Dreigingen			Oplossingen/aandachtspunten	
Verantwoordelijkheid			Ekklesia/Efkasoft	kerkenraad
	1 Beveiligingsinbreuken als gevolg van ontbreken van coordinatie vanuit de directie.	De directie heeft geen maatregelen getroffen op het gebied van informatiebeveiliging. Een informatiebeveiligingsbeleid en/of ISMS ontbreekt.	Ekklesia is voorzien van diverse beveiligingsmogelijkheden. De handleiding bevat aanvullende aanbevelingen.	Taak kerkenraad: beleid opstellen
	2 Beveiligingsinbreuken als gevolg van het ontbreken of niet oppakken van verantwoordelijkheden door leidinggevenden.	Leidinggevenden hebben niet de juiste verantwoordelijkheden en middelen toegewezen gekregen om het beleid goed door te voeren binnen de organisatie of pakken deze verantwoordelijkheden onvoldoende op. Het eigenaarschap van informatiesystemen is niet goed belegd. Beveiliging vormt geen vast onderdeel van projecten.	Beveiliging van de gegevens is onderdeel van Ekklesia	Taak kerkenraad: ledenadministrateur verantwoordelijkheid geven om toegangrechten af te schermen door gebruikmaking van wachtwoorden en toegangsrestricties op de ledenadministratie.
	3 Medewerkers hebben onvoldoende aandacht voor het informatiebeveiligingsbeleid.	Het ontbreekt de medewerkers aan awareness op het gebied van informatiebeveiliging.	Efkasoft is zich bewust van de noodzaak van informatiebeveiliging en past deze toe in haar producten.	Taak kerkenraad: bewustwording stimuleren bij gebruikers van Ekklesia, bijv. door geheimhoudingsverklaring te laten tekenen.
Wet- en regelgeving				
	4 Tegen het bedrijf worden juridische stappen genomen vanwege het niet veilig omgaan met vertrouwelijke informatie.	De organisatie en/of haar medewerkers handelen bewust of onbewust in strijd met de wet.	Efkasoft biedt binnen Ekklesia mogelijkheden om de gebruikers van het pakket in overeenstemming met de wet te kunnen laten handelen. Zo nodig wordt dit gestimuleerd door middel van voorlichting.	Taak kerkenraad: uitvoeringsregels opstellen, bijv. omtrent gebruik gegevens en bewaartermijnen.
	5 Tijdens een rechtszaak is het bedrijf niet in staat om de benodigde bewijzen te kunnen leveren.	Het bedrijf heeft een probleem met de beschikbaarheid, vertrouwelijkheid en/of integriteit van bewijsmateriaal, zoals logbestanden.	Efkasoft kan aantonen dat Ekklesia databestanden niet toegankelijk zijn buiten het programma om en dat toegang tot dit programma door middel van wachtwoorden kan worden beschermd.	Taak ledenadministratie: default wachtwoorden aanpassen.

6	Het niet hard kunnen maken van welke persoon over welk account beschikt.	Gedeelde accounts, het gebruiken van een account van een ex-medewerker of het niet beschikbaar hebben van de juiste loginformatie.	Ekklesia biedt de mogelijkheid om per gebruiker een login/wachtwoord account aan te maken en hieraan toegangsbeperkingen te koppelen. Het beheer ervan is uitsluitend verstrekt aan de ledenadministrateur, die dit bij iedere update van de databestanden kan intrekken. Alleen de Ekklesia in bezit van de ledenadministratie (dus niet de Ekklidon kijkversie gebruikers) heeft volledige toegang tot alle gegevens inclusief accounts. Voor het installeren van Ekklesia op een pc geldt een registratieprocedure bij Efkasoft, waardoor het ongeautoriseerd installeren van Ekklesia wordt tegengegaan en Efkasoft altijd beschikt over minimaal het e-mailadres van degene(n) die beschikt(en) over het programma.	Taak ledenadministratie: iedere gebruiker eigen account geven. Indien nodig intrekken van accounts. Taak kerkenraad: geheimhoudingsverklaring van ledenadministateur eisen.
