Preview

Informatie-Beveiligingsbeleid

NEN-ISO/IEC 27002 (CvI / BIG)

*

Gemeentelijk Efficiency Adviesbureau bv
Schoonouwenseweg 10
2821 NX Stolwijk
☎0182-341350
info@gea-bv.nl

---

* Versie: preview
Datum: oktober 2014

INHOUDSOPGAVE

0 Inleiding

De huidige stand van technologie biedt ons de mogelijkheid om onze zaken veelal elektronisch af te handelen. We wisselen e-mails uit en kunnen elektronisch winkelen. Gegevens worden met behulp van de meest uiteenlopende communicatiemedia uitgewisseld en komen in diverse systemen bij verschillende organisaties voor. We zijn afhankelijk van technologie. Welke gevaren voor onze persoonlijke levenssfeer de toepassing van deze technologie in werkelijkheid met zich meebrengt, is vaak nog onbekend.

Sinds het begin van de jaren tachtig probeert de overheid de privacy van de burgers in de huidige informatiemaatschappij met bijzondere wet- en regelgeving te beschermen.

Het Europese parlement en de Raad van de Europese Unie hebben daarom een richtlijn vastgelegd.

Met de Wet Bescherming Persoonsgegevens (WBP) wordt deze richtlijn in Nederland uitgevoerd. De WBP dicteert een aantal dwingende normen over de verwerking van en omgang met persoonsgegevens.
Waar persoonsgegevens geautomatiseerd worden verwerkt, is het beveiligen van de daarbij gebruikte informatiesystemen een noodzakelijke voorwaarde om aan de doelstellingen van de wet te voldoen.

In toenemende mate worden informatiesystemen, zowel openbare als private netwerken, onderling verbonden. De onderlinge verbondenheid en het delen van informatiemiddelen maken het steeds moeilijker om de toegang te beveiligen.
Veel informatiesystemen zijn niet ontworpen met het oog op veiligheid. De beveiliging die met technische middelen kan worden bereikt is begrensd en dient te worden ondersteund door passende maatregelen en procedures.

Als uitgangspunt voor de informatiebeveiliging is de internationaal gehanteerde Code voor Informatiebeveiliging (Nederlandse versie van het NEN-ISO/IEC 27002) gebruikt. Deze code is goed toepasbaar voor de gemeentelijke situatie. De Informatiebeveiligingsdienst voor gemeenten (IBD) heeft deze standaard ook gebruikt bij het opstellen van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).
Het rapport “Beveiliging van persoonsgegevens” (achtergrondstudies en verkenningen 23) van het College Bescherming Persoonsgegevens is mede gebruikt bij de opzet van dit document.
Alleen door bewust te werken aan informatiebeveiliging en mensen expliciet op hun taken, verantwoordelijkheden en bevoegdheden te wijzen, kunnen een aantal essentiële stappen gezet worden in dit traject.

0.1 Wat is informatiebeveiliging?

Informatiebeveiliging beschermt informatie tegen bedreigingen die de bedrijfsvoering in gevaar (kunnen) brengen. Deze bescherming voorkomt of beperkt eventuele schade voor de organisatie, waardoor het rendement van investeringen vergroot en de kansen voor de organisatie geoptimaliseerd worden. Afhankelijk van de vorm waarin de informatie gepresenteerd wordt, dienen altijd passende beveiligingsmaatregelen toegepast te worden.

De beveiligingsmaatregelen worden bezien vanuit de twee gezichtspunten.

Deze zijn:

- Technische maatregelen: Dit zijn logische en fysieke maatregelen in en rondom de informatiesystemen. Hierbij valt te denken aan toegangscontroles, vastlegging van informatiegebruik, brandpreventie, back-upvoorzieningen enz.
- Organisatorische maatregelen: Deze maatregelen zijn gericht op de inrichting van de organisatie en het verwerken van informatie. Zoals het toekennen en definiëren van

verantwoordelijkheden, bevoegdheden en taken, het geven van instructies en trainingen en het opstellen van calamiteitenplannen.

0.2 Waarom informatiebeveiliging nodig is

Voor een gemeentelijke organisatie is informatie één van de meest waardevolle bedrijfsmiddelen dat voortdurend op een passende manier beveiligd moet zijn.

De minimale eisen waaraan de informatiebeveiliging moet voldoen, worden bepaald door de nationale en internationale wet- en regelgeving.

