Verslag over de evaluatie van het raamwerk voor ICT-risicobeheersing

Een praktische handleiding voor het opstellen van het verslag over de evaluatie van het raamwerk voor ICT-risicobeheersing

Een template van NOREA

Auteurs:

Stef Smit – Kouters Van der Meer

Marvin Kruin – MNK Risk

Jesper de Boer – Deloitte

Sandeep Gangaram Panday - Brightlyn

Postbus 242, 2130 AE Hoofddorp

Telefoon: +31 (0) 88 4960 380

Nederland

E-mail: norea@norea.nl

Taskforce reviewers
De template is gereviewed door de volgende leden van de NOREA Taskforce Regulatory:

Naam	Rol	Bedrijf
Andrey Prozorov	Cyber security & Privacy expert	ISMS PRO
Danny Bos	Senior manager Cybersecurity & Privacy	Eraneos

De template is ontwikkeld in samenwerking met Kouters Van der Meer.

Voor de volledige ledenlijst en meer door de Taskforce ontwikkelde content, zie https://www.norea.nl/dora of volg ons op LinkedIn: https://www.linkedin.com/showcase/taskforce-dora.

Inhoudsopgave

0 Leeswijzer

De template is ontwikkeld door NOREA, de beroepsvereniging van IT-auditors, ter ondersteuning van organisaties bij het opstellen van het verslag over de evaluatie van het ICT-risicobeheersingsraamwerk overeenkomstig artikel 6, lid 5, van Verordening (EU) 2022/2554 (DORA) en artikel 27 van de RTS inzake ICT-risicobeheersing. De template is bedoeld als praktisch hulpmiddel om de uitkomsten van de evaluatie op een consistente en volledige wijze te structureren, documenteren en communiceren.

De template is ontworpen als een basisdocument. Gestandaardiseerde teksten, toelichtingen en voorbeeldformuleringen zijn in het **zwart** opgenomen om een consistente interpretatie en toepassing te ondersteunen. Deze kunnen rechtstreeks worden overgenomen of worden aangepast aan de specifieke context van de organisatie. Onderdelen die door de gebruiker moeten worden ingevuld en die betrekking hebben op verplichte DORA-vereisten zijn **groen** gemarkeerd en dienen te worden uitgewerkt om aansluiting op de wettelijke vereisten te waarborgen. Aanvullende onderdelen die **blauw** zijn gemarkeerd betreffen aanbevolen werkwijzen die, hoewel niet verplicht onder DORA, bijdragen aan een robuuster en volwassener ICT-risicobeheersingsraamwerk en daarom worden aanbevolen.

Van organisaties wordt verwacht dat zij de template aanvullen, aanpassen en valideren op basis van hun eigen governancestructuur, risicoprofiel en specifieke context. De template dient niet te worden beschouwd als een checklist die strikt moet worden gevolgd. Zij moet in plaats daarvan worden gebruikt als een gestructureerde leidraad die professionele oordeelsvorming en een organisatiespecifieke interpretatie van de DORA-vereisten ondersteunt.

Disclaimer

De template wordt uitsluitend ter beschikking gesteld ter ondersteuning en als hulpmiddel bij het opstellen van het verslag over de evaluatie van het ICT-risicobeheersingsraamwerk. Hoewel de template met de nodige zorgvuldigheid en professionele deskundigheid is ontwikkeld, geeft NOREA geen garantie ten aanzien van de volledigheid, juistheid of geschiktheid ervan voor een specifieke organisatie of toezichtsrechtelijke context. De verantwoordelijkheid voor het voldoen aan de vereisten van DORA en andere toepasselijke wet- en regelgeving berust uitsluitend bij de organisatie die van de template gebruikmaakt. Gebruikers dienen zelf een beoordeling uit te voeren en, waar nodig, onafhankelijk professioneel of juridisch advies in te winnen.

