Provincie Noord-Brabant

# PNB Architectuur Handboek PICRA

## Provincie Noord-Brabant

## Cloud & Infrastructuur Architectuur

Beschreven voor: Provincie Noord-Brabant
Auteur: Peter van de Bree
Datum: 20/12/2023

Opmerkingen:

# Inhoudsopgave





# 1 Document historie

## 1.1 Document richtlijnen

### Licentie beheer



Voor vragen of meer informatie kunt u contact opnemen met:

P.E.V. van de Bree
Eigenaar
Cloud and Clear IT Consultancy
Ekster 25
3191 DA Rotterdam

### Document Classificatie

Alleen toegankelijk voor *Provincie Noord-Brabant* (IT) personeel en projectleden.

### Disclaimer



### Document gebruik



## 1.2 Versie beheer

| Datum | Versie | Auteur(s) | Wijziging |
|---|---|---|---|
| 27-03-2023 | 0.1 | Peter van de Bree | Initiële template versie |
| 30-03-2023 | 0.2 | Peter van de Bree | Aanvullingen |
| 31-03-2023 | 0.3 | Peter van de Bree | Aanvullingen |
| 01-04-2023 | 0.4 | Peter van de Bree | Aanvullingen |
| 05-04-2023 | 0.5 | Peter van de Bree | Aanvullingen |
| 06-05-2023 | 0.6 | Peter van de Bree | Aanvullingen |
| 07-06-2023 | 0.9 | Peter van de Bree | Oplevering 0.9 aan Architecture Board |
| 31-08-2023 | 0.91 | Peter van de Bree | Review Jeffrey Otten |
| 27-09-2023 | 0.92 | Peter van de Bree | Review Claus Hormann |
| 02-10-2023 | 0.93 | Peter van de Bree | Review Ruud van der Lee |
| 20-12-2023 | 1.0 | Peter van de Bree | Reviews verwerkt en afgestemd. Final |

## 1.3 Distributie

Dit document is op de onderstaande locatie gedeeld:

| Versie | Datum | Locatie | Firma |
|---|---|---|---|
| 1.0 | 20-12-2023 | Teams Project Site Architectuur Board | *Provincie Noord-Brabant* |
| 1.0 | 20-12-2023 | Teams Project Site DVL-ICT | *Provincie Noord-Brabant* |
| | | | |
| | | | |

## 1.4 Afkortingen en begrippen

| | |
|---|---|
| **CA** | Certificate Authority: servers die gemachtigd zijn beveiligingscertificaten uit te delen in een PKI |
| **CISO** | Chief Information Security Officer |
| **CRL** | Certificate Revocation List, een lijst van ingetrokken certificaten die de client raadpleegt om te bepalen of een aangeboden certificaat geldig is. |
| **CPG** | Common Provisioning Group |
| **C2RA** | Cloud and Clear Reference Architecture |
| **PICRA** | PNB Infrastructuur Cloud Referentie Architectuur |
| **CPU** | central processing unit |
| **DR/ Disaster Recovery** | Herstel van rampen, zoals het uitvallen van een volledig datacenter. |
| **DTO** | Detail Technisch Ontwerp ook wel Low Level Design (LLD) genoemd. |
| **LLD** | Low Level Design (LLD) ook wel genoemd Detail Technisch Ontwerp. |
| **DYA** | Dynamische Architectuur, architectuurframework/-methode ontwikkeld door Sogeti |
| **DNS** | Domain Name System |
| **NTP** | Network Time Protocol |
| **DHCP** | Dynamic Host Configuration Protocol |
| **GTO** | Globaal Technisch Ontwerp |
| **HA** | High Availability |
| **FTP** | File Transfer Protocol |
| **HLD** | High Level Design |
| **NTFS** | New Technology File System |
| **LLD** | Low Level Design |
| **LCM** | Life Cycle Management |
| **IaaS** | Infrastructure as a Service: alle diensten tot het operating system worden als dienst geleverd |
| **IR** | Implementatierichtlijn |

| | |
|---|---|
| **AR** | Architectuurrichtlijn |
| **SSL** | Secure Sockets Layer |
| **IDS/IPS** | Intrusion detectionsystemen / intrusion prevention system |
| **PKI** | public key infrastructure |
| **NPS/NAP** | Network Policy Server / Network Access Protection |
| **QoS** | Quality of Service |
| **OSI** | Open Systems Interconnect |
| **NFR** | Non-Functional Requirement |
| **NIST** | National Institute of Standards and Technology |
| **PID** | Project Initiation Document |
| **PKI** | Public Key Infrastructure: servers en diensten die tezamen zorgen voor uitrol, onderhoud en eventueel intrekken van beveiligingscertificaten |
| **PSA** | Project Start Architectuur, onderdeel werkwijze in DYA |
| **REF** | Referentie naar Brondocument |
| **REQ** | Requirement |
| **RFID** | Radio Frequency Identification |
| **RPO** | Restore Point Objective |
| **RTO** | Restore Time Objective |
| **SaaS** | Software as a Service: alle diensten t/m de applicatie worden als dienst geleverd |
| **SBC** | Service Based Computing |
| **SLA** | Service Level Agreements |
| **RBAC** | Role Based Access Control |
| **IAM** | Identity en Access Management |
| **IRF** | Intelligent Resilient Framework |
| **LDAP** | Lightweight Directory Access Protocol |
| **RADIUS** | Remote Authentication Dial In User Service |
| **WPA** | Wired Equivalent Privacy |
| **WiFi** | Wireless Fidelity |
| **SNMP** | Simple Network<br>Management Protocol |
| **DNS** | Dynamic Name Resolution |
| **VPN** | Virtual Private Network |
| **VLAN** | Virtual LAN |
| **SPOF** | Single Point of Failure |
| **VM** | Virtual Machines |
| **WAN** | Wide Area Network; het IT-netwerk tussen de verschillende panden of campussen |
| **LAN** | Local Area Network; het IT-netwerk binnen het pand of campus |



# 2 Introductie

Dit document beschrijft de PNB Architectuur Handboek PICRA.

Een High Level Design (HLD) beschrijft de oplossing tot een bepaald niveau. Het bepaalt keuzes gebaseerd op de eisen uit een Functioneel Ontwerp (FO), mits aanwezig, of Project Initiatie Document (PID). Op het HLD volgen Low Level Designs (LLDs) per laag uit de PICRA, daarna wordt per expertise gebied een onderdeel uitgewerkt in het LLD.

Het PNB Architectuur Handboek PICRA is vooral een functionele beschrijving. Publiek: management, projectmanagers, architecten en anderzijds engineers en consultants die technische ontwerpen moeten schrijven of de configuratie c.q. oplossing moeten beoordelen. Doel van het PNB Architectuur Handboek PICRA is om een globaal plaatje te maken waarbij de verhoudingen tussen de deelcomponenten behouden worden. Een Architect met het PNB Architectuur Handboek PICRA in de hand moet aan de slag kunnen om te komen tot een PSA of Solution/Doel Architectuur.

Het PNB Architectuur Handboek PICRA geeft richting en bepaalt de te gebruiken componenten.

## 2.1 Leeswijzer

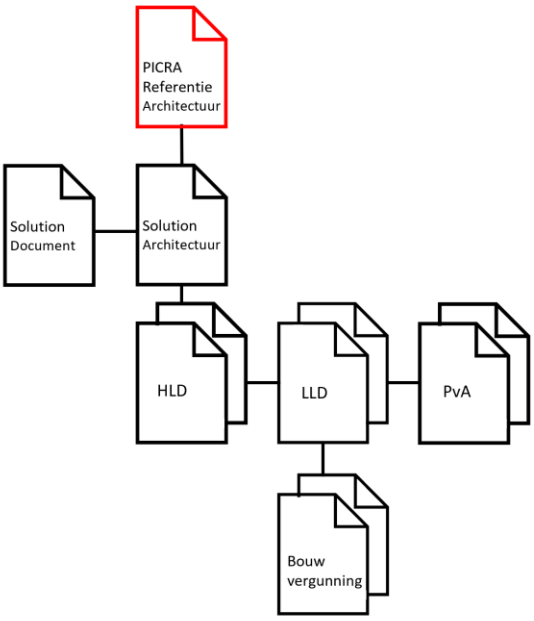
Dit document is de basis voor elk  design, dat een integraal onderdeel wordt van High Level Designs. Ieder hoofdstuk van het PNB Architectuur Handboek PICRA geeft een inzicht over de referentie architectuur en de rationale vanuit functionaliteit. Die door een LLD specifiek kan worden ingevuld. In het PNB Architectuur Handboek PICRA wordt een overzicht gegeven van alle hoofdstukken en de belangrijkste te behandelen onderwerpen per (sub)hoofdstuk.