In geval van calamiteiten of een ramp moeten de bestuurders en hulpdiensten worden voorzien van betrouwbare informatie vanuit de gemeentelijke organisatie. Te denken valt dan aan persoonsgegevens, vastgoedinformatie omtrent eigenaar en gebruiker, bouwvergunningen en milieugegevens van bedrijven. De informatie die we in onze organisatie hebben en beheren is van vitaal belang voor onze eigen bedrijfsprocessen en voor onze afnemers.

In toenemende mate worden organisaties en hun informatiestromen en netwerken geconfronteerd met beveiligingsrisico's uit allerlei bronnen, zoals fraude, vandalisme, brand etc. Daarbij komen dan nog eens de nieuwe oorzaken van schade zoals computervirussen, hacking en verhinderen van dienstverlening. Deze nieuwe oorzaken worden steeds verder verfijnd en steeds ambitieuzer.

De toenemende afhankelijkheid van informatiesystemen en –diensten impliceert ook dat de organisatie steeds kwetsbaarder wordt voor bedreigingen ten aanzien van de beveiliging.

nformatie is waardevol. Dit kunnen we o.a. ook concluderen uit alle commotie die in 2010 is ontstaan rondom het vrijgeven van geheime informatie op Wikileaks. Of men het er nu mee eens is of niet, de informatie die is vrijgegeven heeft een enorme impact gehad op de wereld en een verandering in gang gezet. Ook in Nederland kunnen we zien dat informatie en de waarde die daaraan vastzit een cruciale rol heeft gespeeld bij bijvoorbeeld het omvallen van de DSB-bank.

0.3 Opstellen van beveiligingseisen

Om tot een beveiligingsbeleid te komen, dient een organisatie eerst haar beveiligingsbehoeften te bepalen. We kunnen de volgende bronnen onderscheiden:

1. De risico's die een organisatie loopt. Via een risicoanalyse worden de bedreigingen ten aanzien van bedrijfsmiddelen vastgesteld en wordt bepaald wat hiervan de effecten kunnen zijn en hoe groot de waarschijnlijkheid is dat een bedreiging zich voordoet;
2. Het geheel aan wettelijke, regulerende en contractuele eisen waaraan de organisatie dient te voldoen;
3. Het stelsel van principes, doelstellingen en eisen voor het verwerken van informatie die de organisatie heeft ontwikkeld ter ondersteuning van haar bedrijfsvoering.

0.4 Inschatting van beveiligingsrisico’s

Door beoordeling van de bedrijfsrisico's kan vastgesteld worden wat de beveiligingsbehoefte is.

Vervolgens dienen de kosten van de beveiligingsmaatregelen te worden afgewogen tegen de schade die ontstaat door beveiligingsincidenten en de waarschijnlijkheid dat het incident zich voordoet.
Technieken om de bedrijfsrisico’s in kaart te brengen kunnen worden toegepast op de

gehele organisatie, onderdelen daarvan, maar ook op individuele informatiesystemen of specifieke netwerkcomponenten.
Op basis van de resultaten van de risicoanalyse kan vastgesteld worden welke activiteiten het management/bestuur dient te ondernemen. Direct daaraan gerelateerd worden de prioriteiten vastgesteld.
Het eerder aangehaalde document “Beveiliging van persoonsgegevens” van het CBP heeft maatregelen gerangschikt naar de volgende categorieën:

1. Beveiligingsbeleid, beveiligingsplan en implementatie van het stelsel van procedures en maatregelen
2. Administratieve organisatie
3. Beveiligingsbewustzijn
4. Eisen te stellen aan personeel
5. Inrichting van de werkplek
6. Beheer en classificatie van de IT-infrastructuur
7. Toegangsbeheer en –controle
8. Netwerken en externe verbindingen
9. Gebruik van software
10. Bulkverwerking van gegevens
11. Bewaren van gegevens
12. Vernietiging van gegevens
13. Calamiteitenplan
14. Uitbesteding van verwerking van persoonsgegevens.

Deze indeling kan de basis vormen voor een risicoanalyse.