Hoewel de template waardevolle handvatten kan bieden, blijven de wettelijke vereisten zoals opgenomen in DORA te allen tijde leidend.

[logo van de financiële entiteit]

Verslag over de evaluatie van het raamwerk voor ICT-risicobeheersing

[naam van de financiële entiteit]

[start evaluatieperiode – einde evaluatieperiode]

Documentbeheer

Veld	Toelichting
Verslag versie	V [X.X]
Datum van opstellen	[DD/MM/JJJJ]
Datum van goedkeuring door het leidinggevend orgaan	[DD/MM/JJJJ]
Voor de evaluatie verantwoordelijke functie	[bijv. CISO]
Classificatie	[bijv. vertrouwelijk/ intern]

Opgesteld in een elektronisch doorzoekbaar formaat overeenkomstig artikel 6, lid 5, van Verordening (EU) 2022/2554 (DORA) en artikel 27 van de RTS inzake ICT-risicobeheersing.

1 Inleiding

Als onderdeel van haar raamwerk voor ICT-risicobeheersing voert [financiële entiteit] (hierna: ["afgekorte naam" of "de financiële entiteit"]) jaarlijks een evaluatie uit van het raamwerk voor ICT-risicobeheersing. Deze evaluatie stelt [financiële entiteit] in staat de volwassenheid van haar raamwerk voor ICT-risicobeheersing stapsgewijs te verbeteren door verbeterpunten te identificeren en daarop actie te ondernemen. Het leidinggevend orgaan behoudt de eindverantwoordelijkheid voor de adequaatheid en doeltreffendheid van het raamwerk voor ICT-risicobeheersing.

Dit verslag is opgesteld op basis van informatiebronnen, waaronder [beschrijf de informatiebronnen die zijn opgenomen in hoofdstuk 8]. Met dit verslag, dat door het leidinggevend orgaan van [financiële entiteit] wordt goedgekeurd als onderdeel van haar toezichtverantwoordelijkheden ten aanzien van ICT-risicobeheersing en digitale operationele weerbaarheid, voldoet [financiële entiteit] aan de vereisten zoals opgenomen in artikel 6, lid 5, van Verordening (EU) 2022/2554 (DORA) en artikel 27 van de RTS inzake ICT-risicobeheersing.

Dit verslag bevat een nadere toelichting op de uitgevoerde activiteiten met betrekking tot het raamwerk voor ICT-risicobeheersing, de evaluatie van dat raamwerk en de corrigerende maatregelen die moeten worden getroffen. Dit verslag is opgesteld door [voor de evaluatie verantwoordelijke functie] onder verantwoordelijkheid van het leidinggevend orgaan van [financiële entiteit]. Dit verslag is opgesteld [als onderdeel van de reguliere evaluatie van het raamwerk voor ICT-risicobeheersing / naar aanleiding van een ernstig ICT-gerelateerd incident (neem alle ICT-gerelateerde incidenten met oorzaakanalyse op) / naar aanleiding van instructies van toezichthouders (verwijs naar de instructies) / naar aanleiding van conclusies uit relevante testen van digitale operationele weerbaarheid (verwijs naar de conclusies) / naar aanleiding van conclusies uit relevante auditprocessen (verwijs naar de conclusies)].

1.1 Managementsamenvatting

[geef een beknopte samenvatting van de bevindingen, corrigerende maatregelen en conclusies van dit verslag]

1.2 De financiële entiteit en haar context

Onderwerp: [beschrijf de financiële entiteit waarop het verslag betrekking heeft, met inbegrip van de volledige juridische naam, LEI-code, statutaire zetel, bevoegde autoriteit en, waar relevant, de groepsstructuur]

Context: [beschrijf de aard, schaal en complexiteit van de diensten, activiteiten en operaties van de financiële entiteit]

Organisatie: [beschrijf de organisatie en strategie van de financiële entiteit]

Kritieke functies: [noem de kritieke functies van de financiële entiteit of geef een samenvatting en verwijs naar de volledige lijst]

