

Cumulatief	↑	Beschikbaarheid	Integriteit	Veiligheid
		<p>Hoog</p> <ul style="list-style-type: none"> - Er is een volledige redundante architectuur geïmplementeerd 	<ul style="list-style-type: none"> - Alle gebruik, starten en stoppen van audit logs wordt gelogged - Create en verwijdering van system-level objects wordt gelogged - Alle mutaties van audit trails, configuratiebestanden en parameter files wordt gelogged - Audit trails worden minimaal 3 maanden online en 1 jaar offline, opvraagbaar 48 uur bewaard - Logs worden beschermd door file-integrity monitoring of wijzigingsdetectiesystemen - Integriteitscontroles zijn aanwezig om de integriteit van systeem en configuratiebestanden te monitoren. 	<ul style="list-style-type: none"> - 2-factor authenticatie moet worden toegepast - Deblokkeren van geblokkeerde account dient handmatig plaats te vinden.. - Alle data worden versleuteld opgeslagen - Alle gebruik van authenticatiemiddelen wordt gelogged - Gedetecteerde extreme aantallen verkeerde inlogpogingen worden direct aan Security Management gemeld. - Host based IDS dient geactiveerd te zijn - Interne IT beheerder maken gebruik van een Stepping Stone om toegang te krijgen tot de omgeving.
		<p>Midden</p> <ul style="list-style-type: none"> - De datacenter facility (UPS, Cooling, energieleveringspaden) componenten in het datacenter zijn alle redundant uitgevoerd (Tier 3 datacenter) en daardoor gelijktijdig onderhoudbaar - Dagelijks worden full back-ups gemaakt - De bewaartijd van back-ups voor kritische systemen zonder bewaarplicht is 1 jaar - De bewaartijd van back-ups voor kritische systemen met bewaarplicht is 7 jaar - Servers bevatten slecht 1 primaire functie - Er is een uitwijdraisboek voor het herstellen van systemen in geval van een calamiteit - Het uitwijdraisboek wordt elk 1 jaar getest - Elk jaar wordt een uitwijktest uitgevoerd - Er is een redundante architectuur geïmplementeerd met behulp van een hot standby 	<ul style="list-style-type: none"> - Alle acties die worden uitgevoerd door personen die Root of Admin (high privileged accounts) autorisaties worden gelogged - Alle toegang tot audit trails wordt gelogged 	<ul style="list-style-type: none"> - Autorisaties in applicaties worden toegekend op basis van 'need-to-know' en 'need-to-have' - Applicaties (incl. klantapplicaties) maken gebruik van verificatie van username en password (SSO) of 1-factor authenticatie - Alle data buiten VIPF wordt versleuteld opgeslagen en verstuurd. - Voor versturen geldt dat gebruik gemaakt wordt van TLS 1.2, vergelijkbaar of beter aangeboden door de leverancier en door VIPF gevalideerd. - Voor opslag van gegevens in databases geldt dat gebruik gemaakt wordt van Transparent Data Encryption met AES 256, vergelijkbaar of beter aangetoond door de leverancier en door VIPF gevalideerd. - Network Intrusion Detection dient aanwezig te zijn - Netwerkkomponenten die aan het externe netwerk zijn gekoppeld bevatten 2-factor authenticatie - Time-out van 15 minuten op de actieve connecties - Alle software (maatwerk, pakket, SaaS) dienen te voldoen aan best practice beveiligingsprofiel (bij OWASP) - VIPF IT omgevingen dienen logisch te zijn gescheiden en van andere organisaties - Elk jaar en na elke significante wijziging wordt een interne en externe penetratietest uitgevoerd. Indien nodig ook bij een groot incident. - Risk based logging is geconfigureerd om toegang te loggen en monitoren. - Er wordt gebruik gemaakt van netwerk filtering en analyse maatregelen binnen de IT domeinen
		<p>Laag</p> <ul style="list-style-type: none"> - Er is een redundante architectuur geïmplementeerd met behulp van een cold standby - 1 keer per jaar wordt de backup en recovery procedure lowel de volledigheid en recovery van de backup zelf getest - Kopieën van Back-ups worden op een tweede/secundaire locatie bewaard in overeenstemming met de bewaartijd van het origineel - De fysieke omgeving van de IT apparatuur bevat maatregelen ter preventie, detectie en repressie van incidenten en calamiteiten zoals brand en wateroverlast - De secundaire locatie is op voldoende (smart maken) afstand van de primaire locatie en is vastgesteld op basis van een risicoanalyse. 	<ul style="list-style-type: none"> - Bewaar audit trails minstens 1 jaar online direct toegankelijk - Richt antivirus/malware maatregelen in op servers van informatiesystemen - In VIPF interne domein zijn de volgende maatregelen reeds ingericht: <ul style="list-style-type: none"> - Antivirus/malware maatregelen zijn aanwezig op werkstations en externe gateways om malware te detecteren en te verwijderen 	<ul style="list-style-type: none"> - Toegang tot de applicaties en fleshares (non-sensitive data) wordt verleend op basis van de rol van een gebruiker (rol management) - Alle netwerkkomponenten, systemen, databases en middleware zijn gehardened - Default wachtwoorden van systemen, databases, middleware en applicaties zijn gewijzigd - Elke user heeft een persoonlijk account - Alle niet persoonlijke accounts zijn gekoppeld aan/ herleidbaar naar natuurlijke personen - Accounts met hoge privileges worden alleen gebruikt voor administratieve doeleinden - Inactieve accounts worden automatisch gedeactiveerd na 3 maanden inactiviteit en uiterlijk 1,5 jaar na deactivering permanent verwijderd - Uitgeven 'normal'account en autorisaties worden elk half jaar gereviseerd - Elk kwartaal worden high privileged accounts en autorisaties gereviseerd - 1-factor authenticatie met een complex wachtwoord wordt toegepast [vereisten complex] - Na 3 foutieve inlogpogingen wordt een wachtwoord geblokkeerd - Screensaver wordt binnen 15 minuten geactiveerd - Wachtwoorden en authenticatie data worden versleuteld tijdens transmissie en opslag middels sterke encryptietechnieken (one-way encryptie en sterke sleutels) - Logging van in- en uitloggen op het interne netwerk - Remote access gebruikt 2-factor authenticatie en versleutelde communicatie - Vulnerability scans (intern en extern) worden voor in beheername en vervolgens elke 6 maanden uitgevoerd - Alle data & media worden verwijderd of vernietigd conform - Alle data & media worden verwijderd of vernietigd conform de bir normen - Productie, test en ontwikkelnetwerken zijn gescheiden - Alle backups worden versleuteld opgeslagen - Visueel is onderscheid in productie, acceptatie en ontwikkeling front end omgevingen