De positie van de PICRA in de Enterprise Architectuur is door de Architectuur Board als volgt vastgesteld en in onderstaande figuur weergegeven.

Enterprise Architectuur PNB
referentie architectuur hiërarchie


De hiërarchie van de Architectuur artefacten is door Architectuur als volgt vastgesteld en in onderstaande figuur weergegeven.

Architectuur producten hiërarchie vanuit PICRA



## 2.2 Doel van het document

Het doel van dit document is het beschrijven van de PNB Infrastructuur Cloud Referentie Architectuur, die is gebaseerd op de (C2RA van Cloud and Clear IT Consultancy) t.b.v. de ontwikkeling en realisatie van het werken onder architectuur bij de Provincie Noord-Brabant.

Naast een functioneel document, zijn in dit PNB Architectuur Handboek PICRA ook zaken beschreven die verwacht mogen worden in een PSA of in een product-dienstencatalogus. Hiermee wordt bereikt dat in één document zowel doel, werkwijze als oplossing beschreven staat en dat het document dus voor meerdere doelgroepen relevant is.

Een Referentie Architectuur beschrijft de functionele oplossingsrichting, inclusief de architectuurrichtlijnen per bouwblok en zijn elementen.

Een HLD beschrijft – op basis van de PICRA - de globale technische oplossingsrichting, inclusief de architectuurrichtlijnen per technische oplossing/deelgebied. Daarom is dit PNB Architectuur Handboek PICRA een fundamenteel onderdeel wat zorgt voor de structuur voor een HLD een dus belangrijke brondocumenten voor de technische deelontwerpen (LLD). Naast de benoemde richtlijnen kunnen ook de architectuurbeslissingen die gaandeweg genomen zijn onderdeel zijn van een HLD. Omwille van het borgen van deze beslissingen zijn bepaalde elementen méér in detail beschreven dan andere.

In het HLD en in de deelontwerpen (LLD) waarbij PICRA als fundamenteel onderdeel, verzorgt een duidelijke relatie aanwezig tussen de gestelde requirements en de gerealiseerde oplossingen.

# 3 PNB Infrastructuur Cloud Referentie Architectuur (PICRA)

IT Infrastructuur wordt geïmplementeerd op basis van de PNB Architectuur Handboek PICRA. De PICRA is een gelaagd model die van onder naar boven wordt doorlopen in dit document.

De gelaagde vorm maakt het mogelijk om per laag een onderwerp af te bakenen. Elke volgende laag maakt gebruik van begrippen uit de onderliggende laag en dus in voorgaande teksten, wat tot een logische en gefundeerde opbouw leidt.

In de fase waarin low level designs (LLD) tot in detail worden uitgewerkt, wordt gebruik gemaakt van Bouwblokken om per onderdeel een low level design op te leveren.

Het PNB Architectuur Handboek PICRA bestaat uit de volgende lagen (layers) en bouwblokken (zie Figuur 1):

- Datacenter layer: Housing;
- Core Infra layer: Compute, Storage, Network;
- Supporting Infra layer: Backup, Security, Operations Management, etc.;
- Middleware layer, Dbases, Integration, etc.;
- Applications services: Collaboration, Business applications, etc.;
- Presentation services: Client-platform, Web-based, user experience, etc.;
- Compliance & Control layer: Confidentiality, Availability, Integrity, Scalability etc.;
- Governance & Management layer: Architecture, ITSM, Project Management, etc.

De Application en Presentation services bieden het merkbare en zichtbare: een desktop, applicaties, portals, e-mail, et cetera. Deze worden beheerd en bestuurd door de onderliggende “onzichtbare” infrastructuur, platform en datacenter services.

Over alle lagen heen zijn de security en managementservices ingericht, die onder meer de betrouwbaarheid en integriteit bieden, en daarnaast de gereedschappen en voorwaarden leveren om de SLA’s waar te maken.

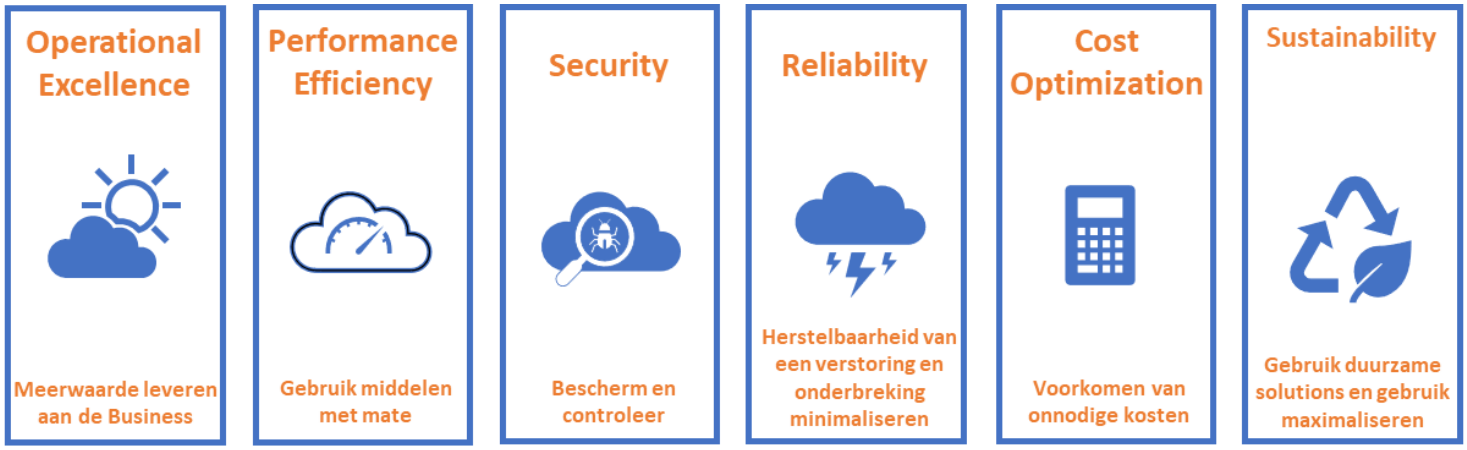
Met deze architectuur wordt voorzien in een volledig gelaagde, betrouwbare en veilige ICT-infrastructuur. Uitbreidingen op het gebied van applicatiediensten kunnen eenvoudig worden geïmplementeerd, omdat de onderliggende platformdiensten zorg dragen voor zaken als back-up, monitoring, patch management, et cetera.