ICT-omgeving: [beschrijf de interne en gecontracteerde ICT- diensten en -systemen en de implicaties die een totaal verlies van of ernstige degradatie van die systemen zou hebben in termen van kritieke of belangrijke functies en marktefficiëntie]

Belangrijke lopende projecten of activiteiten: [beschrijf significante transformatie-, uitbestedings- of veranderprogramma's die relevant zijn voor ICT-risico]

1.3 Samenvatting van wijzigingen [sinds het vorige verslag/ in het afgelopen jaar]

[wanneer er een vorig verslag beschikbaar is] Sinds het vorige verslag, betreffende [start evaluatieperiode - einde evaluatieperiode], waren de belangrijkste wijzigingen in het raamwerk voor ICT-risicobeheersing:

[wanneer dit het eerste gedocumenteerde verslag is] In de afgelopen 12 maanden waren de belangrijkste wijzigingen in het raamwerk voor ICT-risicobeheersing:

[Wijziging 1]: [vat de wijziging en de impact daarvan op digitale operationele weerbaarheid in enkele zinnen samen]

[herhaal voor iedere wijziging]

1.4 Samenvatting van het ICT-risico

Actueel ICT-risicoprofiel: [beschrijf het actuele ICT-risicoprofiel van de financiële entiteit en verwijs waar mogelijk naar eerdere risicobeoordelingen en bedrijfsimpactanalyses]

ICT-risicoprofiel op korte termijn: [beschrijf het ICT-risicoprofiel van de financiële entiteit op korte termijn en verwijs waar mogelijk naar geïdentificeerde belangrijke opkomende risico's of verwachte wijzigingen]

Dreigingslandschap: [beschrijf de dreigingen voor de financiële entiteit die tijdens de evaluatieperiode zijn geïdentificeerd]

Doeltreffendheid van beheersmaatregelen: [beschrijf de doeltreffendheid van de tijdens de evaluatieperiode uitgevoerde beheersmaatregelen en de impact daarvan op de risico's van de financiële entiteit in relatie tot haar risicotolerantie, met inbegrip van een beoordeling of de doeltreffendheid van de beheersmaatregelen toereikend is gegeven de risicobereidheid van de entiteit]

Security posture: [beschrijf de security posture van de financiële entiteit met betrekking tot digitale operationele weerbaarheid]

[Governance en integratie: beschrijf hoe ICT-risicobeheersing is geïntegreerd in het algehele raamwerk voor ondernemingsbrede risicobeheersing, met inbegrip van rollen, verantwoordelijkheden, escalatiemechanismen en afstemming op besluitvorming binnen de bedrijfsvoering]

2 Majeure wijzigingen en verbeteringen

Zoals samengevat in hoofdstuk 1.2 hebben [sinds het vorige verslag/ in het afgelopen jaar], verschillende wijzigingen en verbeteringen plaatsgevonden. Voor iedere wijziging of verbetering is een analyse uitgevoerd om de aard en impact daarvan op digitale operationele weerbaarheid, risicobeheersing en governance te beoordelen en inzicht te geven in de effecten op [de financiële entiteit]. De analyse omvat een beoordeling van de wijze waarop deze wijzigingen bijdragen aan het verbeteren van de doeltreffendheid en volwassenheid van het raamwerk voor ICT-risicobeheersing.

2.1 Interne wijzigingen en verbeteringen

[bijv. wijzigingen in de strategie voor digitale operationele weerbaarheid, het interne-controleraamwerk voor ICT of de governance voor ICT-risicobeheersing, etc.]

- **[wijziging of verbetering]:** [beschrijf de wijziging of verbetering, met inbegrip van: of het een wijziging of verbetering betreft, de relevantie daarvan voor geïdentificeerde risico's, de doeltreffendheid van beheersmaatregelen en de algehele weerbaarheid, wanneer deze heeft plaatsgevonden, hoe deze is afgehandeld en wat de impact was op de digitale operationele weerbaarheid, risicobeheersing en governance van de financiële entiteit]

  [herhaal voor iedere wijziging en verbetering]

2.2 Externe wijzigingen en verbeteringen

[bijv. relevante opkomende technologieën, wet- en regelgeving, werkwijzen in de sector, etc.]