7	Inbreuk op vertrouwelijkheid door wetgeving ten aanzien van informatie in de cloud.	Door wetgeving in sommige landen kan de overheid van zo'n land inzage krijgen in informatie welke in de cloud ligt opgeslagen.	Ekklesia draait (nog) niet in de cloud, dus niet van toepassing.	Taak kerkenraad: wanneer export van gegevens vanuit Ekklesia naar de cloud worden opgeslagen, moet deze beveiligd worden tegen inbraak.
8	Inbreuk op vertrouwelijkheid door wetgeving ten aanzien van het bezoeken van dat land.	Door wetgeving in sommige landen kan de overheid inzage eisen in de gegevens op meegenomen systemen bij een bezoek aan dat land.	n.v.t.	Verantwoordelijkheid ledenadministrateur: Evt. laptops waarop Ekklesia is geïnstalleerd, bij voorkeur niet meenemen op reis.
9	Inbreuk op vertrouwelijkheid door wetgeving ten aanzien van gebruik van cryptografie.	Door wetgeving in sommige landen kan de overheid een kopie van cryptografische sleutels opeisen.	Ekklesia databestanden zijn versleuteld. Het versleutelingsalgoritme is door een externe databaseleverancier gemaakt. De broncode hiervan is beschikbaar, dus in geval van opeisbaarheid te verstrekken.	n.v.t.

	10 Tegen het bedrijf worden juridisch stappen genomen vanwege schenden van auteursrechten / IPR.	De organisatie en/of haar medewerkers handelen bewust of onbewust in strijd met de wet.	n.v.t.	n.v.t.
Incidenten en incidentafhandeling				
	11 Systemen raken besmet met malware.	Het ontbreekt aan een goed antivirus- en/of patchbeleid of het goed uitvoeren daarvan.	Ekklesia is voorzien van een controle bij opstarten van het programma op aantasting van de originele executable. Wanneer de executable blijkt te zijn aangetast, beëindigt het programma onmiddellijk na opstarten met een foutmelding	Taak ledenadministratie: installeren virusscanner, als extra maatregel naast de in Ekklesia ingebouwde beveiliging wordt aanbevolen.
	12 Overbelasten van netwerkdiensten.	Het overbelasten van een netwerkdienst waardoor deze niet meer beschikbaar is voor gebruikers.	n.v.t.	n.v.t.
	13 De gevolgen van incidenten worden onnodig groot, doordat deze niet tijdig gezien / opgepakt worden.	Binnen het bedrijf is er onvoldoende netwerkmonitoring en is er geen centraal meldpunt voor beveiligingsincidenten.	Aangezien Ekklesia op een lokale pc draait, zijn de gegevens slechts beperkt toegankelijk.	Taak kerkenraad: beleid opstellen t.a.v. vanuit Ekklesia verstrekte rapportages met gegevens.
	14 Incidenten kunnen niet (snel genoeg) opgelost worden omdat de nodige informatie en actieplannen ontbreken.	Systeembeheerders hebben onvoldoende technische informatie over het probleem om het te kunnen oplossen. Een actieplan ontbreekt waardoor het incident onnodig lang blijft duren.	Bewaking van de databestanden is primair verantwoordelijkheid van de gebruiker, derhalve n.v.t. Efkasoft biedt gratis ondersteuning bij mogelijke incidenten, voor zover van toepassing.	Taak kerkenraad: eisen opstellen wanneer gegevens online worden gezet.
	15 Herhaling van incidenten.	Incidentrapportages ontbreken of worden niet bijgehouden. Veel voorkomende incidenten worden daardoor niet pro-actief aangepakt.	n.v.t.	Taak kerkenraad: beleid opstellen t.a.v. incidentrapportages indien van toepassing.
Misbruik				
	16 Systemen worden niet gebruikt waarvoor ze bedoeld zijn.	Het ontbreken van een beleid op bijvoorbeeld het internetgebruik, vergroot de kans op misbruik.	n.v.t.	n.v.t.

