

Release Management

Doelstelling

RLM draagt zorg voor de kwaliteit van de productieomgeving bij het implementeren van nieuwe hardware en software versies door gebruik te maken van formele procedures en door controles tijdens het plannen, ontwerpen, bouwen, configureren en testen

Voordelen

- meer succesvolle hardware en software releases
- efficiënter uitvoeren van releases
- in staat een hoger change niveau aan te kunnen
- minder incidenten als gevolg van implementaties
- minder incidenten als gevolg van versieconflicten

Begrippen

Release: Bestaat uit een geheel van nieuwe, gewijzigde en bestaande CI's dat op een moment beschikbaar wordt gesteld voor exploitatie

Package release: samengesteld uit individuele releases (full en/of delta releases) die gecombineerd, op dezelfde tijd uitgerold kunnen/moeten worden. Zo wordt het aantal releasementen beperkt en daarmee blijft de omgeving waarin wordt uitgerold stabiel.

DSL

Definitive Software Library: beschermde omgeving waar alle **geautoriseerde** versies van software-CI's worden opgeslagen. Bevat een kopie van alle aangeschafte en ontwikkelde software inclusief licentiegegevens en documentatie.

Randvoorwaarden:

- Toegang tot de DSL moet beveiligd zijn. Procedures noodzakelijk om foutieve en ongeautoriseerde wijzigingen te voorkomen: beveiliging,
- Beschikbaarheid van de DSL moet zijn gewaarborgd: backups, herstelplan
- Bepalen wanneer oude releases en software mag worden verwijderd uit de DSL
- Er moet een procedure worden opgesteld voor het uitvoeren van audits op de DSL
- De inhoud van de DSL moet worden bepaald: source code, object code, documentatie
- Naamgeving conventie binnen de DSL en van fysieke media waarop de DSL wordt bewaard
- Moet onderdeel zijn van het releasebeleid dan wel het Change- en Configuratie Management plan van de organisatie
- Moet zowel test- als productieomgevingen ondersteunen
- Er moet een capaciteitsplan zijn voor de DSL + een procedure om de grootte te kunnen monitoren

DHS

Definitive Hardware Storage: opslagplaats in de vorm van een beschermde omgeving voor reserveonderdelen en hardwarevoorraden.

Randvoorwaarden:

- beveiliging gewaarborgd
- beschikbaarheid onderdelen gewaarborgd
- details over de reserveonderdelen moeten in de CMDB worden opgenomen (!) voor het samenstellen van nieuwe systemen (hardware voorraad) of om bestaande onderdelen te vervangen (reserve onderdelen)
- gebruik van de componenten uit de DHS is tijdelijk (!). Dus na herstel van het origineel gaat het reserveonderdeel terug de DHS in of de DHS wordt aangevuld.

Back-outplan

Omschreven welke acties worden ondernomen om de service te herstellen als een uitrol van een release geheel of gedeeltelijk faalt

- Verantwoordelijkheid back-outplanning: Change Management
- Release Management voegt de back-outplannen van alle changes samen tot een Release Back-Outplan
 - Terugdraaien naar de Previous Trusted State: noodzakelijk bij full release, aanbevolen bij Delta release
 - Noodmaatregelen: bij een Delta Release als een back-out niet praktisch is

Indeling releases

- Impact en Omvang
 - Major Release
 - Minor Release
 - Emergency Fixes
- Type: Samenstelling en vorm
 - Delta Release
 - Full Release
 - Package Release

Succesfactoren

- Het belang voor de business duidelijk maken
- Aan de uitrol en releases gestelde eisen door de klant zijn bekend
- Configuration Management en Change Management dienen te zijn ingericht en naar behoren te functioneren
- Voldoende tijd en resources voor het vormgeven van release management

Prestatie Indicatoren

- de mate waarin releases binnen de gestelde planning worden afgerond
- aantal keren dat een release tot een backout leidde
- aantal bugs en andere fouten die in de productie-versies zijn aangetroffen

Knelpunten procesinrichting

- Weerstand
- Omzeilen; ook onbewust door bijvoorbeeld een nieuwe versie van software te downloaden vanaf internet
- Haast
- Versieverschillen; rekening mee houden bij gefaseerde distributie van software
- Testen: kostbaar

Relaties met

- configuration management: de uitrol van nieuwe CI versies heeft invloed op statusinformatie van- en relaties tussen CI's
- change management: wijzigingen kunnen resulteren in nieuwe HW, SW of documentatie versies die veilig, beheerst en gepland (Ezelsbrug GVB) door Release Management worden uitgerold
- service level management
- incident management en problem management: RIM procedures kunnen intern door INC en PRB worden gebruikt

Activiteiten

1. Release beleid: hoe en wanneer releases worden samengesteld

6 aspecten

- Naamgeving en nummering releases; moeten logisch zijn
- Vaststellen definitie en frequentie major en minor releases
- Beleid ten aanzien van spoedwijzigingen (emergency fixes) moet zijn beschreven
- Vaststellen van bedrijfskritische tijden gedurende welke releases moeten worden vermeden
- Bepalen deliverables (installatie instructies, release notes)
- Beleid voor het opstellen en testen van back-out plannen

2. Opstellen van een releaseplanning:

- afstemming over de inhoud van de release
- afspraken over fasering in tijd, locaties en organisatieonderdelen
- bepaal de release vorm

3. Release ontwerp, bouw en samenstelling

4. Release acceptatie: voor elke stap in de testprocedure moet formeel acceptatie worden afgegeven aan Change Management. Alleen als alle release onderdelen zijn getest en geaccepteerd, wordt de release door change management vrijgegeven