- **[wijziging of verbetering]:** [beschrijf de wijziging of verbetering, met inbegrip van: of het een wijziging of verbetering betreft, de relevantie daarvan voor geïdentificeerde risico's, de doeltreffendheid van beheersmaatregelen en de algehele weerbaarheid, wanneer deze heeft plaatsgevonden, hoe deze is afgehandeld en wat de impact was op de digitale operationele weerbaarheid, risicobeheersing en governance van de financiële entiteit]

  [herhaal voor iedere wijziging en verbetering]

3 Bevindingen uit de evaluatie

Deze integrale evaluatie van het raamwerk voor ICT-risicobeheersing van [de financiële entiteit] is gebaseerd op een systematische analyse van bewijs dat uit meerdere interne en externe bronnen is verzameld. Deze bronnen vormen de basis voor het identificeren van zwakke punten, tekortkomingen en lacunes binnen onze architectuur voor ICT-risicobeheersing. De evaluatie integreert bevindingen uit [bijv. beheersactiviteiten van de eerste, tweede en derde lijn, operationele incidentgegevens en de uitkomsten van gerichte weerbaarheidsbeoordelingen], aangevuld met [bijv. monitoring van het externe dreigingslandschap en opkomende ontwikkelingen in wet- en regelgeving].

De volgende bronnen en input zijn samengebracht ter ondersteuning van deze evaluatie:

Interne bronnen:

- [beschrijf een interne bron die is opgenomen in hoofdstuk 8 van dit verslag]
  [herhaal voor iedere interne bron]

Externe bronnen:

- [beschrijf een externe bron die is opgenomen in hoofdstuk 8 van dit verslag]
  [herhaal voor iedere externe bron]

Interne en externe informatiebronnen worden opgenomen en nader beschreven in hoofdstuk 8. Om de bevindingen van deze evaluatie te verzamelen, beschouwt [de financiële entiteit] ieder kerngebied binnen haar raamwerk voor ICT-risicobeheersing, evalueert zij de uitvoering daarvan, analyseert zij de geïdentificeerde zwakke punten, tekortkomingen en lacunes en bepaalt zij de ernst en impact daarvan, met inbegrip van de relevantie ervan in relatie tot onze risicobereidheid en bedrijfsimpact.

[kerngebieden kunnen onder meer omvatten: governance en risicobeheersing, operationeel beheer, continuïteitsbeheer, incidentmanagement, software- en systeemontwikkeling, risicobeheersing van derde aanbieders, weerbaarheidstesten en beveiligingsbeheer]

Veld	Toelichting
Bevinding-ID	[bijv. B-001]
Domein	[beschrijf het domein of de domeinen waarin de bevinding is geconstateerd]
Beschrijving	[beschrijf het zwakke punt, de tekortkoming of de lacune in detail]
Ernst	[bijv. kritiek/ hoog/ midden/ laag, met inbegrip van de impact van de bevinding op bedrijfsoperaties, kritieke functies of doelstellingen]
Onderbouwing van de ernstbeoordeling	[beschrijf de methodiek en onderbouwing die zijn gebruikt om de ernst te beoordelen]
Bron	[beschrijf de informatiebron(nen) die zijn gebruikt om het zwakke punt, de tekortkoming of de lacune te identificeren en te analyseren, met inbegrip van een verwijzing naar hoofdstuk 8]

[herhaal voor iedere bevinding]

4 Corrigerende maatregelen

Om geïdentificeerde zwakke punten, tekortkomingen en lacunes aan te pakken, zal [de financiële entiteit] de volgende maatregelen implementeren:

