingsoplossingen worden beheerd om de veiligheid en veerkracht van systemen en activa te waarborgen, in overeenstemming met het desbetreffende beleid, de desbetreffende procedures en de desbetreffende overeenkomsten.	Audit/log records worden vastgelegd, gedocumenteerd, geïmplementeerd en geëvalueerd in overeenstemming met het beleid
		Verwijderbare media worden beveiligd en het gebruik ervan wordt beperkt conform het beleid
		Het principe van minimale functionaliteit wordt toegepast door systemen zodanig te configureren dat ze alleen essentiële mogelijkheden bieden
		Communicatie- en besturingsnetwerken worden beschermd
		Er worden mechanismen (bijv. failsafe, load balancing, hot swap) geïmplementeerd om de veerkrachtvereisten in normale en ongunstige situaties te halen

DETECTEREN	**Anomalieën en gebeurtenissen:** Anomalieën worden gedetecteerd en de potentiële impact van gebeurtenissen wordt begrepen.	Er wordt een basislijn van netwerkoperaties en verwachte gegevensstromen voor gebruikers en systemen opgesteld en beheerd
		Geconstateerde gebeurtenissen worden geanalyseerd om inzicht te krijgen in aanvalsdoelen en -methoden
		Gebeurtenisgegevens worden verzameld en gecorreleerd uit meerdere bronnen en sensoren
		De impact van gebeurtenissen wordt bepaald
		Incident-alarmdrempels worden vastgesteld
	Voortdurende monitoring van de beveiliging: Het informatiesysteem en de bedrijfsmiddelen worden gemonitord om gebeurtenissen op het gebied van cyberbeveiliging vast te stellen en de doeltreffendheid van beschermingsmaatregelen te controleren.	Het netwerk wordt gemonitord om potentiële cyberbeveiligingsgebeurtenissen te detecteren
		De fysieke omgeving wordt bewaakt om potentiële cyberbeveiligingsgebeurtenissen op te sporen
		Personeelsactiviteiten worden gemonitord om potentiële cyberbeveiligingsgebeurtenissen op te sporen
		Kwaadaardige code wordt gedetecteerd
		Onbevoegde mobiele code wordt gedetecteerd
		De activiteit van externe dienstverleners wordt gemonitord om potentiële cyberbeveiligingsgebeurtenissen op te sporen
		Er wordt toezicht gehouden op ongeautoriseerd personeel, verbindingen, apparatuur en software
		Scans op kwetsbaarheden worden uitgevoerd
	Opsporingsprocessen: Detectieprocessen en -procedures worden onderhouden en getest om ervoor te zorgen dat men zich bewust is van afwijkende gebeurtenissen.	De rollen en verantwoordelijkheden voor detectie zijn duidelijk gedefinieerd om de verantwoordingsplicht te waarborgen
		Detectieactiviteiten voldoen aan alle toepasselijke vereisten
		Detectieprocessen worden getest
		Informatie over detectie van voorvallen wordt gecommuniceerd
		Detectieprocessen worden continu verbeterd

REAGEREN	**Reactieplanning:** Responseprocessen en -procedures worden uitgevoerd en gehandhaafd, zodat kan worden gereageerd op ontdekte cyberbeveiligingsincidenten.	Het reactieplan wordt tijdens of na een incident uitgevoerd
	Communicatie: De reactieactiviteiten worden gecoördineerd met interne en externe belanghebbenden (bv. externe steun van rechtshandhavingsinstanties).	Het personeel kent zijn rol en de volgorde van operaties wanneer een reactie nodig is
		Incidenten worden gemeld in overeenstemming met de vastgestelde criteria
		Informatie wordt gedeeld in overeenstemming met de reactieplannen
		Coördinatie met belanghebbenden vindt plaats in overeenstemming met de reactieplannen
		Vrijwillig delen van informatie met externe belanghebbenden om het situationeel bewustzijn inzake cyberbeveiliging te vergroten
	Analyse: Analyse wordt uitgevoerd om een doeltreffende reactie te waarborgen en herstelactiviteiten te ondersteunen.	Meldingen van detectiesystemen worden onderzocht
		De impact van het incident wordt begrepen
		Forensisch onderzoek wordt uitgevoerd
		incidenten worden gecategoriseerd in overeenstemming met de reactieplannen
		Er zijn processen ingesteld om kwetsbaarheden die door interne en externe bronnen (bv. interne tests, beveiligingsbulletins of beveiligingsonderzoekers) aan de organisatie worden meegedeeld, te ontvangen, te analyseren en daarop te reageren.
	Verminderen: Activiteiten worden uitgevoerd om uitbreiding van een gebeurtenis te voorkomen, de gevolgen ervan te beperken en het incident op te lossen.	Incidenten worden onder controle gehouden
		Incidenten worden beperkt
		Nieuw vastgestelde kwetsbaarheden worden beperkt of als aanvaard risico gedocumenteerd
	Verbeteringen: De organisatorische reactieactiviteiten worden verbeterd door lessen te trekken uit huidige en eerdere detectie/reactieactiviteiten.	In reactieplannen wordt rekening gehouden met opgedane ervaringen
		Responsstrategieën worden geactualiseerd
HERSTEL	**Herstelplanning:** Herstelprocessen en -procedures worden uitgevoerd en bijgehouden om te zorgen voor het herstel van systemen of activa die getroffen zijn door cyberbeveiligingsincidenten.	Tijdens of na een incident op het gebied van cyberbeveiliging wordt een herstelplan uitgevoerd
	Verbeteringen: De herstelplanning en -processen worden verbeterd door de geleerde lessen in toekomstige activiteiten te verwerken.	In de herstelplannen is rekening gehouden met de opgedane ervaring
		De herstelstrategieën worden geactualiseerd
	Communicatie: De herstelactiviteiten worden gecoördineerd met interne en externe partijen (bv. coördinatiecentra, internetproviders, eigenaars van aanvallende systemen, slachtoffers, andere CSIRT's, en verkopers).	Public relations worden beheerd
		De reputatie wordt hersteld na een incident
		De herstelactiviteiten worden meegedeeld aan interne en externe belanghebbenden en aan directie- en managementteams