5. Uitrol/rollout plan:

Releaseplan aanvullen met

5 aspecten

- tijdschema
- overzicht bemensing
- te installeren CI's
- communicatieplan
- vergaderplan

Mogelijke Scenario's

- Big Bang
- Gefaseerd: als oude en nieuwe versies geen versieconflicten geven
 - Incrementeel: functionaliteit gefaseerd uitgerold naar alle gebruikers
 - Evolutionair: alle functionaliteit per groep gebruikers of per locatie uitgerold

6. communicatie, voorbereiding en training

- het ontwikkelen van een kwaliteitsplan voor de release
- het plannen van de acceptatie van de release door de beheerorganisatie en door gebruikers

7. distributie en installatie

Daarnaast:

- Het bewaken en beheren van de inhoud van de DSL en DHS
- Het beheren en distribueren van alle hardware- en software versies die in gebruik zijn en door de ICT afdeling worden ondersteund, ten einde te voldoen aan het vereiste niveau van de dienstverlening
- Het zekerstellen dat alleen correcte en geautoriseerde versies worden uitgerold en dat de aan te passen hard- en software wordt beheerd

Service Level Management

Doelstelling

Onderhouden en verbeteren van de met de klant overeengekomen dienstverlening door afspraken te maken, diensten te monitoren en hier over te rapporteren aan de klant

- Doorlopen van een continue cyclus van afspreken, bewaken en rapporteren van IT service resultaten
- starten van acties om gebreken in de dienstverlening te elimineren in juiste verhouding tot de business en de kosten
- Ontwikkelen van een betere relatie tussen IT en de klanten.

Voordelen

- IT diensten worden ontworpen conform de verwachtingen van de klanten
- Diensten worden meetbaar gemaakt en kunnen daardoor beheerst worden
- De business kan een goede afweging maken tussen de gewenste kwaliteit en de te maken kosten
- Een verbeterde relatie met- en grotere tevredenheid bij de klant
- Betere kwaliteit dienstverlening
- Duidelijkheid in wederzijdse verwachtingen

Begrippen

2 Verschillen tussen een klant en een eindgebruiker:

Klant:

- Namens de organisatie bevoegd om afspraken te maken
- Focus op kwaliteit en kosten

Eindgebruiker:

- Niet bevoegd om afspraken te maken
- Focus op functionaliteit

Service Catalogus / Dienstencatalogus: gedetailleerd overzicht in, voor de klant, begrijpelijke bewoordingen van aangeboden diensten + het niveau van de serviceverlening

Service Improvement Plan (SIP): Een formeel project met vastgestelde doelen, acties en opleverdata voor meetbare verbeteringen van de ICT dienstverlening. Is SMART, bevat:

- Wat onderzoeken en wat realiseren scope
- Op welke termijn planning
- Met welke middelen
- Normen om verbeteringen te kunnen meten

Service Quality Plan (SQP): document met daarin alle benodigde informatie om de kwaliteit van een ICT dienst bij te sturen. Streefwaarden worden als Performance Indicatoren (PI's) vastgelegd zoals: responstijd, beschikbaarheid, doorlooptijd, kosten.

Verschillen tussen een SLA, OLA en een UC

Operational Level Agreement:

- Afspraken met interne leverancier
- Geen juridische status

Underpinning Contract:

- Contract met een externe leverancier
- Heeft een juridische status

Service Level Agreement:

- Afspraken met een klant
- Geen juridische status

SLA: overeenkomst tussen de ICT organisatie en een klant met een overzicht van afgesproken diensten in, voor de klant, begrijpelijke bewoordingen

- Service Based
Eén of meerdere services beschreven die voor alle gebruikers van deze services gelden
- Customer Based
Een SLA overeengekomen met een specifieke klant met daarin alle services die gelden voor die klant
- Multi Level
Afspraken op corporate level, customer level en service level vastgelegd

Activiteiten

- Onderhoud Dienstencatalogus
- Opstellen en uitvoeren SIP
- Afspraken maken
 - Identificeren (behoeften klant: deze uitdrukken in meetbare eenheden)
 - Definieren (diensten: resultaten zijn getekende SLR's)
 - Contracteren (SLA, OLA, UC)
- Afspraken borgen
 - Monitoren (bewaken streefwaarden van diensten)
 - Rapporteren (service resultaten)
 - Evalueren (service levels, vaststellen trends)

Succesfactoren

management van verwachtingen

ken uw klant

UC's en OLA's

inzichtelijk maken dat IT kosten dalen voor stabiele services

Prestatie Indicatoren

welk deel van de SLA wordt ondersteund door OLA's en UC's

welk deel van de afgesproken service levels wordt gehaald

hoe verloopt de trend t.a.v. de geleverde service levels

Knelpunten

- Cultuuromslag bij zowel de klant als de leverancier
- Eisen en verwachtingen van een dienst lastig te formuleren
- Lastig om diensten in meetbare waarden uit te drukken
- Oppassen voor al te ambitieuze plannen
- Service levels meten en bewaken kost veel overhead
- Volgorde wordt niet altijd aangehouden, maar er wordt meteen met een SLA begonnen

Relaties met

- service desk, incident management, problem management, configuration management, release management, financial management, availability management, capacity management, IT service continuity management
- change management:
 - Wijzigingen kunnen van invloed zijn op afspraken in de SLA
 - SLM bewaakt de kwaliteit van de service en de afspraken in de SLA op het moment dat wijzigingen worden vastgesteld en als ze worden doorgevoerd

Financial management for IT services

Doelstelling

Het voorzien in een kosteneffectief beheer van de ICT-middelen door kosten te identificeren en vervolgens te relateren aan Diensten, Activiteiten en Klanten.