4.1 Samenvatting van maatregelen

Bevinding-ID	Maatregel-ID	Maatregelbeschrijving	Status	Prioriteit
[bijv. B-001]	[bijv. M-001]	[vat de maatregel samen]	[gepland/ in uitvoering/ afgerond]	[hoog/ midden/ laag]
[bijv. B-002]	[bijv. M-002]	[vat de maatregel samen]	[gepland/ in uitvoering/ afgerond]	[hoog/ midden/ laag]
[bijv. B-003]	[bijv. M-003]	[vat de maatregel samen]	[gepland/ in uitvoering/ afgerond]	[hoog/ midden/ laag]

4.2 Gedetailleerde beschrijving van maatregelen

Veld	Toelichting
Bevinding-ID	[bijv. B-001]
Maatregel-ID	[bijv. M-001]
Maatregelbeschrijving	[beschrijf de maatregel in detail]
Status	[gepland/ in uitvoering/ afgerond]
Streefdatum	[verwachte datum voor implementatie van de maatregel, met inbegrip van de prioriteit]
Controledatum	[verwachte datum voor interne controle van de maatregel]
Huidige voortgang	[beschrijf de huidige voortgang van de implementatie van de maatregel]
Risico op overschrijding van planning	[leg, indien van toepassing, uit of en waarom er een risico bestaat dat de planning niet wordt gehaald]
Gebruikte tools	[beschrijf, indien van toepassing, de interne en externe tools die voor deze maatregel worden gebruikt]
Verantwoordelijke functie	[beschrijf de interne of externe functie die verantwoordelijk is voor deze maatregel]
Impact	[beschrijf de impact van de in de maatregelen voorgenomen wijzigingen op de budgettaire, menselijke en materiële middelen van de financiële entiteit, met inbegrip van de afstemming op de

	risicobereidheid, de verwachte risicoreductie en de middelen bestemd voor de implementatie van corrigerende maatregelen]
Melding aan bevoegde autoriteit	[beschrijf, indien van toepassing, het proces om de bevoegde autoriteit te informeren]

[herhaal voor iedere maatregel]

4.3 Evaluatie van bevindingen waarvoor geen corrigerende maatregelen worden getroffen

[indien de financiële entiteit voor iedere bevinding maatregelen zal implementeren] Aangezien voor alle geïdentificeerde bevindingen corrigerende maatregelen worden getroffen, identificeert [de financiële entiteit] geen bevindingen waarvoor geen corrigerende maatregelen worden getroffen.

[indien er bevindingen zijn waarvoor de financiële entiteit geen maatregelen zal implementeren] Naast de geïdentificeerde bevindingen waarvoor corrigerende maatregelen worden getroffen, analyseert [de financiële entiteit] het restrisico voor de volgende bevindingen waarvoor geen corrigerende maatregelen worden getroffen:

Veld	**Toelichting**
Bevinding-ID	[bijv. B-001]
Criteria voor impact	[beschrijf in detail de criteria die zijn gebruikt om de impact van de bevinding te analyseren]
Impact	[beschrijf de impact van de in de maatregelen voorgenomen wijzigingen op de budgettaire, menselijke en materiële middelen van de financiële entiteit, met inbegrip van de middelen bestemd voor de implementatie van corrigerende maatregelen]
Criteria voor restrisico	[beschrijf de criteria die zijn gebruikt om het betrokken ICT-restrisico te evalueren]
Restrisico	[beschrijf het betrokken ICT-restrisico]
Criteria voor acceptatie	[beschrijf de criteria die zijn gebruikt om het betrokken restrisico te accepteren]
Acceptatie	[beschrijf de acceptatie van het betrokken restrisico]

[herhaal voor iedere bevinding]

4.4 Evaluatie van de cyclus voor ICT-risicobeheersing

[Naast de geïdentificeerde bevindingen en maatregelen voert de financiële entiteit een reflectieve beoordeling uit van de doeltreffendheid van de cyclus voor ICT-risicobeheersing. Deze beoordeling is gebaseerd op interviews met alle relevante stakeholders, met inbegrip van degenen belast met governance]:

[beschrijf de evaluatie op basis van opzetdoeltreffendheid, operationele doeltreffendheid, integratie binnen de organisatie, geïdentificeerde structurele zwakke punten, verbetermogelijkheden, etc.]