PICRA heeft als uitgangspunt te werken met referentie architecturen van leveranciers om op basis hiervan de best bewezen oplossingen te implementeren. Hiermee worden onderstaande doelstellingen behaald:

- Snelheid, door sneller infrastructuur te bouwen en te implementeren
- Eenvoud, door de best practices als richtlijn te gebruiken voor het ontwerpen van oplossingen
- Efficiënt, door sneller time-to-value met een hoger ROI te creëren
- Optimalisatie, door uitvoerig geteste workload afstemming met applicaties en hypervisors

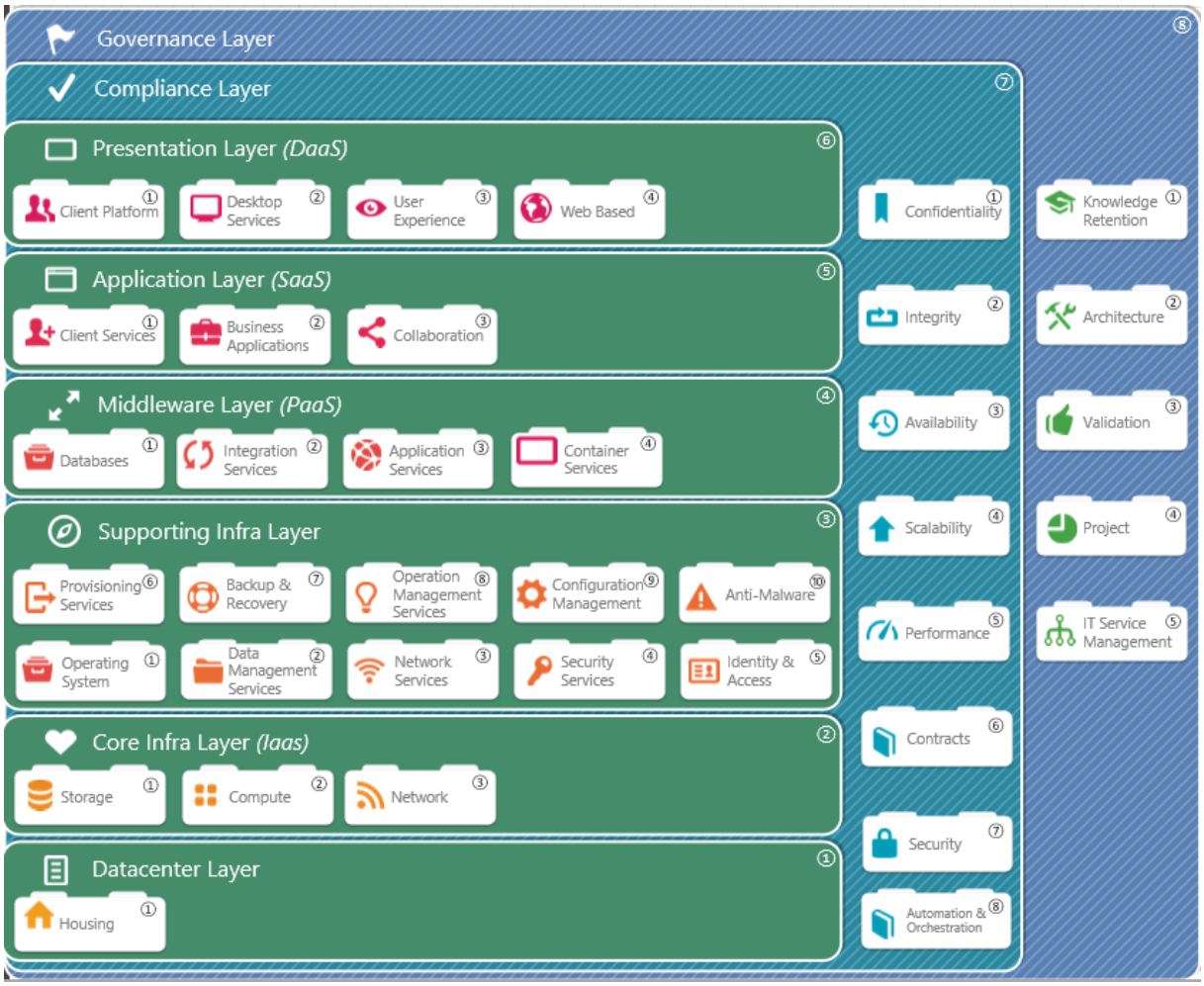
## 3.1 PICRA Framework pilaren

De onderstaande pijlers van PICRA Framework begeleiden en zijn richtinggevend bij het ontwerpen volgens PICRA van Cloud en Infrastructuur vanuit vijf verschillende perspectieven.



## 3.2 Architectuur principes

De PICRA Architectuur principes zijn onderdeel van de verzameling van PNB Architectuur principes, deze zijn samengebundeld in een separaat document genaamd PNB Architectuur principes.

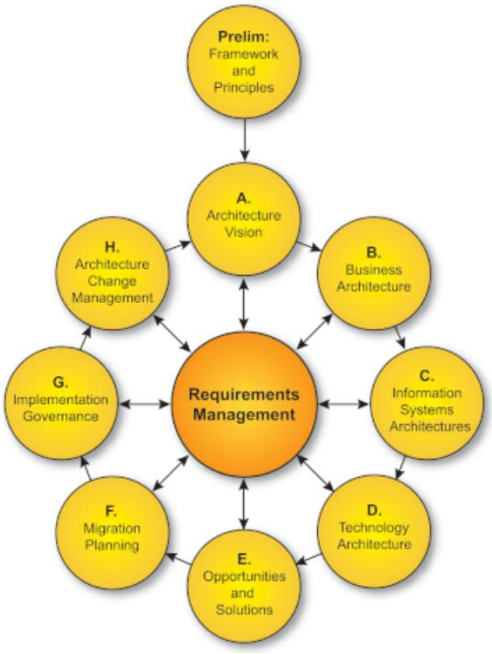



*Figuur 1 –PNB Infrastructuur Cloud Referentie Architectuur (PICRA)*

# 4 Architectuurmodel

## 4.1 TOGAF

Het TOGAF model (The Open Group Architecture Framework) wordt gehanteerd bij het ontwikkelen van de architectuur voor de PNB Architectuur Handboek PICRA. TOGAF is een methode voor het ontwikkelen en beheren van de Enterprise-architectuur. TOGAF is een open standaard. TOGAF bevat een verzameling aan technieken en best-practices. Centraal in de methode staat de Architecture Development Method (ADM). Deze beschrijft de verschillende fasen van ontwikkeling en beheer van de Enterprise-architectuur (zie Figuur 2)




*Figuur 2 - TOGAF ADM Cycle*

Van elk architectuur framework of model kan de gebruiker kiezen wat nuttig en van toepassing is. Het TOGAF Framework wordt op maat toegepast, hetgeen past en goed bruikbaar is voor de PNB Architectuur Handboek PICRA zal vanuit best practices op maat worden toegepast. Hiermee wordt verzanding voorkomen en een pragmatisch aanpak mogelijk wordt.

De belangrijke kenmerken van TOGAF die voor de architectuurontwikkeling van de PNB Architectuur Handboek PICRA omgeving gebruikt worden zijn:

1. Het aansluiten van de business architectuur (waaronder bijvoorbeeld het programma van eisen) op informatiesystemen architecturen en technology (Infrastructuur) architectuur
2. Governance of toezicht op het proces dat borgt dat gevraagde requirements vertaald worden in de ontwerpen en traceerbaar gerealiseerd worden gedurende de implementaties.
3. Het creëren van een repository, waarin de architectuurproducten en artefacten terug te vinden zijn.

