| Term | Definitie | Bron |
|---|---|---|
| **Beveiligingsincident of operationeel veiligheidsincident** | Een losse gebeurtenis of een reeks met elkaar verbonden gebeurtenissen die niet is gepland en die een nadelig effect heeft of waarschijnlijk zal hebben op de integriteit, beschikbaarheid, vertrouwelijkheid van IT systemen en diensten. | EIOPA-BoS-20/600 - Guidelines on information and communication technology security and governance<br>EBA/GL/2019/04 - EBA Guidelines on ICT and security risk management |
| **Business Continuity Plan (BCP)** | Gedocumenteerde informatie die een instelling begeleidt om te reageren op een verstoring en de levering van producten en diensten te voort te zetten, te herstellen en te hervatten in overeenstemming met haar doelstellingen voor bedrijfscontinuïteit. | ISO 22301 |
| **Clouddiensten** | Diensten geleverd met behulp van cloudcomputing, dat wil zeggen een model om via het netwerk overal eenvoudig op verzoek toegang te verlenen tot een gedeelde pool van configureerbare IT-middelen (bijvoorbeeld netwerken, servers, opslagmedia, applicaties en diensten) die met een minimale beheerinspanning of tussenkomst van dienstverleners snel kunnen worden op- en afgeschaald. | EIOPA-BoS-20-002- Guidelines on outsourcing to cloud service providers |
| **Cloud service provider** | Een dienstverlener die verantwoordelijk is voor het uitvoeren van clouddiensten op grond van een uitbestedingsovereenkomst. | EIOPA-BoS-20-002- Guidelines on outsourcing to cloud service providers |
| **Cyber attack** | Een aanval, via cyberspace, die zich richt op het gebruik van cyberspace door een instelling met het doel een computeromgeving / -infrastructuur te verstoren, buiten werking te stellen, te vernietigen of kwaadwillig te controleren; of het vernietigen van de integriteit van de gegevens of het stelen van informatie. | NIST, ISACA |
| **Datalek** | Toegang tot of vernietiging, wijziging of vrijkomen van vertrouwelijke gegevens bij een instelling, zonder dat dit de bedoeling is van deze instelling. | |
| **End User Computing** | De mogelijkheid voor eindgebruikers om zelf hun eigen informatiesystemen te ontwerpen, te implementeren en daarmee data van de instelling in te zien of te bewerken. | ISACA |
| **End-of-life** | Een term die wordt gebruikt voor een (IT) product dat aan klanten wordt geleverd, waarmee wordt aangegeven dat het product aan het einde van zijn levensduur is en dat de leverancier is gestopt met het onderhoud van het product waaronder het leveren van security patches. | |
| **IT asset** | Een component van software of hardware dat deel uitmaakt van de IT voorziening van de instelling. | EIOPA-BoS-20/600 - Guidelines on information and communication technology security and governance |
| **IT availability and continuity risk** | Het risico dat de prestaties en beschikbaarheid van IT systemen en gegevens nadelig worden beïnvloed, inclusief het onvermogen om de diensten van de instelling tijdig te herstellen als gevolg van een storing in de IT hardware of softwarecomponenten; zwakke punten | EBA/GL/2017/07 - EBA Guidelines on ICT and security risk management |

| Term | Definitie | Bron |
|---|---|---|
| | in IT systeembeheer; of een andere gebeurtenis. | |
| **IT change risk** | Het risico dat voortvloeit uit het onvermogen van de instelling om veranderingen in IT systemen tijdig en beheerst te effectueren, met name bij grote en complexe veranderprogramma's. | EBA/GL/2017/07 - EBA Guidelines on ICT and security risk management |
| **IT data integrity risk** | Het risico dat gegevens die worden opgeslagen en verwerkt door IT systemen onjuist, onvolledig of inconsistent zijn tussen verschillende ICT-systemen, (bijvoorbeeld als gevolg van zwakke of afwezige IT-controles) met negatieve invloed op het vermogen van de instelling diensten en (risico) management informatie correct en tijdig te leveren. | EBA/GL/2017/07 - EBA Guidelines on ICT and security risk management |
| **IT- en beveiligingsrisico** | Als een onderdeel van operationeel risico; het risico van verliezen als gevolg van inbreuken op de geheimhouding, falende integriteit van systemen en data, ongeschiktheid of onbeschikbaarheid van systemen en data, of het onvermogen om IT aan te passen binnen een redelijke termijn en met redelijke kosten wanneer de omgeving of de bedrijfsvereisten veranderen (d.w.z. flexibiliteit). Dit omvat beveiligingsrisico's die voortvloeien uit ontoereikende of falende interne processen of externe gebeurtenissen met inbegrip van cyberaanvallen of ontoereikende fysieke beveiliging. | EIOPA-BoS-20/600 - Guidelines on information and communication technology security and governance<br>EBA/GL/2019/04 - EBA Guidelines on ICT and security risk management |
| **IT outsourcing risk** | Het risico dat het inschakelen van een derde partij, of een andere groepsentiteit (intra-group outsourcing), om IT systemen of gerelateerde diensten aan te bieden, een negatieve invloed heeft op de prestaties en het risicobeheer van de instelling. | EBA/GL/2017/07 - EBA Guidelines on ICT and security risk management |
| **IT security risk** | Het risico van ongeautoriseerde toegang tot IT systemen en gegevens van binnen of buiten de instelling (bijvoorbeeld cyberaanvallen). | EBA/GL/2017/07 - EBA Guidelines on ICT and security risk management |
| **IT services** | Services provided through ICT systems and service providers to one or more internal or external users. | EIOPA-BoS-20/600 - Guidelines on information and communication technology security and governance |
| **IT systeem** | Set van applicaties, services, IT-assets of andere informatiebehandelingscomponenten, waaronder de besturingsomgeving. | EIOPA-BoS-20/600 - Guidelines on information and communication technology security and governance |
| **Kritiek of belangrijk systeem / proces** | De instelling stelt vast en documenteert of een functie, activiteit of IT systeem kritiek of belangrijk is aan de hand van de vraag of de betreffende functie, activiteit of systeem van essentieel belang is voor de bedrijfsvoering van de instelling in de zin dat de instelling zonder deze functie, activiteit of IT systeem niet in staat zou zijn om haar diensten aan de | EIOPA-BoS-14/253 - Guidelines on system of governance (GL60) |

| Term | Definitie | Bron |
|---|---|---|
| | verzekeringnemers of deelnemers in het pensioenfonds te verlenen. | |
| **Kritieke security patch** | Een software update waarvan de instelling op grond van een risicoanalyse heeft vastgesteld dat deze kritiek of belangrijk is om de bedrijfsvoering van de instelling te beschermen tegen kwetsbaarheden. | |
| **Recovery Time Objective (RTO)** | RTO staat voor *hersteltijddoelstelling* en is het streven om te voldoen aan de afgesproken hersteltijd na een disruptie (bijv. een computercrash) door de afdeling IT en/of een IT dienstverlener. | British Standards Institution (BSI) |
| **Risicobeheersing** | De maatregelen die een instelling neemt om risico's te beheersen. De beoordeling van risicobeheersing is in eerste instantie erop gericht om na te gaan of de opzet, het bestaan en de werking van risicobeheersing van een instelling voldoet aan de gestelde toezichtnormen, en daarnaast of de huidige beheersingsomgeving in lijn is met de grootte en complexiteit van het risiconiveau. | DNB Brochure ATM, zie https://www.dnb.nl/voor-de-sector/open-boek-toezicht/brochure-atm/ |