5 Toekomstige ontwikkelingen

Naast de in hoofdstuk 2 beschreven wijzigingen en verbeteringen identificeert en analyseert [de financiële entiteit] geplande en potentiële ontwikkelingen om de aard en potentiële impact daarvan op digitale operationele weerbaarheid, risicobeheersing en governance te beoordelen, inzicht te geven in de potentiële effecten van deze ontwikkelingen op [de financiële entiteit] en de relevantie daarvan voor risicoblootstelling, doeltreffendheid van beheersmaatregelen en de vereiste prioritering van verbeteracties.

5.1 Interne ontwikkelingen

[bijv. wijzigingen in de strategie voor digitale operationele weerbaarheid, het interne-controleraamwerk voor ICT of de governance voor ICT-risicobeheersing, etc., buiten de geïdentificeerde verbetermaatregelen]

- **[Ontwikkeling]:** [beschrijf de ontwikkeling, met inbegrip van de verwachte impact op risiconiveaus, beheersingsvereisten en prioritering van toekomstige maatregelen, wanneer de ontwikkeling zal plaatsvinden, hoe de ontwikkeling zal worden behandeld en wat de potentiële impact ervan zal zijn op de digitale operationele weerbaarheid, risicobeheersing en governance van de financiële entiteit]

  [herhaal voor iedere ontwikkeling]

5.2 Externe ontwikkelingen

[bijv. relevante opkomende technologieën, wet- en regelgeving, werkwijzen in de sector, etc., buiten de geïdentificeerde verbetermaatregelen]

- **[Ontwikkeling]:** [beschrijf de ontwikkeling, met inbegrip van de verwachte impact op risiconiveaus, beheersingsvereisten en prioritering van toekomstige maatregelen, wanneer de ontwikkeling zal plaatsvinden, hoe de ontwikkeling zal worden behandeld en wat de potentiële impact ervan zal zijn op de digitale operationele weerbaarheid, risicobeheersing en governance van de financiële entiteit]

  [herhaal voor iedere ontwikkeling]

6 Conclusies

Op basis van het uitgevoerde evaluatieproces, de beschreven bevindingen en corrigerende maatregelen concludeert [de financiële entiteit] dat [geef de algemene conclusies die voortvloeien uit de evaluatie van het raamwerk voor ICT-risicobeheersing, waaronder een beoordeling van de volwassenheid ten opzichte van interne of externe raamwerken, een expliciet algemeen oordeel over de adequaatheid en doeltreffendheid van het raamwerk voor ICT-risicobeheersing, een samenvatting van de belangrijkste risico's en tekortkomingen in beheersmaatregelen en een vooruitblik op vereiste verbeteringen]

Algemeen oordeel:
[adequaat/ gedeeltelijk adequaat/ inadequaat/ andere door de financiële entiteit gedefinieerde classificatie]

7 Eerdere evaluaties

[wanneer dit het eerste gedocumenteerde verslag is] Er zijn geen eerder gedocumenteerde evaluatieverslagen.

[wanneer er een vorig verslag beschikbaar is] Hieronder is een lijst opgenomen van de eerder gedocumenteerde evaluatieverslagen:

Verslag #	Evaluatieperiode	Datum van goedkeuring	Reden voor evaluatie
[bijv. 1]	[start - einde]	[DD/MM/JJJJ]	[jaarlijks, naar aanleiding van een ernstig ICT-gerelateerd incident, naar aanleiding van instructies van toezichthouders, etc.]
[bijv. 2]	[start - einde]	[DD/MM/JJJJ]	[jaarlijks, naar aanleiding van een ernstig ICT-gerelateerd incident, naar aanleiding van instructies van toezichthouders, etc.]