Voordelen

- groter vertrouwen in het opzetten en beheren van budgetten
- het berekenen van de kosten van IT-diensten
- indien noodzakelijk de IT-organisatie te laten functioneren als een business unit
- doorbelasten van kosten aan de organisatie maakt sturing op kosten mogelijk
- klantgedrag kan worden bijgestuurd (binnen het proces Capacity Management), bijvoorbeeld door gescheiden tarieven voor piek- en daluren
- Professionalisatie van de IT organisatie en van de relatie met de klanten

Activiteiten (*Ezelsbrug: BAC*)

- Budgetting – kosten voorspellen en uitgaven beheersen
 - Zero-based = geen rekening houdend met het budget van afgelopen periode
Vaak voor de langere periode
 - Incremental = rekening houdend met cijfers verleden jaar
Vaak jaarlijkse bijstelling
- IT Accounting
 - Verantwoorden waaraan geld is uitgegeven. Aan welke Dienst, Activiteit, Klant (*ezelsbrug DAK*)
 - Identificeren kosten om zo kostensoorten in te delen in kostenposten
 - Informatie verstrekken over de return op investeringen

Return = de verhouding tussen de toename van de winst en het geïnvesteerde bedrag die er mee kan worden bereikt

ROI = Return On Investment = $\text{gem. toename van de winst} / \text{investeringskosten over een aantal jaren}$

TCO = Total Cost of Ownership: de totale kosten gedurende de gehele life cycle van een product of dienst. Inclusief afschrijving, personeelskosten, allocatie en geplande vervanging

- Charging – het doorbelasten aan de klant van de aan hem geleverde diensten
Methoden:
 - Communication of Information: alleen informatie over kosten en door te belasten bedragen
 - Pricing Flexibility: prijzen per jaar, extra kosten achteraf verrekenend
 - Notational Charging: Wel facturatie, geen betaling
 - Pricing: betalen van de prijs per product/dienst
 - Cost plus = gemaakte kosten + winstopslag
 - Going Rate = diensten met standaard prijsafspraken
 - Target Return = diensten waarvoor van te voren is vastgesteld wat ze op moeten brengen
 - What the market will bear = prijzen zijn marktconform
 - Negotiated Contract Price = over prijzen wordt onderhandeld

Implementeren

- Accounting Center. Alleen accounting om kostenbewustheid te verhogen
- Recovery Center. Het berekenen en verdelen van kosten over de ICT-diensten.
- Profit Center: ICT-afdeling opereert als aparte business unit die werkt met Subsidie, Break-even of zelfs met winst

Kostencategorieën

Per product/dienst kijken welke kosten wel/niet kunnen worden gerekend

Indeling 1:

- Directe kosten – kosten van een product/dienst die direct aan dit product of deze dienst toe te wijzen zijn
- Indirecte kosten (overhead)
 - Hoofdelijk omslaan gebruikers
 - Activity Based Costing gebruik

Indeling 2:

- Vaste kosten – kosten die verbonden zijn aan de levering van een product/dienst en die niet afhankelijk zijn van de hoogte van de productie (bijv. telefoon abonnement voor een internet aansluiting)
- Variabele kosten (bijv. papier voor een printer)

Indeling 3:

- Capitalkosten - Afschrijving aanschafkosten productiemiddelen
- Revenuekosten (operational ofwel regelmatige kosten waar geen ICT-productiemiddel tegenover staat): diensten zoals verzekeringen, onderhoud en licenties

Kostensoorten (HH SOUP)

- Hardwarekosten
- Softwarekosten
- Personeelskosten
- Huisvestingskosten
- Uitbestedingskosten (hardware, software, personeel, huisvesting)
- Overdraagbare kosten (van/aan een interne afdeling, dus niet aan een klant)

Succesfactoren

- | | |
|--|------------|
| • SLA's zijn afgesloten en zijn in werking | afspraken |
| • Voldoende kennis van accounting en charging | kennis |
| • Zo eenvoudig mogelijke kostenberekening en doorbelasting | eenvoud |
| • Voldoende informatie uit andere processen | informatie |
| • Erkenning van het belang door het management | belang |

Knelpunten

- Geen acceptatie bij de klant omdat betalen voor ICT diensten nieuw is
- Niet serieus genomen door gebrek aan betrokkenheid bij- en beleid vanuit- het ICT Management
- Weinig mensen met zowel financiële als ICT kennis

Prestatie Indicatoren

- Accurate kosten- en batenanalyse
- De methode van verrekening wordt als redelijk ervaren door de klant
- Het gebruiksgedrag van de klant verandert

Relaties met

- service level management: stelt verwachtingen van de klant vast en maakt afspraken over de verplichtingen
- capacity management en configuration management: asset data in de CMDB nodig om kosten van (de capaciteit van) een dienst vast te kunnen stellen

Availability Management

Doelstelling

Het kosteneffectief bewaken van de met de klant in het SLA overeengekomen beschikbaarheid van de ICT dienstverlening.