## 4.2 Architectuur deliverables

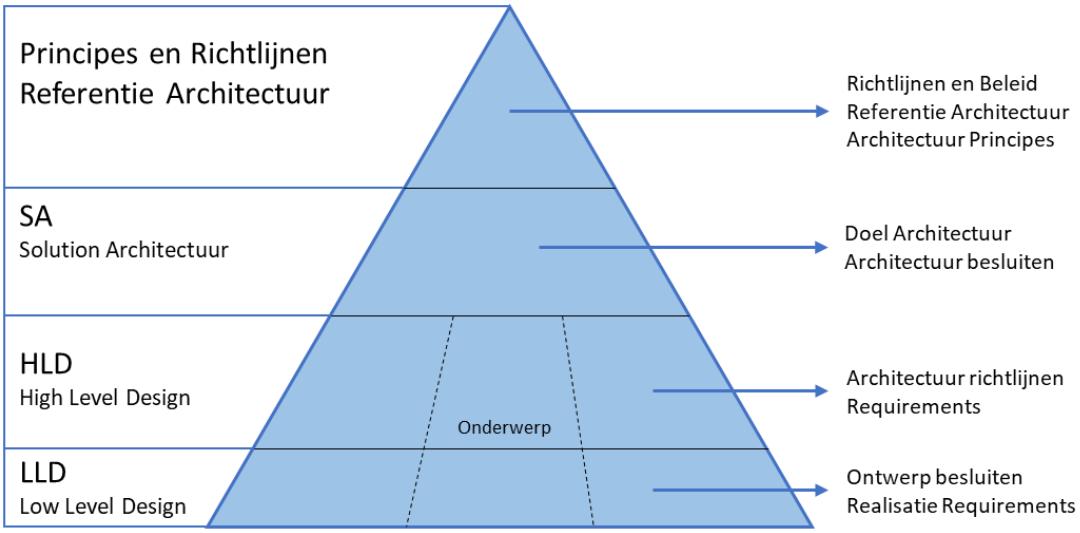
De onderstaande architectuurproducten zijn benodigd:

- Referentie-architectuur (zie Figuur 1)
- Architectuur Proces (zie § 4.5)
- Een Design process (zie § 4.5.1)
- Een High Level Design (HLD) template
- Een Architectuur Exception template

## 4.3 Architectuur vs. Design

Het volgende onderscheid tussen architectuur en ontwerp wordt gemaakt:

1. Architectuur beschrijft een probleem, de eisen en begrenzingen van de oplossing
   - Verander de architectuur: los een ander probleem op
2. Ontwerp beschrijft een oplossing binnen de grenzen van de architectuur
   - Verander het ontwerp: vind een andere oplossing voor hetzelfde probleem

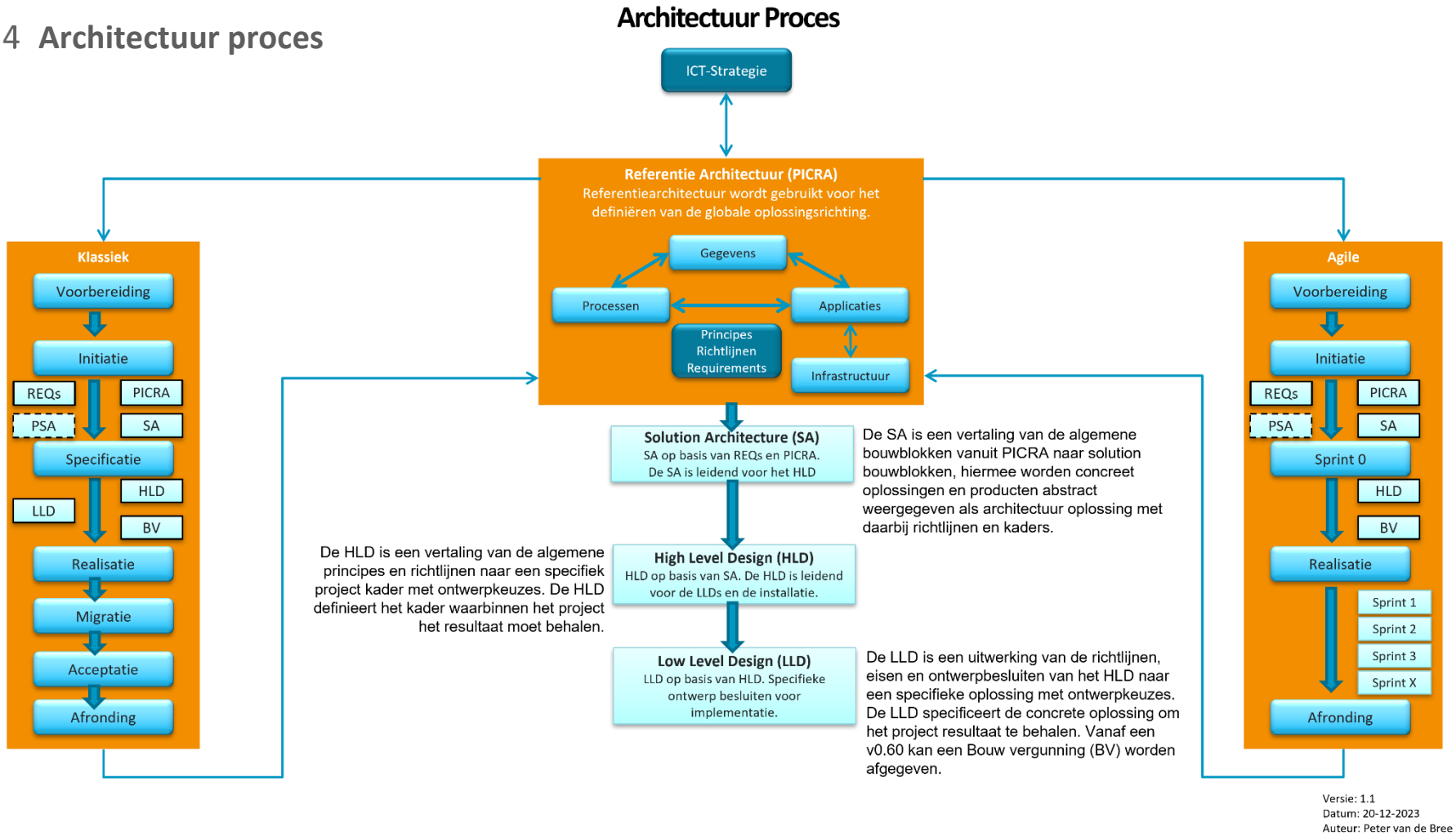



*Figuur 3 - Hiërarchische weergave van doelgericht ontwerpen*

Het HLD beschrijft de gewenste oplossingen voor de omgeving in termen van ontwerp besluiten en in te zetten bouwblokken. In het HLD worden architectuur richtlijnen genomen op hoofdlijnen. Vanuit Architectuur kan, in samenspraak met materiedeskundigen (SME), de oplossingsrichting worden voorgesteld of voorgeschreven. In dat geval zijn de richtlijnen in feite de facto implementatie standaarden.

De LLD's beschrijven de implementaties van de gebruikte bouwblokken. Zowel dit document, Referentie Architectuur en de Solution Architectuur vormen de belangrijkste bronnen voor een LLD.

## 4.4 Architectuur proces



Provincie Noord-Brabant

### 4.4.1 Design proces

Het ontwerpen start met een interpretatie van het HLD.

Helderheid wordt verkregen over de doelen, de eisen en de randvoorwaarden die aan de oplossing worden gesteld door de ontwerper en de projectmanager. Dit kan in een vergadering- of workshopvorm gebeuren.

Een optioneel advies van de ontwerper kan leiden tot een herformulering van de oplossingsrichting of een andere organisatie/timing van de implementatie.

Er is een LLD Technisch Ontwerpproces uitgewerkt wat gevolgd zal worden. Controle op correcte implementatie.

Vanuit architectuur kan er een controle worden uitgevoerd op het LLD om vast te stellen of de oplossing voldoet aan de gestelde kaders.

Vanuit de ontwerper zal een controle georganiseerd worden met als doel om na te gaan of de implementatie conform het design is uitgevoerd.

<design proces link verwijzing>

# 5 PNB Architectuur Handboek PICRA - Solution Architectuur

De bouwblokken uit de PICRA moeten volgens TOGAF opgevat worden als architectuur bouwblokken. Zij beschrijven in het algemeen de door de betreffende materialen en diensten geboden functionaliteit.

In de Solution/Doel architectuur zal volgens onderstaande legenda aangegeven welke architecturale bouwblokken voor het project/programma van toepassing zijn c.q. in scope van het ontwerp zitten.

In een Solution/Doel Architectuur wordt de referentiearchitectuur als model gevolgd, maar wordt t.a.v. de bouwblokken man en paard genoemd. Met andere woorden: in de Solution Architectuur worden in te zetten producten genoemd en/of solution-specifieke eisen, mogelijkheden en configuraties gesteld.

Om een analogie te gebruiken: de PICRA levert een doos met legosteentjes en de Solution/Doel Architectuur bouwt daarvan een constructie.