[herhaal voor alle eerdere verslagen]

7.1 Samenvatting van eerdere corrigerende maatregelen

[wanneer dit het eerste gedocumenteerde verslag is] Aangezien er geen eerder gedocumenteerde evaluatieverslagen zijn, zijn er geen eerdere corrigerende maatregelen te beschrijven.

[wanneer er een vorig verslag beschikbaar is] Hieronder is een lijst opgenomen van corrigerende maatregelen die voortvloeien uit eerder gedocumenteerde evaluatieverslagen:

Verslag #	Maatregel-ID	Maatregelbeschrijving	Status	Streefdatum
[bijv. 1]	[bijv. M-001]	[vat de maatregel samen]	[beschrijf de huidige stand van implementatie]	[DD/MM/JJJJ]
[bijv.2]	[bijv. M-001]	[vat de maatregel samen]	[beschrijf de huidige stand van implementatie]	[DD/MM/JJJJ]

[herhaal voor alle eerdere maatregelen]

7.2 Ondoeltreffende eerdere corrigerende maatregelen

[wanneer dit het eerste gedocumenteerde verslag is] Aangezien er geen eerder gedocumenteerde evaluatieverslagen zijn, zijn er geen ondoeltreffende eerdere corrigerende maatregelen te beschrijven.

[wanneer er een vorig verslag beschikbaar is en alle eerdere corrigerende maatregelen doeltreffend zijn gebleken en niet tot onverwachte uitdagingen hebben geleid] Aangezien alle eerdere corrigerende maatregelen doeltreffend zijn gebleken en niet tot onverwachte uitdagingen hebben geleid, hoeven deze niet te worden verbeterd.

[wanneer er een vorig verslag beschikbaar is en niet alle eerdere corrigerende maatregelen doeltreffend zijn gebleken of wanneer zij tot onverwachte uitdagingen hebben geleid] Met betrekking tot het overzicht van eerdere corrigerende maatregelen in hoofdstuk 7.1 zijn de volgende corrigerende maatregelen ondoeltreffend gebleken of hebben zij tot onverwachte uitdagingen geleid:

Veld	**Toelichting**
Verslag #	[bijv. 1]
Maatregel-ID	[bijv. M-001]
Issue	[maatregel is ondoeltreffend gebleken/ maatregel heeft tot onverwachte uitdagingen geleid]
Beschrijving van het issue	[beschrijf het issue in detail]
Verbetering	[beschrijf hoe de maatregel kan worden verbeterd of gewijzigd om de doeltreffendheid te vergroten of uitdagingen te verhelpen]

[herhaal voor iedere maatregel]

8 Informatiebronnen

In dit evaluatieverslag heeft [de financiële entiteit] verwezen naar gebruikte bronnen. Deze bronnen worden hieronder opgenomen en nader beschreven:

[bronnen dienen de uitkomsten van interne audits, de uitkomsten van compliancebeoordelingen, de uitkomsten van testen van digitale operationele weerbaarheid en, waar van toepassing, de uitkomsten van geavanceerde testen op basis van Threat-Led Penetration Testing (TLPT) van ICT-tools, -systemen en -processen en externe bronnen te omvatten]

Bron	**Beschrijving**	**Gebruik**
[bijv. uitkomsten van interne audits]	[beschrijf de bron]	[beschrijf het gebruik van de bron voor dit evaluatieverslag]
[bijv. uitkomsten van compliancebeoordelingen]	[beschrijf de bron]	[beschrijf het gebruik van de bron voor dit evaluatieverslag]
[bijv. uitkomsten van testen van digitale operationele weerbaarheid]	[beschrijf de bron]	[beschrijf het gebruik van de bron voor dit evaluatieverslag]

[herhaal voor iedere informatiebron]