	17 Wegnemen van bedrijfsmiddelen.	Door onvoldoende controle op de uitgifte en onjuiste inventarisatie van bedrijfsmiddelen bestaat de kans dat diefstal niet of te laat wordt opgemerkt.	n.v.t.	Taak kerkenraad/ledenadministratie: bijhouden wie beschikt over de databestanden/programmatuur
	18 Beleid wordt niet gevolgd door ontbreken van sancties.	Door het ontbreken van sancties op het overtreden van regels bestaat de kans dat medewerkers de beleidsmaatregelen niet serieus nemen.	n.v.t.	Taak kerkenraad: beleid opstellen
	19 Inbreuk op vertrouwelijkheid van informatie door het toelaten van externen in het pand of op het netwerk.	Het toelaten van externen, zoals leveranciers en projectpartners, kunnen gevolgen hebben voor de vertrouwelijkheid van de informatie die binnen het pand of via het netwerk beschikbaar is.	Efkasoft beschikt uitsluitend op initiatief van een gebruiker over de databestanden, uitsluitend ten behoeve van het oplossen van gebruikersproblemen. Efkasoft gaat daarmee uiterst zorgvuldig om. Alleen de directeur/eigenaar van Efkasoft heeft in een dergelijk geval toegang.	Taak kerkenraad: beleid opstellen
Ongeautoriseerde toegang				
	20 Misbruik van andermans identiteit.	Door onvoldoende (mogelijkheid op) controle op een identiteit, kan ongeautoriseerde toegang verkregen worden tot vertrouwelijke informatie. Denk hierbij ook aan social engineering.	Zie 6	Taak ledenadministratie: default wachtwoorden aanpassen. Iedere gebruiker een eigen account geven.
	21 Onterecht hebben van rechten.	Door een ontbrekend, onjuist of onduidelijk proces voor het uitdelen en innemen van rechten, kan een aanvaller onbedoeld meer rechten hebben.	Zie 6	Taak ledenadministratie: default wachtwoorden aanpassen. Iedere gebruiker een eigen account geven. Zo nodig extra toegangsbeperkingen definiëren.
	22 Misbruik van bevoegdheden.	Door onvoldoende controle op medewerkers met bijzondere rechten, zoals systeembeheerders, bestaat de kans op ongeautoriseerde toegang tot gevoelige informatie.	Zie 19	De beslissing is aan ledenadministratie om databestanden af te staan in geval van problemen.

23	Toegang tot informatie door slecht wachtwoordgebruik.	Het ontbreken van een wachtwoordbeleid en bewustzijn bij medewerkers kan leiden tot het gebruik van zwakke wachtwoorden, het opschrijven van wachtwoorden of het gebruik van hetzelfde wachtwoord voor meerdere systemen.	Ekklesia ondersteunt sterke wachtwoorden. De ledenadministrateur definieert deze voor alle gebruikers.	Taak kerkenraad: beleid opstellen. Taak ledenadministrateur: sterke wachtwoorden uigeven
24	Toegang tot informatie door onbeheerd achterlaten van werkplekken.	Door het ontbreken van een clear-desk en/of clear-screen policy kan toegang verkregen worden tot gevoelige informatie.	n.v.t.	Meestal n.v.t. Zonodig beleid opstellen.
25	Toegang tot informatie door onduidelijkheid over bevoegdheid en vertrouwelijkheid van informatie.	Door onduidelijkheid in de classificatie van informatie bestaat de kans op ongeautoriseerde toegang tot gevoelige informatie.	Zie 6	Taak kerkenraad/ledenadministratie: beleid opstellen t.a.v. vertrouwelijke velden in Ekklesia.
26	Toegang tot informatie op systemen of systeemonderdelen bij reparatie of verwijdering.	Gevoelige informatie kan lekken indien opslagmedia of systemen welke opslagmedia bevatten worden weggegooid of ter reparatie aan derden worden aangeboden.	Zie 5. Uitgevoerde rapportages naar leesbare bestanden vallen buiten de verantwoordelijkheid van Efkasoft	Taak ledenadministratie: ervoor zorgen dat rapportages vanuit Ekklesia regelmatig / tijdig worden verwijderd.