De Solution/Doel Architectuur - op basis van de PNB Architectuur Handboek PICRA - komt tot stand na overleg met Engineers en de IT Architecten evenals het raadplegen van de documentatie waarin de algemene constructie op hoofdlijnen werd vastgesteld. Hierin zijn de leidende technieken, principes en beslissingen opgenomen.

Een meer specifieke architectuur uitwerking per bouwblok is echter noodzakelijk, om tot solution-designs (LLD), installaties en configuraties te kunnen komen. Deze uitwerking, inclusief de bijbehorende ontwerprichtlijnen, volgen in de LLDs.

Legenda van de kleuren:

Provincie Noord-Brabant

## 5.1 Datacenter layer


*Figuur 4 - Datacenter Layer*

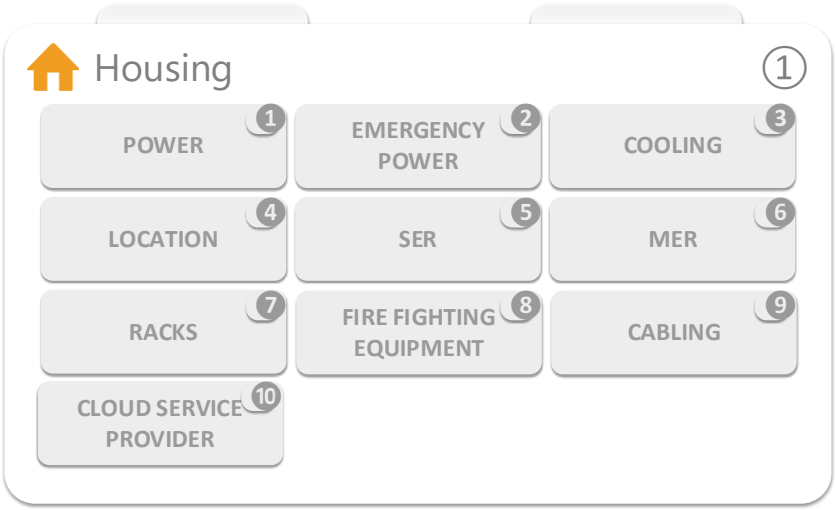
Deze laag (layer) beschrijft de aspecten die van belang zijn bij het huisvesten en aansluiten van de ICT-hardware.

Hierin staat een onderverdeling weergegeven van de *datacenter services*. Het gaat hier in essentie om de housing: de plaats waar de centrale apparatuur komt te staan. Het kan zowel om een bezemkast gaan als een tier-3 gecertificeerd professioneel datacenter.

Elementen die hier altijd terugkomen: de locatie moet over voldoende stroom beschikken voor de hardware en ook voor de koeling daarvan. Er dient een noodstroomvoorziening te zijn (aggregaat of tweede type aansluiting) en/of een 'batterij'-voorziening om een normale shutdown te kunnen draaien bij stroomuitval. Er dient berekend te worden hoeveel 'racks' er moeten te zijn en de daarmee af te nemen m2 vloerruimte. Er dient bepaald te worden wie wanneer toegang mag hebben tot het gebouw/ruimte. Het dient bekend te zijn welke brandblusmaatregelen er zijn getroffen en hoe de operator wordt gealarmeerd bij ongeregeldheden. Deze zijn deels ingegeven door het vraagstuk beschikbaarheid en continuïteit. Andere overwegingen vanuit informatiebeveiliging zijn: Waar staat het pand? Kan het onder water lopen? Zijn er aardbevingen? Is er uitwijk geregeld naar een ander pand? Hoeveel moeite gaat het kosten om deze locatie aan te sluiten op het bedrijfsnetwerk?

Belangrijke kenmerken die op dit niveau al spelen zijn de Recovery Point Objective (RPO) en de Recovery Time Objective (RTO) die respectievelijk informatie verschaffen over hoeveel tijd verstreken mag zijn sinds de laatste volledig herstelbare back-up (Systeem herstel, het punt in het verleden dan na uitval teruggehaald kan worden) en de tijd die het mag duren voordat relevante informatiesystemen voldoende hersteld zijn, zodat gebruikers ze weer kunnen gebruiken (gemeten na het ontstaan van de uitval tot het moment dat gebruikers weer kunnen werken). In beide begrippen zit behoorlijke diepgang die hier niet verder verkend wordt. De tendens is dat aan beide steeds hogere eisen gesteld worden en beide dus steeds korter worden, bijvoorbeeld RPO=4h en RTO=4h, en dit vraagt om passende maatregelen op datacenter niveau.

### 5.1.1 (ABB) Architectuur Bouwblok Housing



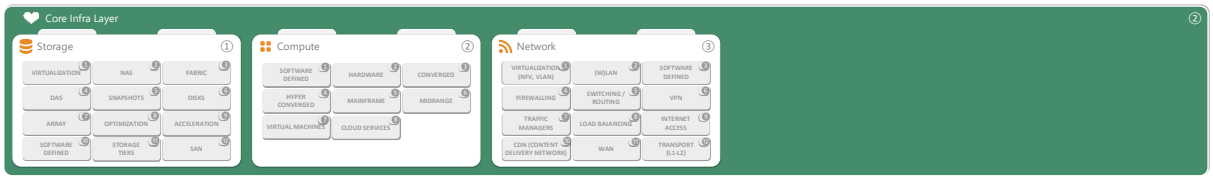

*Figuur 5 - Architectuur Bouwblok - Housing*

In onderstaand overzicht worden alle elementen met betrekking tot bouwblok Housing nader beschreven.

| Element | Beschrijving |
|---|---|
| 1. Power | Datacenters moeten te beschikken over voldoende stroom voorzieningen om alle benodigde apparatuur correct te kunnen aansluiten. |
| 2. Emergency Power | Om de fluctuaties en onderbreking van de netspanning op te vangen is een aansluiting op een UPS noodzakelijk. Wanneer de fysieke hardware ongecontroleerd uitgeschakeld wordt, kan er allerlei corruptie plaatsvinden waardoor de systemen niet meer normaal op starten. Bij langer durende stroom onderbreking wordt gebruik gemaakt van (diesel)generatoren. |
| 3. Cooling | Datacenters moeten te beschikken over koeling in de ruimtes zodat apparatuur niet oververhit zal raken en uitvallen. |
| 4. Location | De fysieke locatie(s) (datacenternaam, adres, zaalnummer etc.) waar de computersystemen zich bevinden en of deze is opgebouwd uit verschillende Availability Zones verspreid over twee of meer logische of fysieke datacenters. |
| 5. SER | Sateliet Equipment Room; oftewel een ruimte waarin vaak alle networkaansluitingen van werkplekken samenkomen en worden gekoppeld aan de back-end infrastructuur. |
| 6. MER | Main Equipment Room; oftewel een ruimte waarin de core-infrastructuur is geplaatst zoals servers, storage en netwerk voorzieningen. |
| 7. Racks | 19 Inch racks waarin o.a. servers en switches worden geïnstalleerd. |

| | |
|---|---|
| 8. Fire Fighting Equipment | Brand preventie voorziening, die voorkomt dat er grote schade ontstaat in geval van brand in een datacenter. |
| 9. Cabling | Aansluitingen en kabels om alle apparatuur met elkaar te verbinden. |
| 10. Cloud Service Provider | Een cloudserviceprovider is een extern bedrijf dat een platform, infrastructuur, toepassing of opslag in de cloud aanbiedt. Net zoals een huiseigenaar voor elektriciteit of gas betaalt, moeten bedrijven gewoonlijk betalen voor het aantal cloudservices dat ze gebruiken, naargelang de vraag.<br><br>Cloudserviceproviders laten alleen voor het gebruik betalen en bieden daarnaast talloze voordelen. Dankzij de voordelen van schaalbaarheid en flexibiliteit zijn bedrijven niet langer afhankelijk van de fysieke beperkingen van on-premises servers. Daarnaast kunnen ze vertrouwen op meerdere datacentra met een ruime mate van redundantie, kunnen servers naar eigen voorkeur worden aangepast en is sprake van responsieve taakverdeling waardoor eenvoudig op een veranderende vraag kan worden ingespeeld. Bedrijven dienen bij het opslaan van gegevens in de cloud echter de beveiliging te evalueren om ervoor te zorgen dat wordt voldaan aan door de branche aanbevolen beheerconfiguraties en -praktijken in verband met toegang en naleving |