Na implementatie van beveiligingsmaatregelen dient er een periodieke evaluatie plaats te vinden. Op deze wijze kan:

1. ingespeeld worden op wijzigingen in bedrijfsbehoeften en prioriteiten;
2. bepaald worden wat nieuwe bedreigingen en kwetsbaarheden zijn;
3. vastgesteld worden dat maatregelen wellicht niet meer relevant zijn, niet meer effectief of geschikt zijn, zodat aanpassing c.q. vernieuwing van de maatregelen mogelijk is.

De risicoanalyse wordt vaak op een top-down werkwijze aangepakt. Op het hoogste niveau binnen de organisatie worden de prioriteiten vastgesteld, terwijl op een lager niveau de specifieke risico's aangepakt worden (bijv. op afdelingsniveau of per registratie).

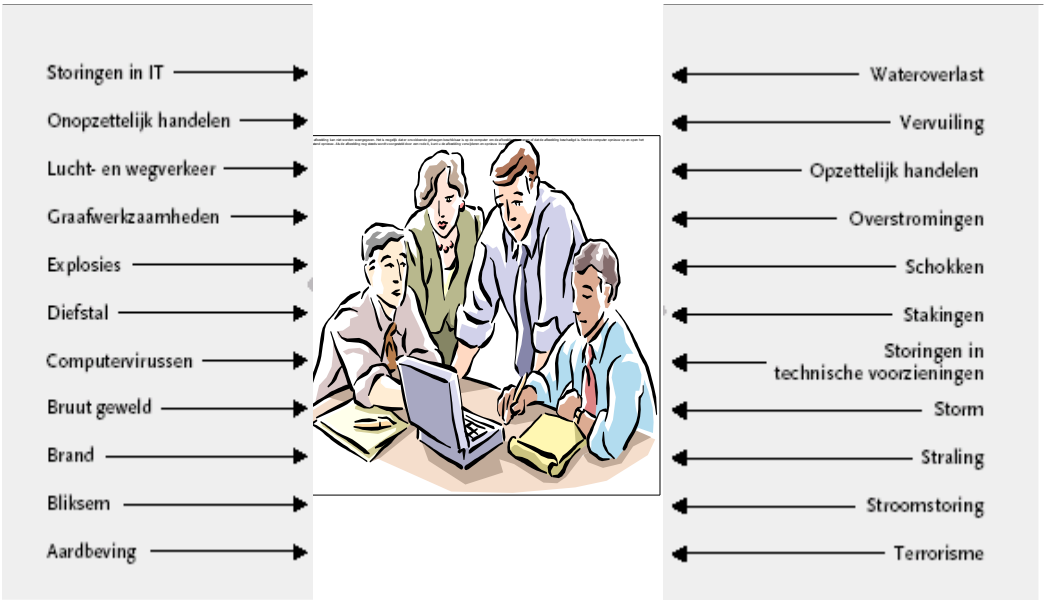
0.5 Beveiligingsmaatregelen selecteren

Er zijn verschillende risico’s te onderkennen, die ertoe kunnen leiden dat verwerkingsprocessen stagneren. Of nog erger, verlies van informatie of onrechtmatig gebruik van gegevens teweeg brengen.

Het beveiligingsniveau dient wel “passend” te zijn, m.a.w. er moet evenwicht zijn in de kosten, de stand van de techniek en de risico’s die daarbij worden gelopen.

Niet alle maatregelen die genomen worden zullen betrekking hebben op alle systemen, het is heel goed mogelijk dat er een breed scala aan maatregelen genomen dient te worden voor slechts één systeem, terwijl een beperkt aantal maatregelen juist weer betrekking kan

hebben op het merendeel van de systemen.
Een voorbeeld van maatregelen die getroffen kan worden, is het invoeren van een duidelijke functiescheiding.



Implementatie van het beveiligingsbeleid gebeurt niet dagelijks en wijkt sterk af van de reguliere werkzaamheden.

Het implementatieplan dient dan ook **SMART** te zijn:

Specifiek: Heldere doelstelling, de effecten en prestaties zijn eenduidig en duidelijk omschreven.

Meetbaar : Voor het meten van de effecten en prestaties zijn indicatoren gedefinieerd.

Acceptabel : De projectleden zijn akkoord met de doelstellingen en de wijze van uitvoer.

Realistisch : De doelstellingen moeten te realiseren zijn met de geboden tijd en middelen.

Tijdsgebonden : Voor wat betreft de planning moet het duidelijk zijn welk onderdeel wanneer afgerond is.