27	Toegang tot informatie door misbruik van kwetsbaarheden in applicaties.	Kwetsbaarheden in applicaties worden misbruikt (exploits) om ongeautoriseerde toegang te krijgen tot een applicatie en de daarin opgeslagen informatie.	De risico's zijn hierin zeer gering vanwege dataopslag op lokale pc.	n.v.t.
28	Toegang tot informatie door misbruiken van zwakheden in netwerkbeveiliging.	Zwakheden in de beveiliging van het (draadloze) netwerk worden misbruikt om toegang te krijgen tot dit netwerk.	Zie 5.	Toegang is beperkt tot leesbare rapportages vanuit Ekklesia. Hiervoor dient de ledenadministrateur beveiligingsmaatregelen te treffen.
29	Toegang tot informatie door onvoldoende aandacht voor beveiliging bij uitbesteding van werkzaamheden.	Doordat externe partijen / leveranciers hun informatiebeveiliging niet op orde hebben, kunnen inbreuken ontstaan op de informatie waar zij toegang tot hebben.	Zie 19. Efkasoft draagt zorg voor max. beveiliging van aan hem verstrekte informatie.	n.v.t.

	30 Toegang tot informatie doordat deze zich buiten de beschermde omgeving bevinden.	Informatie die voor toegestaan gebruik meegenomen wordt naar bijvoorbeeld buiten het kantoor wordt niet meer op de juiste wijze beschermd.	Wanneer Ekklesia databestanden door middel van back-up bestanden worden verspreid, dan zijn dit buiten Ekklesia om onleesbare bestanden. Per kerkelijke gemeente (klant) zijn de gegevens met een eigen unieke sleutel versleuteld. Het is dus niet mogelijk om met Ekklesia de databestanden van een andere kerkelijke administratie te openen dan de eigen administratie.	Zie 28
	31 Toegang tot informatie door middel van afluisterapparatuur.	Door middel van keyloggers of netwerktaps wordt gevoelige informatie achterhaald.	n.v.t.	Ledenadministrateur dient zo nodig maatregelen te treffen op zijn pc
	32 Misbruik van cryptografische sleutels en/of gebruik van zwakke algoritmen.	Door een onjuist of ontbrekend sleutelbeheer bestaat de kans op misbruik van cryptografische sleutels. Het gebruik van zwakke cryptografische algoritmen biedt schijnveiligheid.	De door de databaseleverancier toegepaste encryptie is geen zeer sterke cryptografie volgens huidige normen, maar in de context van de lokale toegankelijkheid van de data meer dan voldoende.	n.v.t.
Uitwisselen en bewaren van informatie				
	33 Onveilig versturen van gevoelige informatie.	Inbreuk op vertrouwelijkheid van informatie door onversleuteld versturen van informatie.	Zie 30	Ten aanzien van verstuurde rapport uitdraaien (leesbare vorm, bijv. pdf) dient beleid opgesteld te worden.
	34 Versturen van gevoelige informatie naar onjuiste persoon.	Inbreuk op vertrouwelijkheid van informatie door het onvoldoende controleren van ontvanger.	Zie 30	Zie 34
	35 Imagoschade door onjuiste berichtgeving.	Het vrijgegeven van ongecontroleerde informatie of onjuiste informatie kan leiden tot imagoschade.	Zie 5. Wanneer gevoelige informatie (persoonlijke notities) worden opgeslagen, dan biedt Ekklesia de mogelijkheid om deze met een afzonderlijk wachtwoord te beveiligen, die de gebruiker zelf kan kiezen (ook wanneer de overige toegang door de ledenadministrateur is toegekend)	De vrijgegeven informatie betreft doorgaans NAW + geb.datum. Wanneer meer wordt opgeslagen dan dienen hiervoor beleidsregels t.a.v. vrijgave te worden opgesteld.