## 5.2 Core Infra layer




*Figuur 6 - Core Infra Layer*

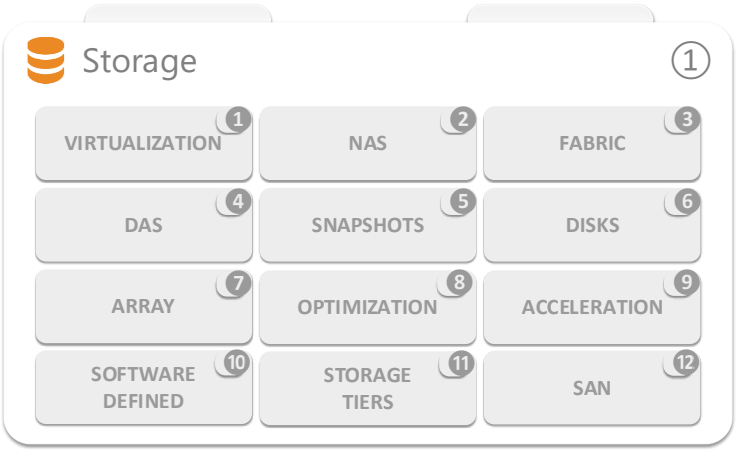
Deze laag beschrijft de Core Infra waarop de infrastructuur services draaien. Denk hierbij aan (gevirtualiseerde) servers, storage, netwerkcomponenten – tezamen ook wel Core Infra genoemd.

De Core Infra is gebaseerd op de voorzieningen in de Datacenter Services laag. Zoals het laat zien bevat deze laag de core infrastructuur componenten Servers, Storage en Network en in zekere abstracte vorm ook de End User Devices. Op de platform laag moeten dus hardware keuzes gemaakt worden, inclusief de kenmerken en keuzes op het gebied van virtuele hardware (server virtualisatie, netwerk virtualisatie, storage virtualisatie etc.)

Op deze laag worden tevens keuzes gemaakt ten aanzien van standaardisatie op fysieke en virtuele hardware en bijbehorende software zoals het server besturingssysteem, netwerkbesturingssysteem, fabrics etc. Het loont vaak de moeite om op deze laag al te standaardiseren op merk en type (hardware, firmware en software).

Ook hier spelen weer vragen vanuit beschikbaarheid: Hoe zorg ik ervoor dat mijn data beschikbaar is in een ander datacenter? Welke opslagvoorzieningen moeten getroffen worden? Welke performance is nodig voor mijn opslag (IOPS) en servers (snelheid van processoren)? Welke capaciteit is benodigd (aantal processoren/servers, hoeveelheid geheugen etc.) en welk aantal en type disks. Wat is de verwachtte toename in dataopslag? Welke bandbreedte heb ik nodig om aan te sluiten op het bedrijfsnetwerk en voor de replicatie van data naar een ander datacenter? Is clustering van servers noodzakelijk? Welke voorzieningen moeten worden getroffen om ongewenst netwerkverkeer buiten de deur te houden terwijl legitieme gebruikers en beheerders normaal kunnen werken? Worden de telefoonlijnen en –centrales geïntegreerd in het netwerk en werkplek (VOIP)? Van invloed is ook het vervanging/afschrijvingsbeleid, de bewaar- en archieftermijnen voor gegevens en andere beleidsregels. Met de antwoorden op deze en vele andere vragen wordt het WAN en LAN-plaatje gemaakt, de opslaginrichting bepaald en het serverplatform vorm gegeven.

### 5.2.1 (ABB) Architectuur Bouwblok Storage




*Figuur 7 - Architectuur Bouwblok Storage*

Het bouwblok Storage bevat alle componenten die benodigd zijn voor opslag van data binnen de datacenter locatie(s). Gebruik van de storage kan op diverse manieren plaatsvinden die allemaal hun eigen specifieke requirements kunnen hebben op bijvoorbeeld verwerkingssnelheid, fouttolerantie en kostprijs. Binnen de storage oplossing kunnen ook aanvullende diensten vallen voor onder andere optimalisatie, performance en acceleratie.

In onderstaand overzicht worden alle elementen met betrekking tot bouwblok Storage nader beschreven.

| Element | Beschrijving |
|---|---|
| 1. Virtualization | Beschrijving van de virtualisatie technieken/producten die zijn toegepast op de centraal aangeboden storage. Een oplossing om meer opslagcapaciteit te geven die gevraagd wordt, maar om alleen datgene op te slaan wat daadwerkelijk wordt gebruikt. Dit wordt thin provisioning genoemd. Het is een intelligente methode om het LUN-formaat al naar gelang de noodzaak daartoe op een dynamische wijze aan te passen |
| 2. NAS | Beschrijving van het type bekabeling, SAN switches en gebruikte protocol dat wordt gebruikt voor het koppelen en ontsluiten van storage via het netwerk. |
| 3. Fabric | Een San-fabric is de hardware die servers en werkstations verbindt met opslagapparaten in een SAN. Een San is geconfigureerd in een aantal zones. Deze zones omvatten hostzones, systeemzones en schijfzones. De SAN-fabric bestaat uit de apparaten die deze zones met elkaar verbinden, waardoor een verbindingsomgeving met elke opslag en elk apparaat mogelijk is. Dit omvat een aantal op Fibre Channel gebaseerde switches en routers die soms domeinen worden genoemd. Een SAN-fabric kan tweehonderdnegenendertig domeinen bevatten, uitgroeiend tot meer dan vijftien miljoen verbindingen binnen een enkele fabric. Het aantal apparaten binnen een SAN-fabric bepaalt welk niveau van SAN-topologie kan worden geïmplementeerd. Hoe complexer en veerkrachtiger een SAN-topologie is, hoe groter de SAN-fabric nodig heeft om deze te ondersteunen. |
| 4. DAS | Een DAS, wat ook wel staat voor Direct Attached Storaged, is een opslagmedium dat direct aangesloten is op een computersysteem. Een DAS beheert de gegevens als de computer niet aanstaat. Dit houdt in dat er aan de computer een extra opslagmogelijkheid wordt toegevoegd die bestanden en gegevens vasthoudt. |

