Hoe operationaliseer ik de BIC?

Baseline
Informatiebeveiliging
Corporaties

UTRECHT, 14 November 2017.

Code voor Informatiebeveiliging

- NEN/ISO 27001;
  Informatietechnologie - Beveiligingstechnieken - Managementsystemen voor Informatiebeveiliging – Eisen
- NEN/ISO 27002;
  Informatietechnologie - Beveiligingstechnieken - Praktijkrichtlijn met beheersmaatregelen op het gebied van informatiebeveiliging

Baseline Informatiebeveiliging Corporaties

- Wat is de BIC:
  - Een methodiek om te komen tot implementatie van een beheer(sings)syteem voor informatiebeveiliging voor woningcorporaties. Een ISMS.
  - Een richtlijn om te komen tot een volledige en integrale Informatiebeveiliging.
  - In lijn met BIG en BIR, respectievelijk de Baseline Informatiebeveilging voor Gemeenten en Rijksoverheid.

Baseline Informatiebeveiliging Corporaties

- Wat is de BIC niet:
  - Verplicht, maar meer dan aanbevelingswaardig in relatie tot Governance.
  - Alomvattend, een richting, kaders, maar het blijft het werk van mensen, procedures en processen
  - Een risicomonitor
  - Een kennisbank

CorpoNet

Daarom: NEN/ISO 27002

- Een handvat om per hoofdbeveiligings-categorie de juiste afweging te maken in termen van beheerdoelstellingen en beheersmaatregelen.
- Een richtlijn voor implementatie van mitigerende maatregelen.

Informatiebeveiligingsbeleid

- Aansturing door de directie van de informatiebeveiliging
- Beleidsregels voor informatiebeveiliging
- Beoordeling van het informatiebeveiligingsbeleid

Organiseren van informatiebeveiliging

- Interne organisatie
  - Rollen en verantwoordelijkheden bij informatiebeveiliging
  - Scheiding van taken
  - Contact met overheidsinstanties
  - Contact met speciale belangengroepen
  - Informatiebeveiliging in projectbeheer
- Mobiele apparatuur en telewerken
  - Beleid voor mobiele apparatuur
  - Telewerken

Veilig personeel

- Voorafgaand aan het dienstverband
  - Screening
  - Arbeidsvoorwaarden
- Tijdens het dienstverband
  - Directieverantwoordelijkheden
  - Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging
  - Disciplinaire procedure
- Beëindiging en wijziging van dienstverband
  - Beëindiging of wijziging van verantwoordelijkheden van het dienstverband

CorpoNet

Beheer van bedrijfsmiddelen

- Verantwoordelijkheid voor bedrijfsmiddelen
  - Inventariseren van bedrijfsmiddelen
  - Eigendom van bedrijfsmiddelen
  - Aanvaardbaar gebruik van bedrijfsmiddelen
  - Teruggeven van bedrijfsmiddelen
- Informatieclassificatie
  - Classificatie van informatie
  - Informatie labelen
  - Behandelen van bedrijfsmiddelen
- Behandelen van media
  - Beheer van verwijderbare media
  - Verwijderen van media
  - Media fysiek overdragen

Toegangsbeveiliging

- Bedrijfseisen voor toegangsbeveiliging
  - Beleid voor toegangsbeveiliging
  - Toegang tot netwerken en netwerkdiensten
- Beheer van toegangsrechten van gebruikers
  - Registratie en afmelden van gebruikers
  - Gebruikers toegang verlenen
  - Beheren van speciale toegangsrechten
  - Beheer van geheime authenticatie-informatie van gebruikers
  - Beoordeling van toegangsrechten van gebruikers
  - Toegangsrechten intrekken of aanpassen
- Verantwoordelijkheden van gebruikers
  - Geheime authenticatie-informatie gebruiken
  - Toegangsbeveiliging van systeem en toepassing
  - Beperking toegang tot informatie
  - Beveiligde inlogprocedures
  - Systeem voor wachtwoordbeheer
  - Speciale systeemhulpmiddelen gebruiken
  - Toegangsbeveiliging op programmabroncode

Cryptografie

- Cryptografische beheersmaatregelen
  - Beleid inzake het gebruik van cryptografische beheersmaatregelen
  - Sleutelbeheer

Fysieke beveiliging en beveiliging van de omgeving

- Beveiligde gebieden
  - Fysieke beveiligingszone
  - Fysieke toegangsbeveiliging
  - Kantoren, ruimten en faciliteiten beveiligen
  - Beschermen tegen bedreigingen van buitenaf
  - Werken in beveiligde gebieden
  - Laad- en loslocatie
- Apparatuur
  - Plaatsing en bescherming van apparatuur
  - Nutsvoorzieningen
  - Beveiliging van bekabeling
  - Onderhoud van apparatuur
  - Verwijdering van bedrijfsmiddelen
  - Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein
  - Veilig verwijderen of hergebruiken van apparatuur
  - Onbeheerde gebruikersapparatuur
  - ‘Clear desk’- en ‘clear screen’-beleid