	36 Informatieverlies door verlopen van houdbaarheid van opslagwijze.	Informatie gaat verloren door onleesbaar geraken van medium of gedateerd raken van bestandsformaat.	Ekklesia is voorzien van een back-up module, waarmee reservekopieën van de databestanden gemaakt kunnen worden. Ekklesia waarschuwt iedere keer bij afsluiten wanneer ten opzichte van de laatst gemaakte back-up wijzigingen zijn uitgevoerd, die een mogelijke nieuwe back-up noodzakelijk maken. De gegevens worden opgeslagen in het dBase III / FoxPro formaat. Dit is een gangbaar databaseformaat dat nog lange tijd ondersteund zal worden. Door de versleuteling van de gegevens zijn ze echter niet leesbaar zonder deze versleuteling te kennen. Hierdoor zijn de bestanden uitsluitend leesbaar via Ekklesia. Wanneer ook de Ekklidon leesversie binnen de gemeente wordt gebruikt, is er altijd een alternatieve locatie beschikbaar waarop in noodgevallen de data toegankelijk gemaakt kan worden.	Het is de taak van de ledenadministrateur om regelmatig back-ups te maken. Wanneer ook de Ekklidon leesversie binnen de gemeente wordt gebruikt, is er altijd een alternatieve locatie beschikbaar waarop in noodgevallen de data toegankelijk gemaakt kan worden.
	37 Foutieve of vervalste informatie.	Ongewenste handelingen als gevolg van foutieve / vervalste bedrijfsinformatie of toegestuurd krijgen van foutieve / vervalste informatie.	n.v.t.	De informatie kan door de betreffende personen worden opgevraagd en zo nodig gecorrigeerd. De gegevens worden uitsluitend voor interne kerkelijke doeleinden gebruikt, dus fouten komen op andere plaatsen niet naar buiten.
Mobiele apparatuur en telewerken				
	38 Verlies van mobiele apparatuur en opslagmedia.	Door het verlies van mobiele apparatuur en opslagmedia bestaat de kans op inbreuk op de vertrouwelijkheid van gevoelige informatie.	Zie 5.	Zie 28

	39 Aanvallen via onbeveiligde systemen.	Door onvoldoende grip op de beveiliging van prive- en thuisapparatuur bestaat de kans op bijvoorbeeld besmetting met malware.	Zie 11	Zie 28
Systeem- en gebruikersfouten				
	40 Uitval van systemen door softwarefouten.	Fouten in software kunnen leiden tot systeemcrashes of het corrupt raken van de in het systeem opgeslagen informatie.	Zie 36	n.v.t.
	41 Uitval van systemen door configuratiefouten.	Onjuiste configuratie van een applicatie kunnen leiden tot een verkeerde verwerking van informatie.	n.v.t.	n.v.t.
	42 Uitval van systemen door hardwarefouten.	Hardware van onvoldoende kwaliteit kunnen leiden tot uitval van systemen.	Zie 36	n.v.t.
	43 Gebruikersfouten.	Onvoldoende kennis of te weinig controle op andermans werk vergroot de kans op menselijke fouten. Gebruikersinterfaces die niet zijn afgestemd op het gebruikersniveau verhogen de kans op fouten.	Ekklesia heeft een zeer directe en gebruiksvriendelijke gebruikersinterface, waardoor de kans op fouten minimaal is.	n.v.t.
	44 Fouten als gevolg van wijzigingen in andere systemen.	In een systeem ontstaan fouten als gevolg van wijzigingen in gekoppelde systemen.	n.v.t.	n.v.t.
	45 Onvoldoende aandacht voor beveiliging bij softwareontwikkeling.	Onvoldoende aandacht voor beveiliging bij het zelf of laten ontwikkelen van software leidt tot inbreuk op de informatiebeveiliging.	Bij de ontwikkeling van Ekklesia is vanaf het begin aandacht gegeven aan beveiliging.	n.v.t.