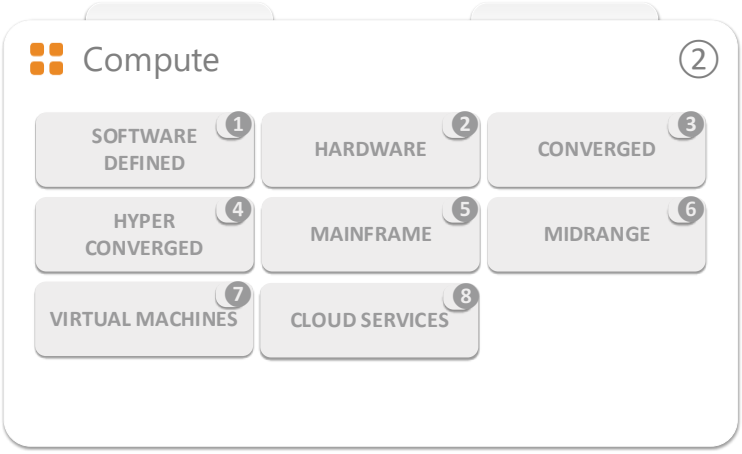
| | |
|---|---|
| 5. Snapshots | Een snapshot kopie is geen echte fysieke kopie, maar slechts een punt-in-de-tijdmarkering binnen de actuele en operationele dataset. Hierdoor neemt de kopie weinig extra ruimte in beslag. Dit maakt snapshot kopieën snel en ruimtebesparend. Snapshots zijn niet te gebruiken om vorige versies van individuele bestanden terug te zetten, omdat snapshot kopieën alleen ingesteld kunnen worden op het niveau van hele volume of 'aggregates'. Snapshots worden met vaste tussenpozen gemaakt, en zijn tevens ideaal bij het aanbrengen van risicovolle wijzigingen zoals updates van applicaties, databases en servers. |
| 6. Disks | Een disk zijn er in diverse vormen zoals SSD, SAS, NL-SAS, ML-SAS etc. Deze bepalen capaciteit en snelheid van de data dragers. Een bepalende factor in sizing en performance richtlijnen. |
| 7. Array | Een disk array wordt toegepast om beschikbaarheid, robuustheid en onderhoudbaarheid te realiseren. In de meeste gevallen zijn alle Single Points Of Failure geëlimineerd. Disk array componenten zijn hierdoor vaak hot-swappable. |
| 8. Optimization | Optimization is een generieke term voor technologieën voor het verhogen van de opslagcapaciteit van de storage. |
| 9. Acceleration | Het verhogen en verbeteren van de snelheid op de storage omgeving. |
| 10. Sofrtware Defined | Software Designed Storage (SDS) is een opslagarchitectuur die storagesoftware loskoppelt van de hardware, waardoor u een grotere schaalbaarheid, flexibiliteit en controle over uw data-opslaginfrastructuur krijgt. |
| 11. Storage tiers | Storage tiers is de toewijzing van verschillende gegevenscategorieën aan verschillende soorten opslagmedia om de totale opslagkosten te verlagen. Gebruikelijk bestaat een storage tier uit 3 lagen, te weten:<br><br>Tier 1 – Primary Storage<br>Missie-kritische, onlangs geopende of belangrijke bestanden. Worden opgeslagen op dure en hoge kwaliteit media zoals dubbel-pariteit RAIDs (redundant matrices of independent disks). Hierbij is sprake van disk to disk, d2 storage.<br><br>Tier 2- Secondary Storage<br>Tier 2 gegevens (zoals financiële, zelden gebruikte of vertrouwelijke bestanden) mogelijk op minder dure media in conventionele storage area networks (San's) opslag apparatuur. Hiervoor geldt disk to disk to tape, d2d2t storage.<br><br>Tier 3 - Archive<br>Tier 3 is minder frequent gebruikte of niet-geclassificeerde bestanden op tapes of beschrijfbare optische media al dan niet "worm" (write once read many) bevatten. Hiervoor worden meestal een tape library of een optical library gebruikt. |
| 12. SAN | Een Storage Area Network of SAN is een high-speed netwerk (of subnetwerk), dat verschillende soorten apparaten en data-opslag-servers met bijbehorende gegevens ten behoeve van een groter netwerk van gebruikers met elkaar verbindt. Een Storage Area Network is meestal geclusterd in de nabijheid van andere IT-middelen, maar kan ook uitgebreid worden naar afgelegen locaties voor back-up en archivering met behulp van Wide Area Network technologieën.<br><br>Een Storage Area Network kan gebruik maken van bestaande communicatietechnologieën, zoals optische vezelkabels of de nieuwere Fibre Channel-technologie. |





SAN ondersteunt disk mirroring, back-up en restore, archivering en het terughalen van gearchiveerde gegevens, datamigratie van het ene opslagapparaat naar het andere, en de uitwisseling van gegevens tussen verschillende servers in een netwerk.

### 5.2.2 (ABB) Architectuur Bouwblok Compute




*Figuur 8 - Architectuur Bouwblok Compute*

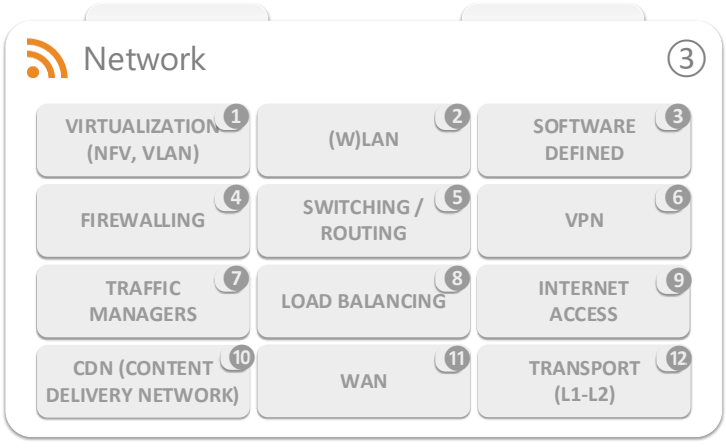
Het compute bouwblok omvat de 'intelligente' rekenkracht die binnen de infrastructuur wordt geboden. Dit wordt ingevuld door fysieke servers waarvan de belangrijkste componenten de rekenprocessoren (CPU's) en werkgeheugen (RAM-memory) zijn. De compute functionaliteit is er in diverse verschijningsvormen met o.a. software lagen voor management of aanvullende functionaliteit, integratie met andere infrastructuurcomponenten of voor hele specialistische toepassingen.

In onderstaand overzicht worden alle elementen met betrekking tot bouwblok Compute nader beschreven.

| Element | Beschrijving |
|---|---|
| 1. Software Defined | Virtualisatie is nodig om te komen tot een dynamisch datacenter. Virtualisatie is dan ook de basis van een dynamisch datacenter. Door deze virtualisatie technieken kun je flexibel omgaan met resources, neem je afhankelijkheden van bijvoorbeeld een fysieke server of een OS weg en kun je downtime tot een minimum beperken. De hypervisor is de virtualisatielaag tussen de application servers en de hardware. |
| 2. Hardware | Overzicht van de gebruikte Compute hardware, inclusief CPU processorsnelheid, en aantallen CPU's en cores per host |
| 3. Converged | Geconvergeerde infrastructuur, ook wel bekend als geconvergeerde architectuur, is een benadering van datacenterbeheer die compute-, netwerk-, servers-, opslag- en virtualisatietools verpakt op een vooraf gekwalificeerd kant-en-klaar apparaat. Geconvergeerde systemen bevatten een toolkit met beheersoftware. |

| | |
|---|---|
| 4. Hyper Converged | Hyperconverged infrastructuur is een softwaregedefinieerde IT-infrastructuur die alle elementen van conventionele "hardware-gedefinieerde" systemen virtualiseert. HCI omvat ten minste gevirtualiseerde computing, softwaregedefinieerde opslag en gevirtualiseerde netwerken. |
| 5. Mainframe | Een mainframe is een centrale computer. De gegevens werden oorspronkelijk in een mainframe ingevoerd met gegevensdragers als ponskaarten, ponsbanden en magneetbanden. In de jaren 70 werden op enige schaal terminals aan mainframes aangesloten, aanvankelijk schrijfmachineterminals en later ook beeldschermen |
| 6. Midrange | Midrange computers zijn computers die in kracht en capaciteit het midden houden tussen mainframes en personal computers. Nagenoeg alle grote bedrijven en instellingen werken met een of meer midrange computers, waarop de bedrijfssoftware draait. Tegenwoordig fungeren PC's als werkstation van deze midrange computers |
| 7. Virtual Machines | Vorm en type van virtuele machines die standaard worden gebruikt in de omgeving. |
| 8. Cloud Services | Welke type cloud services/diensten worden er geboden vanuit de omgeving. |

### 5.2.3 (ABB) Architectuur Bouwblok Network




*Figuur 9 - Architectuur Bouwblok Network*

Het core network bevat de verzameling van fysieke netwerkcomponenten, bekabeling, externe verbindingen (WAN/internet), configuraties e.d. die de basis vormen voor interconnectiviteit binnen het datacenter, en naar buiten toe. De componenten moeten ruim voldoende geschaald zijn om de benodigde bandbreedte te kunnen verwerken en vaak ook lage latency (vertraging) bieden, om informatie snel te kunnen verzenden. Juist het core network moet zeer robuust zijn, hierin mogen zich normaal gesproken geen SPOF's bevinden en middels configuraties zijn snelle failover mechanismen gebruikelijk. Vergeleken met het gebruikersnetwerk, dat zich op een hogere layer bevindt, is het core network relatief statisch.