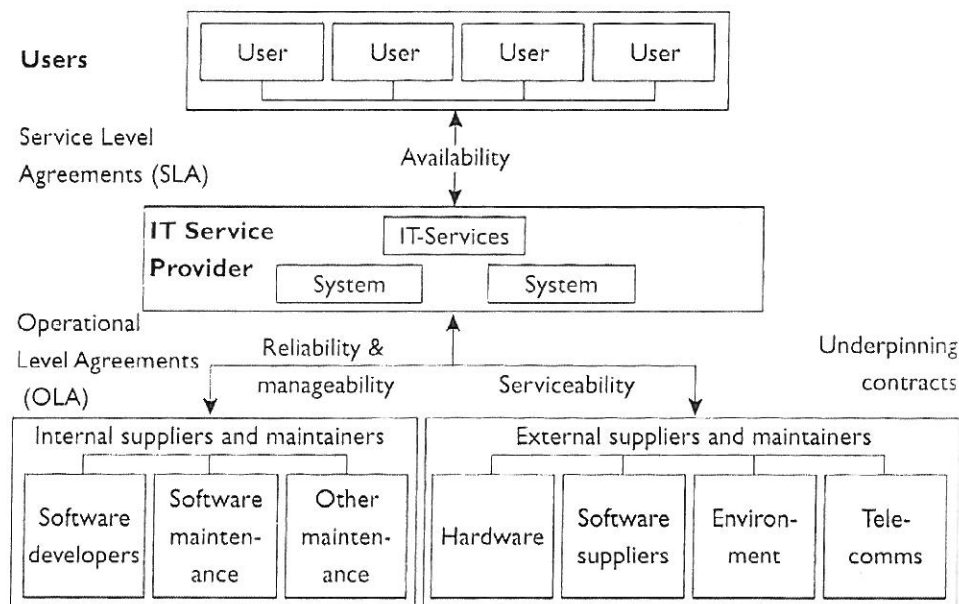
Hiertoe worden de wensen van de klant in overeenstemming gebracht met de mogelijkheden van de ICT-infrastructuur.

Proactief: storingen voorkomen door te plannen

Reactief: storingen verhelpen door te bewaken

Uitgangspunten

- AVA vormt de kern van de tevredenheid van de klant over de ICT dienstverlening
- Ook als dingen misgaan, is het nog mogelijk om de klant tevreden te stellen
- AVA alleen te verbeteren met inzicht in hoe ICT-diensten de bedrijfsprocessen bij de klant ondersteunen



Aspecten: Ezelsbrug AM RRR SS

Availability	Beschikbaarheid	De mate waarin de klant over een dienst kan beschikken op de <u>tijd</u> en de <u>plaats</u> die de klant wenst. Beïnvloed door: • Complexiteit van de ICT-infrastructuur • Betrouwbaarheid van de onderdelen van de ICT-infrastructuur • Betrouwbaarheid van de omgeving van de ICT-infrastructuur • Het vermogen om snel te reageren op verstoringen • Niveau en hoeveelheid onderhoud door leveranciers • Kwaliteit van operationele processen en procedures
Reliability	Betrouwbaarheid	De mate waarin de klant kan vertrouwen op de JGTV van de gegevensverwerking: • Juistheid • Volledigheid • Tijdigheid • Geoorloofdheid
Resilience	Veerkracht	De mate waarin een dienst of de componenten van een dienst blijft functioneren als één van de onderdelen van de dienst is uitgevallen
Serviceability	Onderhoudsverplichting	De mate waarin in contractuele verplichtingen op afgesproken configuratie items (in UC's) door externe leveranciers (Third Party IT Service Providers) worden nagekomen. Indirect gemeten: • Beschikbaarheid • Betrouwbaarheid • Onderhoudbaarheid
Maintainability	Onderhoudbaarheid	De mate waarin <u>onderdelen van de ICT-infrastructuur</u> kunnen worden hersteld naar de operationele status. Een indicatie voor het gemak waarmee onderhoud aan een ICT-dienst kan worden gepleegd. Aspecten: • Anticiperen op fouten • Detectie van fouten • Diagnose van fouten • Herstellen van fouten • Herstellen van data en dienstverlening • Preventief onderhoud
Recoverability	Herstelbaarheid	De inspanning die nodig is om een <u>dienst</u> te herstellen als deze uitvalt Aspecten: • Detectie van fouten • Diagnose van fouten • Herstellen van fouten • Herstellen van de dienstverlening
Security	Beveiliging	De mate waarin de onderdelen van de ICT-infrastructuur zijn beschermd tegen • Opzettelijke wijziging • Vernietiging • Ongeoorloofde toegang Aspecten: • Vertrouwelijkheid, Integriteit en Beschikbaarheid ('VIB' van Security Management) van data

Beschikbaarheid component

$$BP = 100\% * (OT - ST) / OT$$

Beschikbaarheid dienst

$$BP1 * BP2 \dots * BPn$$

Beschikbaarheid dubbel uitgevoerd component

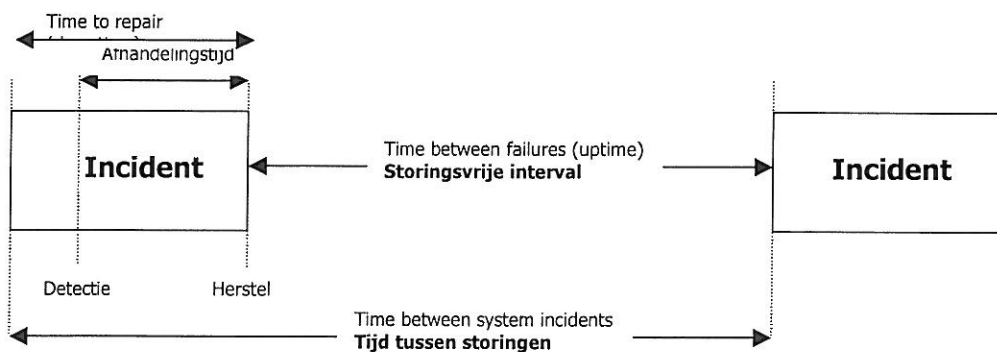
$$100\% - ((100\% - BP1/100) * (100\% - BP2/100))$$

