Bijlage 3 - Rapport van de Risicobeoordeling en Risicobehandeling

Comment [DK1]: Om te leren hoe dit document in te vullen, bekijk handleiding videonadleiding "How to Write ISO 27001 Risk Assessment Report"
- Indien u de toolkit koopt, dan vindt u het in het ISO 27001 & ISO 22301 Klantenportaal: https://epps.customerhub.net/
- Indient u de toolkit niet hebt gekocht, dan vindt u de preview van de handlelding hier: http://www.iso27001standard.com/how-to-write-iso-27001-risk-assessment-report

Versieblad

Datum	Versie	Gemaakt door	Omschrijving van de aanpassing
DD/MM/JJJJ	0.1	Dejan Kosutic	Concept basisdocument

Inhoudsopgave

1. Doel, toepassingsgebied en gebruikers

Het doel van dit document is een gedetailleerd overzicht te geven van het proces en de documenten die worden gebruikt tijdens de risicobeoordeling en -behandeling van informatierisico's in [naam organisatie]in de periode [specificeer periode].

Risicobeoordeling was toegepast op het gehele Managementsysteem van Informatiebeveiliging (ISMS).

Dit document is bedoeld voor het topmanagement van [naam organisatie], [functie verantwoordelijk voor informatiebeveiliging], eigenaren van informatiebedrijfsmiddelen, en iedereen betrokken in planning, implementatie, bewaking en verbetering van het ISMS.

2. Gerefereerde documenten

- ISO/IEC 27001 norm, clausules 8.2 en 8.3
- Document Toepassingsgebied ISMS
- Informatiebeveiligingsbeleid
- Methodologie voor Risicobeoordeling en Risicobehandeling

3. Proces van beoordeling en behandeling van informatierisico's

Het gehele proces van risicobeoordeling en risicobehandeling is uitgevoerd volgens het document Methodologie voor Risicobeoordeling en Risicobehandeling.

3.1. Doel van risicobeheer

Het doel van risicobeheer is het identificeren van alle bedrijfsmiddelen, hun kwetsbaarheden en bedreigingen die zowel deze kwetsbaarheden kunnen aantasten, als ook om deze parameters te evalueren teneinde de kritieke factor van de afzonderlijke risico's vast te stellen.

Het doel van risicobehandeling is om systematische manieren voor vermindering of beheersing van zulke risico's te definiëren.

3.2. Toepassingsgebied van risicobeoordeling en risicobehandeling

Risicobeoordeling en risicobehandeling worden uitgevoerd [naam van de organisatieonderdelen], in overeenstemming met het Document Toepassingsgebied ISMS.

3.3. Periode

Risicobeoordeling werd geïmplementeerd in de periode van [dag/maand/jaar] tot [dag/maand/jaar]. Risicobehandeling werd geïmplementeerd van [dag/maand/jaar] tot [dag/maand/jaar]. Definitieve rapporten opgesteld in de loop van [specifeer periode].

3.4. Deelnemers in het proces en verzameling van informatie

Het proces van risicobeoordeling en risicobehandeling werd beheerd door [naam en functie], met deskundige hulp van [indien gebruik is gemaakt van deskundige hulp, vermeld dan naam en bedrijf].

In de loop van de risicobeoordeling werd informatie verzameld door vragenlijsten en interviews met verantwoordelijken, d.w.z. eigenaren van bedrijfsmiddelen vanuit alle organisatieonderdelen.

Comment [DK2]: Of beschrijf enig andere methode indien gebruikt.

3.5. Beknopt overzicht van de toegepaste methodologie

Beknopt, het proces werd op de volgende wijze uitgevoerd:

- alle informatiebedrijfsmiddelen werden geïdentificeerd als ook de eigenaren
- bedreigingen werden voor elk bedrijfsmiddel geïdentificeerd, en corresponderende kwetsbaarheden werden voor elke bedreiging geïdentificeerd
- risico-eigenaren werden geïdentificeerd voor elk risico
- gevolgen van verlies van vertrouwelijkheid, integriteit en beschikbaarheid werden geëvalueerd door het gebruik van de waarden 0 tot 2
- de waarschijnlijkheid van het optreden van het risico, d.w.z. dat de bedreiging de kwetsbaarheid zal aantasten, werd geëvalueerd door het gebruik van de waarden 0 to 2
- het risiconiveau was berekend door de gevolgen van en waarschijnlijkheid bij elkaar op te tellen
- de waarden 3 en 4 werden bepaald als onacceptabele risico's
- voor elke onacceptabel risico werd een risicobehandeling bedacht, en maatregelen die het risico tot een acceptabel risico konden terugbrengen werden geselecteerd uit Bijlage A van de ISO/IEC 27001 norm
- nadat de maatregelen werden toegepast, werden de restrisico's beoordeeld

3.6. Overzicht van document gebruikt tijdens het proces van risicobeoordeling en risicobehandeling

De volgende documenten werden gebruikt of opgesteld tijdens de implementatie van de risicobeoordeling en risicobehandeling:

- Tabel voor Risicobeoordeling (Bijlage 1) - toont voor elke combinatie van bedrijfsmiddelen, kwetsbaarheden en bedreigingen, de waarden van gevolgen en waarschijnlijkheid, en berekent het risico
- Tabel voor Risicobehandeling (Bijlage 2) - toont de opties van risicobehandeling, selectie van maatregelen voor onacceptabele risico's, en het niveau van restrisico's

4. Geldigheid en documentbeheer

Dit document is geldig vanaf [datum]. Eigenaar van dit document is [functie].

5. Bijlagen

- Bijlage 1: Tabel voor Risicobeoordeling
- Bijlage 2: Tabel voor Risicobehandeling

[functie]

[naam]

_____

[handtekening]

Comment [DK3]: Alleen indien de Procedure voor Beheersing van Documenten en Registraties voorschrijft dat papieren documenten worden ondertekend.