CorpoNet

Beveiliging bedrijfsvoering

- Bedieningsprocedures en verantwoordelijkheden
  - Gedocumenteerde bedieningsprocedures
  - Wijzigingsbeheer
  - Capaciteitsbeheer
  - Scheiding van ontwikkel-, test- en productieomgevingen
- Bescherming tegen malware
  - Beheersmaatregelen tegen malware
- Back-up
  - Back-up van informatie
- Verslaglegging en monitoren
  - Gebeurtenissen registreren
  - Beschermen van informatie in logbestanden
  - Logbestanden van beheerders en operators
  - Kloksynchronisatie
- Beheersing van operationele software
  - Software installeren op operationele systemen
- Beheer van technische kwetsbaarheden
  - Beperkingen voor het installeren van software
- Overwegingen betreffende audits van informatiesystemen
  - Beheersmaatregelen betreffende audits van informatiesystemen

CorpoNet

Communicatiebeveiliging

- Beheer van netwerkbeveiliging
  - Beheersmaatregelen voor netwerken
  - Beveiliging van netwerkdiensten
  - Scheiding in netwerken
- Informatietransport
  - Beleid en procedures voor informatietransport
  - Overeenkomsten over informatietransport
  - Elektronische berichten
  - Vertrouwelijkheids- of geheimhoudingsovereenkomst

Acquisitie, ontwikkeling en onderhoud van informatiesystemen

- Beveiligingseisen voor informatiesystemen
  - Analyse en specificatie van informatiebeveiligingseisen
  - Toepassingen op openbare netwerken beveiligen
  - Transacties van toepassingen beschermen
- Beveiliging in ontwikkelings- en ondersteunende processen
  - Beleid voor beveiligd ontwikkelen
  - Procedures voor wijzigingsbeheer met betrekking tot systemen
  - Technische beoordeling van toepassingen na wijzigingen besturingsplatform
  - Beperkingen op wijzigingen aan softwarepakketten
  - Principes voor engineering van beveiligde systemen
  - Beveiligde ontwikkelomgeving Uitbestede softwareontwikkeling
  - Testen van systeembeveiliging
  - Systeemacceptatietests
- Testgegevens
  - Bescherming van testgegevens

Leveranciersrelaties

- Informatiebeveiliging in leveranciersrelaties
  - Informatiebeveiligingsbeleid voor leveranciersrelaties
  - Opnemen van beveiligingsaspecten in leveranciersovereenkomsten
  - Toeleveringsketen van informatie- en communicatietechnologie
- Beheer van dienstverlening van leveranciers
  - Monitoring en beoordeling van dienstverlening van leveranciers
  - Beheer van veranderingen in dienstverlening van leveranciers

Beheer van informatie-beveiligingsincidenten

- Beheer van informatiebeveiligingsincidenten en –verbeteringen
  - Verantwoordelijkheden en procedures
  - Rapportage van informatiebeveiligingsgebeurtenissen
  - Rapportage van zwakke plekken in de informatiebeveiliging
  - Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen
  - Respons op informatiebeveiligingsincidenten
  - Lering uit informatiebeveiligingsincidenten
  - Verzamelen van bewijsmateriaal

Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer

- Informatiebeveiligingscontinuïteit
  - Informatiebeveiligingscontinuïteit plannen
  - Informatiebeveiligingscontinuïteit implementeren
  - Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren
- Redundante componenten
  - Beschikbaarheid van informatieverwerkende faciliteiten

Naleving

- Naleving van wettelijke en contractuele eisen
  - Vaststellen van toepasselijke wetgeving en contractuele eisen Intellectuele-eigendomsrechten
  - Beschermen van registraties
  - Privacy en bescherming van persoonsgegevens Voorschriften voor het gebruik van cryptografische beheersmaatregelen
- Informatiebeveiligingsbeoordelingen
  - Onafhankelijke beoordeling van informatiebeveiliging
  - Naleving van beveiligingsbeleid en -normen Beoordeling van technische naleving

CorpoNet

Handreiking

Informatiebeveiligingsbeleid
Aansturing door de directie van de informatiebeveiliging
Doelstelling: Het verschaffen van directieaansturing van en –steun voor informatiebeveiliging in overeenstemming met bedrijfseisen en relevante wet- en regelgeving.

Organiseren van informatiebeveiliging
Interne organisatie
Doelstelling: Een beheerkader vaststellen om de implementatie en uitvoering van de informatiebeveiliging binnen de organisatie te initiëren en te beheersen.
Mobiele apparatuur en telewerken
Doelstelling: Het waarborgen van de veiligheid van telewerken en het gebruik van mobiele apparatuur.

Veilig personeel
Voorafgaand aan het dienstverband
Doelstelling: Waarborgen dat medewerkers en contractanten hun verantwoordelijkheden begrijpen en geschikt zijn voor de functies waarvoor zij in aanmerking komen.
Tijdens het dienstverband
Doelstelling: Ervoor zorgen dat medewerkers en contractanten zich bewust zijn van hun verantwoordelijkheden op het gebied van informatiebeveiliging en deze nakomen.
Beëindiging en wijziging van dienstverband
Doelstelling: Het beschermen van de belangen van de organisatie als onderdeel van de wijzigings- of beëindigingsprocedure van het dienstverband.

Handreiking

1. Maak per hoofbeveiligingscategorie;
2. Per beveiligingscategorie;
3. Per doelstelling:

- Een GAP analyse
  - Wat is de huidige, actuele situatie (IST)
  - Waar wil ik naar toe als beveilgingsniveau (SOLL)
  - Wat betekent dat in activiteiten (PROGRAMMA)

CorpoNet

Een programma is meer dan een project

CorpoNet