BP = Beschikbaarheidspercentage

OT = Overeengekomen Service Tijd

ST = Storingstijd tijdens de Overeengekomen Service Tijd

Metten van beschikbaarheid



Verstoring start wanneer een incident is vastgesteld door een gebruiker of een systeemmonitor

Storingstijd = Time to repair = downtime

Bestaat uit

- Detectietijd tijd tussen ontdekken en melden van een incident
- Afhandelingstijd
 - Reactietijd ook wel responsetijd: tijd nodig om in actie te komen
 - incl. Diagnosetijd!
 - Reparatie tijd repareren dienst/component
 - Hersteltijd het weer beschikbaar stellen van dienst/component

Activiteiten (Ezelsbrug PCB's)

1. Planningsgericht (identificatie en ontwerp)
 - Identificeren kritische bedrijfsprocessen
 - Bepalen wat de klant verstaat onder niet-beschikbaarheid
 - Vaststellen wat de impact van niet-beschikbaarheid is op deze bedrijfsprocessen
 - Bepalen beschikbaarheidsbehoefte van de klant voor SLM. Vergeleken met mogelijkheden, kosten in afweging meegenomen
 - ontwerpen van de beschikbaarheid en herstelbaarheid
 - aandachtspunten voor beveiliging
 - managen van onderhoudsactiviteiten, onderhoudsafspraken
2. Controle/Besturingsgericht (meten en rapporteren)

$MTBSI = MTBF + MTTR = \text{mean uptime} + \text{mean downtime}$
 $MTTR = \text{gemiddelde time to repair} / \text{storingstijd} / \text{downtime}$
 $MTBF = \text{gemiddelde time between failures} / \text{storingsvrije interval} / \text{uptime}$
 $MTBSI = \text{gemiddelde time between system incidents} / \text{tijd tussen incidenten}$
3. Opstellen beschikbaarheidsplan
 - Belangrijkste product van AVA.
Géén implementatieplan, maar een meerjarenplan met actuele situatie + voorstellen voor verbeteringen bestaande diensten + richtlijnen nieuwe diensten
Input vanuit SLM, ITSCM, CAP, FIN, SEC.
Bevat:
 - Hoe vorm te geven aan de aspecten (AM RRR SS)
 - Benodigde inspanning / personeel
 - Activiteiten
 - Kosten
 - Aansluiting met het beleid

Voordelen

Belangrijkste: de ICT-organisatie is in staat om ICT-diensten te ontwerpen die voldoen aan de met de klant overeengekomen beschikbaarheidseisen.

- Focus op de beschikbaarheid van kritische bedrijfsprocessen
- Het hebben van 1 aanspreekpunt en 1 eindverantwoordelijke voor de beschikbaarheid van producten en diensten
- Bewaken van beschikbaarheid en beschikbaarheidnormen
- Kunnen meten van alle aspecten van beschikbaarheid
- Correctieve maatregelen bij niet-beschikbaarheid
- Afnemen van het aantal momenten en van de duur van niet-beschikbaarheid

Knelpunten

- Lastig om een afweging te maken tussen het niveau van beschikbaarheid en de kosten (versus de opbrengsten / return)
- Er wordt een te hoge beschikbaarheid nagestreefd
- Beschikbaarheid wordt vaak in technische taal aan een klant uitgelegd: vertaling nodig van beschikbaarheid componenten en informatiesystemen naar diensten (keten).
- Verantwoordelijkheid over beschikbaarheid vaak over meerdere managers verdeeld
- Aansturen van interne en externe leveranciers is moeilijk
- Overige beheerprocessen moeten goed zijn ingericht
- Beschikbaarheid richting internet is een beveiligingsrisico

Succesfactoren

- Kennis nodig van zowel ICT-diensten als bedrijfsprocessen bij de klant
- Kennis van de impact van beschikbaarheids storingen op deze bedrijfsprocessen
- Voldoende mensen met de juiste skills
- Goede system management tools
- Configuration management, incident management en problem management dienen te zijn ingericht en naar behoren te functioneren

Prestatie Indicatoren

- beschikbaarheidspercentage per dienst of gebruikersgroep
- duur van de niet-beschikbaarheid
- de frequentie van de niet-beschikbaarheid

Relaties met

- service level management: afspraken in de SLA. Beschikbaarheid bewaakt/gemeten en gerapporteerd binnen Availability Management
- incident management en problem management: input vanuit INC en PRB over verstoringen om de juiste correctieve acties uit te kunnen voeren
- change management
- configuration management
- capacity management
- IT service continuity management

Ondersteunende Methoden/Technieken

CFIA	Component Failure Impact Analysis	Beschikbaarheidsmatrix. Per dienst het belang per onderdeel
FTA	Fault Tree Analysis	Om keten van gebeurtenissen te herleiden die kan leiden tot een verstoring
CRAMM	CCTA Risk Analysis and Management Method	Risicoanalyse (M iddelen, K wetsbaarheden, B edreigingen) Risicomanagement (T egenmaatregelen)
SOA	System Outage Analysis	Techniek om oorzaak storing te achterhalen + verbeteringen
TOP	Technical Observation Post	<i>"Een team van ICT-specialisten richt zich op een deelaspect van de beschikbaarheid waardoor snel resultaten worden behaald"</i>

Voordelen CRAMM:

- Nuttige informatie over bedreigingen en kwetsbaarheden
- Preventieve maatregelen kunnen worden genomen

Voordelen CFIA:

- Beschikbaarheidsmatrix waardoor afhankelijkheden van componenten voor diensten inzichtelijk worden
- Inzicht in welke diensten complex en foutgevoelig zijn

Capacity Management

Doelstelling

Het tegen verantwoorde kosten beschikbaar stellen van de juiste capaciteit aan ICT middelen die voorzien in de huidige en toekomstige behoeften van de klant
Capacity Management maakt hiertoe voortdurend de afweging tussen enerzijds de kosten en de capaciteit en anderzijds tussen vraag en aanbod

Begrippen

Capaciteitsplan: bevat een analyse van de huidige situatie en, gebruik makend van verschillende scenario's, een voorspelling over de toekomstige capaciteitsvraag.