0.6 Startpunt van informatiebeveiliging

De driejaarlijkse verplichte GBA-audit heeft de aanzet gegeven om een informatiebeveiligingsbeleid op te stellen. Omdat de nadruk lag op de GBA is er in vele situatie alleen een beleid geschreven gericht op de eisen voor de GBA-audit en toegespitst op Burgerzaken en de noodzakelijke ICT-componenten.

Door de invoering van de diverse basisregistraties is het noodzakelijk dat er een gemeentebreed beveiligingsbeleid wordt opgesteld.
Als uitgangspunt voor dit beleidsdocument en alle onderliggende handboeken is gebruik gemaakt van de indeling zoals is gedefinieerd in de NEN-ISO/IEC 27002 standaard. . Deze norm is ook gebruikt door de Informatiebeveiligingsdienst voor gemeenten (IBD) bij het opstellen van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

0.7 Kritische succesfactoren

Uit de ervaring van bedrijven die informatiebeveiliging recent hebben ingevoerd blijken de volgende factoren van belang te zijn voor een geslaagde implementatie van de informatiebeveiliging :

1. beveiligingsbeleid, doelstellingen en activiteiten die de bedrijfsdoelstellingen weerspiegelen;
2. een benadering ten aanzien van het implementeren van beveiligingsmaatregelen die past binnen de organisatiecultuur;
3. zichtbare steun en betrokkenheid van het management;
4. een goed begrip van beveiligingseisen, risicoanalyse en risicomanagement;
5. een effectieve marketing van het thema beveiliging aan alle managers en werknemers;
6. het verstrekken van richtlijnen over beveiligingsbeleid en –normen aan alle werknemers en leveranciers;
7. het verzorgen van passende training en opleidingen;
8. een compleet en evenwichtig meetsysteem, dat gebruikt wordt om de effectiviteit van het management van de informatiebeveiliging te beoordelen en suggesties ter verbetering aandraagt.

0.8 Het ontwikkelen van bedrijfseigen richtlijnen

De gemeente als lokale overheid ontwikkeld geen eigen richtlijnen. Daar waar mogelijk wordt aangesloten bij landelijke richtlijnen opgesteld door erkende organisaties, zoals bij dit document is toegepast, of van overheidswege voorgeschreven dan wel aangereikte richtlijnen.