Fysieke beveiliging				
	46 Ongeautoriseerde fysieke toegang.	Het ontbreken van toegangspasjes, zicht op ingangen en bewustzijn bij medewerkers vergroot de kans op ongeautoriseerde fysieke toegang.	n.v.t.	Indien het programma draait op een pc in een publiek toegankelijke ruimte (kerkelijk bureau), dan dient hiervoor de toegang geregeld te zijn.

	47 Brand.	Het ontbreken van brandmelders en brandblusapparatuur vergroten de gevolgen van een brand.	n.v.t.	Zie 36
	48 Overstroming en wateroverlast.	Overstroming en wateroverlast kunnen zorgen voor schade aan computers en andere bedrijfsmiddelen.	n.v.t.	Zie 36
	49 Verontreiniging van de omgeving.	Verontreininging van de omgeving kan ertoe leiden dat de organisatie (tijdelijk) niet meer kan werken.	n.v.t.	Zie 36
	50 Explosie.	Explosies kunnen leiden tot schade aan het gebouw en apparatuur en slachtoffers.	n.v.t.	Zie 36
	51 Uitval van facilitaire middelen (gas, water, electra, airco).	Uitval van facilitaire middelen kan tot gevolg hebben dat een of meerdere bedrijfsonderdelen hun werk niet meer kunnen doen.	n.v.t.	Zie 36
	52 Vandalisme of overlast door dieren.	Schade aan of vernieling van bedrijfseigendommen als gevolg van een ongerichte actie.	n.v.t.	Zie 36
Bedrijfscontinuïteit				
	53 Rampen.	Een ramp kan het voortbestaan van de organisatie in gevaar brengen.	n.v.t.	Zie 36
	54 Niet beschikbaar zijn van informatie of diensten vanuit derden.	Het niet beschikbaar zijn van cruciale informatie of diensten van derden door uitval van systemen, corrupt raken van de informatie of ongeplande contractbeëindiging kunnen de organisatie schade toebrengen.	Ekklesia kan uitsluitend via een registratieprocedure bij Efkasoft worden geactiveerd. Wanneer Efkasoft niet (meer) beschikbaar is, zou dit een probleem kunnen vormen. Vanwege dit potentiële risico is het altijd mogelijk om ook zonder registratieprocedure (of uiteraard via Ekklidon kijkversie) de gegevens naar buiten toe te ontsluiten via rapportages.	Taak kerkenraad: procedure opstellen om bij calamiteiten altijd op een alternatieve wijze toegang tot de gegevens te kunnen krijgen. Ook de ledenadministrateur kan niet-beschikbaar raken.

55	Software wordt niet meer ondersteund door de uitgever.	Voor software die niet meer ondersteund wordt worden geen securitypatches meer uitgegeven. Denk ook aan Excel- en Access-applicaties.	Indien Efkasoft besluit om ondersteuning van Ekklesia te stoppen, dan zal in ieder geval aan de gebruikers een aangepaste versie van Ekklesia worden verstrekt, waarvoor geen registratieprocedure meer noodzakelijk is.	In het geval dat Ekklesia niet meer wordt ondersteund, zal de kerkenraad zo spoedig mogelijk maatregelen moeten treffen om de gegevens over te zetten naar een dan actueel systeem.
56	Kwijtraken van belangrijke kennis bij vertrek of niet beschikbaar zijn van medewerkers.	Medewerkers die het bedrijf verlaten of door een ongeval (tijdelijk) niet beschikbaar zijn beschikken over kennis die na het verlaten niet meer beschikbaar is.	Zie 55. Bij onverwacht wegvallen van Efkasoft (overlijden directeur/eigenaar) zal de familie proberen dit te regelen. Een procedurebeschrijving hiervoor ontbreekt nog. Overigens wordt sinds versie 6 het programma bij ontbrekende registratie nooit meer helemaal ontoegankelijk (vrijgave na max. 30 seconden)	Taak kerkenraad om hiervoor een regeling te treffen. Zie ook 36