Capacity Management Database (CDB): Een verzameling gegevensbronnen met technische (dienst- en werklust-) en zakelijke (business- en financiële-) gegevens over de capaciteit van de onderdelen van de ICT Infrastructuur

- Resource voorspelling (juistheid en tijdigheid)
- Mate waarin de toepassing van technologie de SLA's beïnvloed
- Hoe de performance van componenten kan worden gemeten
- Voorspelling van uitgaven
- Mate waarin de capaciteit overeenkomt met de huidige en toekomstige wensen van de klant. Dit om performance en capaciteitsincidenten te voorkomen

De wet van Moore: de capaciteit van elke nieuwe geheugenchip is dubbel zo groot als zijn voorganger. Deze verdubbeling vindt ongeveer één keer per anderhalf jaar plaats

De wet van Parkinson: data zal altijd de beschikbare capaciteit vullen

Subprocessen (*Ezelsbrug BSR*)

- Business Capacity Management: verkrijgen van **inzicht** in toekomstige capaciteitsbehoeften
 - Ondersteuning SLM bij het opstellen van de SLR's door
 - Application Sizing: bepalen van de benodigde hardwarecapaciteit van nieuwe of gewijzigde applicaties: verwachte prestaties, benodigde hardware en kosten
 - Modelling: modellen om gevolgen van inzet/uitbreiding van capaciteit in kaart te brengen: Trendanalyse, Analytisch modelleren, Simulatie, Baseline
 - Ontwerp, aanschaf of verbetering van nieuwe diensten
 - Update de CMDB (onder verantwoordelijkheid CFM) en de CDB
 - Verificatie SLA: SLM targets geven die gemeten kunnen worden
 - Aanpassen SLA: SLM aan de hand van SLR's

Financiële gegevens: Bijv. Hardware en Software kosten

Business gegevens: Bijv. aantal gebruikers en locaties

- Service Capacity Management: **monitoren** en **bijsturen** van prestaties van operationele ICT diensten:
 - Proactief, hiermee worden problemen voorkomen
 - Reactief, maatregelen bij performanceproblemen om de overeengekomen serviceperformance te halen

Methode: Demand Management: vraagbeheer, bijsturen van de vraag naar capaciteit

 - Short Term: als op korte termijn een structureel tekort aan capaciteit dreigt en aanvullende capaciteit niet direct voorhanden is
 - Long Term: gedurende langere periode dreigt een tekort aan capaciteit waarbij het uit kostenoverwegingen niet verantwoord is om aanvullende investeringen te doen

Dienst gegevens: Bijv. transactietijden, batch job tijden

- Resource Capacity Management: **beheren** van individuele onderdelen van de ICT infrastructuur. Proactief, hiermee worden problemen voorkomen
 - Proactief, informatie verzamelen over en monitoren van resources zoals processoren, geheugen, schijven, bandbreedte, netwerkverbindingen

Methode: Performance Management: meten, bewaken en bijstellen van de prestaties van onderdelen van de ICT infrastructuur

Werklast gegevens: cpu belasting, bandbreedte, paging

Operationele activiteiten

- Monitoring
- Analyse
- Tuning
- Implementation

Voordelen

- Beter inspelen op capaciteitsbehoefte van de klant (monitoren, voorspellen)
- Verminderen van incidenten als gevolg van te weinig capaciteit
- Verminderen van urgente wijzigingsvoorstellen door verkeerde capaciteitsinschatting
- minder risico's op performance problemen en uitval
- Efficiënter benutten huidige capaciteit
- Kostenbesparing

Knelpunten

- Vaak geen centraal aanspreekpunt
- Te hoge verwachtingen van nieuwe applicaties
- Leveranciers verstrekken verkeerde gegevens
- Veel performanceafhankelijkheden bij veel platforms en koppelingen
- Plannen van de klant vaak niet concreet genoeg om een goed capaciteitsplan op te stellen

Succesfactoren

- Accurate voorspellingen van ontwikkelingen in de business
- Een goed begrip van de huidige en toekomstige technologie
- Het vermogen om kosteneffectiviteit ook aan te tonen
- Goede system management tools

Prestatie Indicatoren

- Het tijdig kunnen aangeven van werklastontwikkelingen en –trends en de accuratesse van het capacity plan
- Reductie van het aantal paniek aankopen, reductie van niet te gebruiken of te dure overcapaciteit
- Reductie van het aantal incidenten vanwege performance problemen

Relaties met

- configuration management
- incident management
- problem management
- change management + release management:
 - informatie uit deze processen ter evaluatie om de impact op capaciteit en performance vast te stellen
 - richting deze processen als er wijzigingen op het gebied van capaciteit plaats moeten vinden
- service level management
- IT service continuity management
- availability management
- financial management

IT service continuity management

Doelstelling

Het optimaal ondersteunen van het totale Business Continuity Management proces door het nemen van preventieve maatregelen

- om calamiteiten te voorkomen
- om de impact van calamiteiten op de bedrijfsprocessen te verminderen
- waarmee na het optreden van een calamiteit de dienstverlening zo snel mogelijk kan worden hervat: binnen de met de business overeengekomen termijn