1 Onderwerp en toepassingsgebied

2 Termen en definities

3 Structuur van deze norm

3.1 Hoofdstukken

3.2 Hoofdbeveiligingscategorieën

4 Risicobeoordeling en risicobehandeling

4.1 Beoordelen van de beveiligingsrisico's

4.2 Behandelen van beveiligingsrisico's

5 Beveiligingsbeleid

5.1 Informatiebeveiligingsbeleid

5.1.1 Beleidsdocument voor informatiebeveiliging

5.1.2 Beoordeling van informatiebeveiligingsbeleid

6 Organisatie van informatiebeveiliging

6.1 Interne organisatie

6.1.1 Betrokkenheid van de directie bij informatiebeveiliging

6.1.2 Coördinatie van informatiebeveiliging

6.1.3 Toewijzing van verantwoordelijkheden voor informatiebeveiliging

6.1.4 Goedkeuringsproces voor IT-voorzieningen

6.1.5 Geheimhoudingsovereenkomst

6.1.6 Contact met overheidsinstanties

6.1.7 Contact met speciale belangengroepen

6.1.8 Onafhankelijke beoordeling van informatiebeveiliging

6.2 Externe partijen

6.2.1 Identificatie van risico's die betrekking hebben op externe partijen

6.2.2 Beveiliging behandelen in de omgang met klanten

6.2.3 Beveiliging in overeenkomsten met een derde partij

7 Beheer van bedrijfsmiddelen

7.1 Verantwoordelijkheid voor bedrijfsmiddelen

7.1.1 Inventarisatie van bedrijfsmiddelen

7.1.2 Eigendom van bedrijfsmiddelen

7.1.3 Aanvaardbaar gebruik van bedrijfsmiddelen

7.2 Classificatie van informatie

7.2.1 Richtlijnen voor classificatie

7.2.2 Labeling en verwerking van informatie

8 Beveiliging van personeel

8.1 Voorafgaand aan het dienstverband

8.1.1 Rollen en verantwoordelijkheden

8.1.2 Screening

8.1.3 Arbeidsvoorwaarden

8.2 Tijdens het dienstverband

8.2.1 Directieverantwoordelijkheid

8.2.2 Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging

8.2.3 Disciplinaire maatregelen

8.3 Beëindiging of wijziging van het dienstverband

8.3.1 Beëindiging van verantwoordelijkheden

8.3.2 Retournering van bedrijfsmiddelen

8.3.3 Blokkering van toegangsrechten

9 Fysieke beveiliging en beveiliging van de omgeving

9.1 Beveiliging van ruimten

9.1.1 Fysieke beveiliging van de omgeving

9.1.2 Fysieke toegangsbeveiliging

9.1.3 Beveiliging van kantoren, ruimten en faciliteiten

9.1.4 Bescherming tegen bedreigingen van buitenaf

9.1.5 Werken in beveiligde ruimten

9.1.6 Openbare toegang en gebieden voor laden en lossen

9.2 Beveiliging van apparatuur

9.2.1 Plaatsing en bescherming van apparatuur

9.2.2 Nutsvoorzieningen

9.2.3 Beveiliging van kabels

9.2.4 Onderhoud van apparatuur

9.2.5 Beveiliging van apparatuur buiten het terrein

9.2.6 Veilig verwijderen of hergebruik van apparatuur

9.2.7 Verwijdering van bedrijfseigendommen

10 Beheer van communicatie- en bedieningsprocessen

10.1 Bedieningsprocedures en verantwoordelijkheden

10.1.1 Gedocumenteerde bedieningsprocedures

10.1.2 Wijzigingsbeheer

10.1.3 Functiescheiding

10.1.4 Scheiding van faciliteiten voor ontwikkeling, testen en productie

10.2 Beheer van dienstverlening door een derde partij

10.2.1 Dienstverlening

10.2.2 Controle en beoordeling van dienstverlening door de derde partij

10.2.3 Beheer van wijzigingen in dienstverlening door een derde partij

10.3 Systeemplanning en acceptatie

10.3.1 Capaciteitsbeheer

10.3.2 Systeemacceptatie

10.4 Bescherming tegen virussen en ‘mobile code’

10.4.1 Maatregelen tegen virussen

10.4.2 Maatregelen tegen 'mobile code'

10.5 Back-up

10.5.1 Reservekopieën maken (back-ups)

10.6 Beheer van netwerkbeveiliging

10.6.1 Maatregelen voor netwerken

10.6.2 Beveiliging van netwerkdiensten

10.7 Behandeling van media

10.7.1 Beheer van verwijderbare media

10.7.2 Verwijdering van media

10.7.3 Procedures voor de behandeling van informatie

10.7.4 Beveiliging van systeemdocumentatie

10.8 Uitwisselen van informatie

10.8.1 Beleid en procedures voor informatie-uitwisseling

10.8.2 Uitwisselingsovereenkomsten

10.8.3 Fysieke media die worden getransporteerd

10.8.4 Elektronische berichtenuitwisseling

10.8.5 Systemen voor bedrijfsinformatie

10.9 Diensten voor e-commerce

10.9.1 E-commerce

10.9.2 Onlinetransacties

10.9.3 Openbare beschikbare informatie

10.10 Controle

10.10.1 Aanmaken audit-logbestanden

10.10.2 Controle op systeemgebruik

10.10.3 Bescherming van informatie in logbestanden

10.10.4 Logbestanden van administrators en operators

10.10.5 Registratie van storingen