Het proces dat binnen de ICT dienstverlening de risico's van calamiteiten voor ICT diensten analyseert en beheerst zodat te allen tijde de minimale ICT dienstverlening wordt gewaarborgd

Vergelijking ITSCM met BCM:

- BCM: Continuïteit van en risico's voor de bedrijfsprocessen met het oog op de productiecapaciteit
- ITSCM: continuïteit van en risico's voor de dienstverlening met het oog op beschikbaarheid

Voordelen

- actief, preventief risicomanagement: bewustwording van risico's
- organisatie beter in staat om te anticiperen op calamiteiten
- gevolgen van calamiteiten blijven beperkt
- hersteltijd voor de dienstverlening is korter

Knelpunten

- Gebrekkig bewustzijn van risico's
- Moeilijk geld vrij te maken als er nooit calamiteiten zijn
- Inrichting moet projectmatig: extra capaciteit vrijmaken
- Vertaalslag van BCM naar ITSCM is lastig

Begrippen

Versil tussen een herstelplan en een uitwijkplan:

- ❖ Herstelplan: Hoe na een calamiteit de zakelijke activiteiten en ICT diensten kunnen worden hersteld
- ❖ Uitwijkplan: Welke uitwijkopties er zijn voor de calamiteiten die niet met voorzorgsmaatregelen worden voorkomen

Calamiteit: verstoring van een ICT dienst of systeem met aanzienlijke gevolgen voor de continuïteit van de dienstverlening

Let op het verschil met

Een incident:

- ❖ Elke gebeurtenis die afwijkt van de standaardwerking van een ICT dienst en die de kwaliteit van de dienst vermindert of verstoort

Een beveiligingsincident:

- ❖ Incident dat de betrouwbaarheid (oftewel de 'VIB') van de informatievoorziening verstoort

Activiteiten (*Ezelsbrug IU BIO*)

Fase 1: Initiatie

- Bepalen BCM en ITSCM beleid
- Bepalen van de scope
- Het toewijzen van middelen
- Inrichten v/e projectorganisatie

Fase 2: Uitgangspunten en strategie / Identificeren Business Requirements

- Uitgangspunten
 - Business Impact Analyse onderzoekt
 - wat de kritische bedrijfsprocessen zijn
 - wat de bijbehorende kritische informatiesystemen zijn
 - wat de bijbehorende infrastructurele componenten zijn
 - welke schade het bedrijf lijdt bij uitval
 - wat de omvang van de schade is
 - Risicoanalyse (*bijvoorbeeld CRAMM zoals bij AVA*)
 - Onderzoekt wat de bedreigingen en kwetsbaarheden van de IT middelen zijn
 - Identificeert voorzorgsmaatregelen
- Continuïteitsstrategie
 - Business Continuity Strategy
 - Weegt kosten en risico's af
 - Bepaalt de keuze tussen risico vermindering en herstelplanning van kritische bedrijfsprocessen

Voorbeelden van risicobeperkende maatregelen

- Backup en recovery strategie
- Eliminatie van Single Points of Failure (SPOF)
- Uitbesteden van diensten aan meer dan één dienstverlener
- Opzetten van een veerkrachtig ICT systeem
- Goede toegangsbeveiliging

Voor de overige risico's: Herstelopties voor (zie de taart "IL DAG ~~POP~~")

- Mensen en Accommodatie
- ICT systemen, netwerken: in samenwerking met AVA
- Bedrijfskritische diensten (stroom, water, telefoon, internet)
- Bedrijfskritische middelen (dossiers, contracten)

Herstelopties

- Niets doen
- Handmatige work-arounds
- Reciprocal Agreements: onderlinge afspraken tussen twee organisaties
- Gradual Recovery / Cold Stand-By (> 72 uur)
 - Vaste ruimte
 - Portable ruimte
- Intermediate Recovery / Warm stand-by (> 24 uur < 72 uur)
 - Interne ruimte
 - Externe ruimte
 - Portable ruimte
- Immediate Recovery / Hot stand-by (< 24 uur)

Fase 3: Implementatie

- inrichten van de organisatie en ontwikkelen implementatieplannen
Gericht op een efficiënte beslissingsstructuur
- implementeren van stand-by maatregelen
- implementeren van risicobeperkende maatregelen
Zoals UPS, noodstroom, RAID, archivering op andere locatie
- Ontwikkelen van herstelplannen en procedures
- Initieel testen

Fase 4: operationeel management (blijvend / continu!)

- opleiding, training en bekendheid bij personeel en management
- training recovery teams
- review en audit
- testen
- change management (impact changes op plannen)
- procesbeheer en rapportages

Succesfactoren

- configuration management, availability management en service level management dienen te zijn ingericht en naar behoren te functioneren
- begeleiding en commitment vanuit de hele organisatie
- goede en moderne tooling
- specifieke training voor participanten van het proces
- regelmatig maar onverwacht testen van het herstelplan

Prestatie Indicatoren

- het aantal geconstateerde tekortkomingen in het recoveryplan
- gemiste inkomsten na een calamiteit
- kosten van het operationeel management van het proces
- Hersteltijd na het optreden van een calamiteit
- Effectiviteit van de risicobeperkende maatregelen

Relaties met

- service level management
- change management: impact wijzigingen op herstelplannen
- configuration management
- capacity management
- availability management: afhankelijkheid van veerkracht + recoverability + backups systemen

Security Management

Doel is tweeledig

- Voldoen aan externe beveiligingseisen zoals vastgelegd in de wet, contracten, SLA's en beleid van de organisatie
- Voldoen aan interne beveiligingseisen om te voorzien in de continuïteit van de ICT-dienstverlener door het voldoen aan een zeker basisniveau van beveiliging