10.10.6 Synchronisatie van systeemklokken

11 Toegangsbeveiliging

11.1 Bedrijfseisen ten aanzien van toegangsbeheersing

11.1.1 Toegangsbeleid

11.2 Beheer van toegangsrechten van gebruikers

11.2.1 Registratie van gebruikers

11.2.2 Beheer van speciale bevoegdheden

11.2.3 Beheer van gebruikerswachtwoorden

11.2.4 Beoordeling van toegangsrechten van gebruikers

11.3 Verantwoordelijkheden van gebruikers

11.3.1 Gebruik van wachtwoorden

11.3.2 Onbeheerde gebruikersapparatuur

11.3.3 ‘Clear desk’- en ‘clear screen’-beleid

11.4 Toegangsbeheersing voor netwerken

11.4.1 Beleid ten aanzien van het gebruik van netwerkdiensten

11.4.2 Authenticatie van gebruikers bij externe verbindingen

11.4.3 Identificatie van netwerkapparatuur

11.4.4 Bescherming op afstand van poorten voor diagnose en configuratie

11.4.5 Scheiding van netwerken

11.4.6 Beheersmaatregelen voor netwerkverbindingen

11.4.7 Beheersmaatregelen voor netwerkrouting

11.5 Toegangsbeveiliging voor besturingssystemen

11.5.1 Beveiligde inlogprocedures

11.5.2 Gebruikersidentificatie en –authenticatie

11.5.3 Systemen voor wachtwoordbeheer

11.5.4 Gebruik van systeemhulpmiddelen

11.5.5 Time-out van sessies

11.5.6 Beperking van verbindingstijd

11.6 Toegangsbeheersing voor toepassingen en informatie

11.6.1 Beperken van toegang tot informatie

11.6.2 Isoleren van gevoelige systemen

11.7 Draagbare computers en telewerken

11.7.1 Draagbare computers en communicatievoorzieningen

11.7.2 Telewerken

12 Verwerving, ontwikkeling en onderhoud van informatiesystemen

12.1 Beveiligingseisen voor informatiesystemen

12.1.1 Analyse en specificatie van beveiligingseisen

12.2 Correcte verwerking in toepassingen

12.2.1 Validatie van invoergegevens

12.2.2 Beheersing van interne gegevensverwerking

12.2.3 Integriteit van berichten

12.2.4 Validatie van uitvoergegevens

12.3 Cryptografische beheersmaatregelen

12.3.1 Beleid voor het gebruik van cryptografische beheersmaatregelen

12.3.2 Sleutelbeheer

12.4 Beveiliging van systeembestanden

12.4.1 Beheersing van operationele programmatuur

12.4.2 Bescherming van testdata

12.4.3 Toegangsbeheersing voor broncode en programmatuur

12.5 Beveiliging bij ontwikkelings- en ondersteuningprocessen

12.5.1 Procedures voor wijzigingsbeheer

12.5.2 Technische beoordeling van toepassingen na wijzigingen in het besturingssysteem

12.5.3 Restricties op wijzigingen in programmatuurpakketten

12.5.4 Uitlekken van informatie

12.5.5 Uitbestede ontwikkeling van programmatuur

12.6 Beheer van technische kwetsbaarheden

12.6.1 Beheersing van technische kwetsbaarheden

13 Beheer van informatiebeveiligingsincidenten

13.1 Rapportage van informatiebeveiligingsgebeurtenissen en zwakke plekken

13.1.1 Rapportage van informatiebeveiligingsgebeurtenissen

13.1.2 Rapportage van zwakke plekken in de beveiliging

13.2 Beheer van informatiebeveiligingsincidenten en –verbeteringen

13.2.1 Verantwoordelijkheden en procedures

13.2.2 Leren van informatiebeveiligingsincidenten

13.2.3 Verzamelen van bewijsmateriaal

14 Bedrijfscontinuïteitsbeheer

14.1 Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer

14.1.1 Informatiebeveiliging opnemen in het proces van bedrijfscontinuïteitsbeheer

14.1.2 Bedrijfscontinuïteit en risicobeoordeling

14.1.3 Continuïteitsplannen ontwikkelen en implementeren waaronder informatiebeveiliging

14.1.4 Kader voor de bedrijfscontinuïteitsplanning

14.1.5 Testen, onderhoud en herbeoordelen van bedrijfscontinuïteitsplannen

15 Naleving

15.1 Naleving van wettelijke voorschriften

15.1.1 Identificatie van toepasselijke wetgeving

15.1.2 Intellectuele eigendomsrechten (Intellectual Property Rights, IPR)

15.1.3 Bescherming van bedrijfsdocumenten

15.1.4 Bescherming van gegevens en geheimhouding van persoonsgegevens

15.1.5 Voorkomen van misbruik van IT-voorzieningen

15.1.6 Voorschriften voor het gebruik van cryptografische beheersmaatregelen

15.2 Naleving van beveiligingsbeleid en –normen en technische naleving

15.2.1 Naleving van beveiligingsbeleid en –normen

15.2.2 Controle op technische naleving

15.3 Overwegingen bij audits van informatiesystemen

15.3.1 Beheersmaatregelen voor audits van informatiesystemen

15.3.2 Bescherming van hulpmiddelen voor audits van informatiesystemen