Voordelen

- Evenwicht tussen de waarde van informatie en passende hoeveelheid beveiligingsmaatregelen
- Draagt bij aan de continuïteit van de business en aan het bereiken van bedrijfsdoelstellingen

Wetten

- Grondwet
- Wet Computer Criminaliteit (WCC)
- Wet Bescherming Persoonsgegevens (WBP)
- Telecommunicatiewet
- Auteurswet

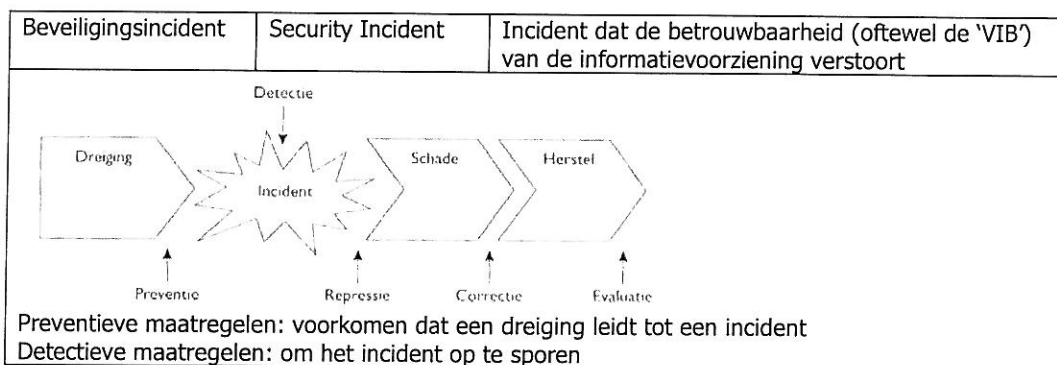
Begrippen

Betrouwbaarheid	Reliability	Combinatie van (<i>Ezelsbrug VIB of CIA</i>) Zie AVA: de JGTV van gegevensverwerking
<i>Vertrouwelijkheid</i>	<i>Confidentiality</i>	De mate waarin toegang tot- en gebruik van gegevens beperkt is tot degenen die daartoe zijn geautoriseerd
<i>Integriteit</i>	<i>Integrity</i>	Juistheid, Correctheid, Volledigheid van informatie
<i>Beschikbaarheid</i>	<i>Availability</i>	De mate waarin informatie op het juiste moment op de juiste plek beschikbaar is voor de gebruiker

Informatiebeveiliging	Information Security	Waarborging betrouwbaarheid (VIB) van de informatiesystemen en de daarin opgeslagen gegevens
-----------------------	----------------------	--

Standaarden voor Informatiebeveiliging

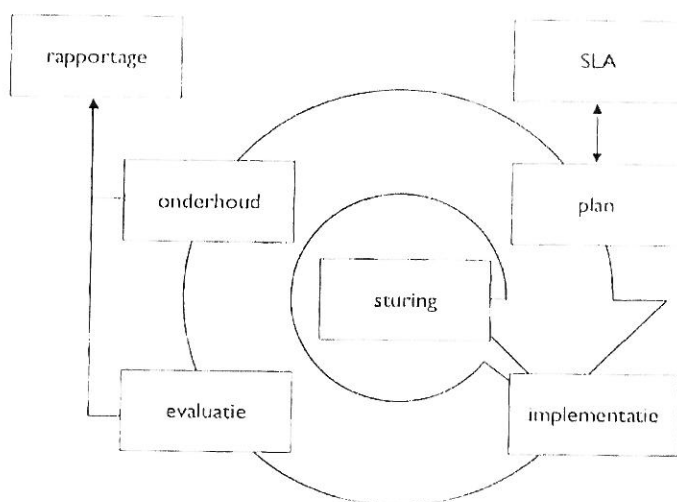
- Security Management binnen ITIL
- Code voor Informatiebeveiliging van het Nederlands Normalisatie Instituut
- Code of Practice for Information Security Management (BS7799)
- Voorschrift Informatiebeveiliging Rijksdienst (VIR94)



Repressieve maatregelen: negatieve invloed van een incident beperken		
Correctieve maatregelen: om objecten te herstellen die zijn beschadigd		
Privacy	Privacy	De vertrouwelijkheid en integriteit (VI) van gegevens die tot een <u>natuurlijke</u> persoon kunnen worden herleid
Bedreiging	Thread	Een gebeurtenis die de betrouwbaarheid (VIB) van informatie aan kan tasten

Veiligheid	Safety	Gevrijwaard zijn van bekende risico's
Beveiliging	Security	Het voorkomen van onbewuste risico's
		Middel om veiligheid te waarborgen

Subprocessen



Sturing	Hart van Security Management. • Organiseert en bestuurt • Ontwikkeling van beleid • Raamwerk voor informatiebeveiliging • Definiëren en aansturen andere subprocessen
Plannen	Activiteiten die leiden tot de beveiligingsparagraaf in de SLA. Vertaling SLA naar OLA's en Underpinning Contracts
Implementatie	Invoering in plannen gespecificeerde maatregelen zoals • Classificatie (VIB) en beheersing ICT-hulpmiddelen • Personele beveiliging • Veilig beheer • Toegangsbeveiliging
Evaluatie	Eigen beoordeling / Self Assessment Interne audit door interne EDP-auditor Externe audit door externe EDP-auditor (Audit = onafhankelijke evaluatie)
Onderhoud	Onderhoud van informatie beveiligingsplannen omdat ICT-infrastructuur en – omgeving voortdurend veranderen. Onderhoud SLA, OLA en Underpinning Contract
Rapportage	Rapportage over geleverde beveiligingsdiensten conform afspraak in de SLA