In onderstaand overzicht worden alle elementen met betrekking tot bouwblok Network nader beschreven.

| Element | Beschrijving |
|---|---|
| 1. Virtualization (NFV, VLAN) | Virtualisatie van netwerkfuncties is een netwerkarchitectuurconcept dat gebruikmaakt van IT-virtualisatietechnologieën om hele klassen van netwerkknooppuntfuncties te virtualiseren tot bouwstenen die verbinding kunnen maken of aan elkaar kunnen worden gekoppeld om communicatiediensten te creëren en te leveren<br><br>Network Function Virtualization, of NFV, is een manier om de kosten te verlagen en de implementatie van services voor netwerkoperators te versnellen door functies zoals een firewall of codering los te koppelen van speciale hardware en deze naar virtuele servers te verplaatsen. |
| 2. (W)LAN | Draadloze netwerken zijn bijna overal aanwezig en er zijn veel fabrikanten die oplossingen leveren. Onderscheidend is het centraal beheer van grote draadloze netwerken en hoe flexibel met access points omgegaan kan worden. Voordat een gebruiker verbinding met het bedrade of draadloze (WiFi) network maakt moet hij zich authenticeren op het netwerk. Op grote draadloze netwerken met centrale authenticatie wordt hiervoor vaak de standaard WPA(2)-Enterprise. Deze authenticatie past het 802.1x protocol toe dat op zijn beurt weer gebruik maakt van een RADIUS service. De RADIUS service kent de directory services (bijv. Active Directory) zodat de gebruiker de credentials zoals deze in de directory service bekend zijn kan benutten. Het 802.1x protocol kan ook toegepast worden op bedrade netwerken zodat niet iedere gebruiker een apparaat kan koppelen op het bedrade netwerk waarna een verbinding tot stand gebracht kan worden. |
| 3. Software Defined | Softwaregedefinieerde netwerktechnologie is een benadering van netwerkbeheer die dynamische, programmatisch efficiënte netwerkconfiguratie mogelijk maakt om de netwerkprestaties en monitoring te verbeteren, waardoor het meer op cloud computing lijkt dan op traditioneel netwerkbeheer. |
| 4. Firewalling | Waar switching en routing functionaliteit gebaseerd is op het doorsturen van informatie (bij een switch ethernet frames, bij een router IP packets), is een firewall bedoeld om verkeer te analyseren of het is toegestaan. Firewalls nemen een dergelijke beslissing op basis van een aantal gegevens. In het geval van een traditionele firewall gebeurt dit op laag vier van het OSI-model. Op basis van bron IP-adres, bestemming IP-adres, TCP en UDP poort nummer wordt bepaald of het verkeer toegestaan is (permit) of niet (deny). In de nieuwe generatie firewalls (next-gen firewalls) wordt hier de gebruiker en de applicatie aan toegevoegd. Bijvoorbeeld MSN Messenger wordt toegestaan, maar file transfer via het MSN Messenger protocol wordt geblokkeerd. |
| 5. Switching / Routing | **Switching:** Het switch symbool wordt in alle trusted locaties gebruikt in het schema om een verbinding te maken met het apparaat of verbinding te maken met de WiFi-functionaliteit. De switch functionaliteit in het schema wordt in alle scenario's toegepast. De switch functionaliteit vindt plaats op laag twee van het OSI-model. Ethernet frames worden naar de juiste bestemming gestuurd op basis van het MAC-adres dat in een tabel van de switch staat (MAC-tabel). De switch ziet welk systeem, dus welk MAC-adres, achter een bepaalde poort aanwezig is en beperkt zo het zogenaamde collissiondomein. Frames komen alleen aan bij het systeem waar de frames voor bedoeld zijn en niet, zoals bij een hub, bij alle systemen binnen het collissiondomein. Binnen de switch functionaliteit zijn tal van technieken geïntroduceerd ten behoeve van snelheid, schaalbaarheid en redundantie. Belangrijkste voorbeeld hiervan is Spanning-Tree. Het spanning-tree protocol zorgt ervoor dat redundante verbindingen gelegd kunnen worden zonder dat een broadcast storm ontstaat doordat er een loop in het netwerk ontstaat. Hiervoor worden verbindingen dicht gezet (blocking) en op het moment dat een redundant pad nodig is wordt de verbinding open gezet (forwarding). Dit gebeurt op basis van een hiërarchie met een root switch en een backup root switch. Binnen spanning-tree zijn verschillende versies actief die het mogelijk maken verbindingen te load balancen per VLAN. Bijvoorbeeld, poort 24 is forwarding voor VLAN 1 en blocking voor VLAN 2 en poort 23 (de redundante verbinding) is blocking voor VLAN 1 en forwarding voor VLAN 2. Om alle poorten in forwarding mode te zetten is het nodig om logisch gezien |




| | |
|---|---|
| | geen loops in het netwerk te krijgen. Oplossing hiervoor is van verschillende fysieke switches één logische switch te maken die binnen de logische switch redundant is opgebouwd.<br>proprietary technieken om van verschillende fysieke switches één logische switch te maken zijn Stackwise en Virtual Switch System (VSS) van Cisco, Intelligent Resilient Framework (IRF) van HP Networking, Virtual Chassis van Juniper Networks en Knowledge Worker van Brocade (voorheen Foundry).<br><br>**Routing:** Verkeer wordt op laag drie van het OSI-model gerouteerd. Waarbij een switch gebruikt maakt van MAC–adressen, gebruikt een router IP-adressering. Op basis van het IP-adres wordt een packet naar de juiste bestemming gestuurd. Dit kan een systeem zijn binnen het subnet van een poort van de router (dan gaat het packet rechtstreeks naar zijn bestemming) of een systeem dat achter een volgende router te vinden is (dan wordt het packet naar de volgende router gestuurd die dan weer een beslissing neemt<br>waar het packet heen moet). De router gebruikt hiervoor een routering en forwarding tabel. In deze tabel zijn alle verbonden IP-subnetten weergegeven en kunnen routes naar andere IP-subnetten geplaatst worden die achter een andere router te vinden zijn. De beslissing wordt genomen op basis van best match: een route die het meest specifiek in de tabel staat voor een bepaald packet wordt gebruikt. Bekend voorbeeld hiervan is de default route met subnet adres 0.0.0.0 en als subnet masker 0.0.0.0 naar een volgende router. Al het verkeer dat niet gespecificeerd staat in de routing table wordt naar de volgende router gestuurd. Vaak is dit de internet router. Routing tables kunnen statisch gevuld worden maar ook dynamisch door gebruik te maken van een routing protocol. Voorbeelden hiervan zijn het Border Gateway Protocol (BGP), Open Shortest Path First (OSPF) en het Cisco proprietary Enhanced Interior Gateway Protocol (EIGRP). BGP wordt over het algemeen niet binnen lokale netwerken gebruikt, maar binnen het internet en WAN-oplossingen. |
| 6. VPN | Een Virtual Private Network, VPN) is een goede manier om een Local Area Network (LAN) over een bestaande verbinding, een Wide Area Network (WAN), zoals het internet, uit te bouwen met behoud van vertrouwelijkheid. De verzonden data wordt beveiligd zodat de integriteit, vertrouwelijkheid en authenticiteit van de data over dit onderliggende netwerk gewaarborgd blijven. |
| 7. Traffic Managers | Network Traffic Management maakt gebruik van netwerkbewakingstools en beheertechnieken zoals bandbreedtebewaking, diepe pakketinspectie en op toepassingen gebaseerde routering om een optimale netwerkwerking te garanderen. Daarbij helpt het de prestaties en beveiliging van bestaande netwerken te maximaliseren. |
| 8. Load Balacing | Een server kan maar een bepaald aantal gelijktijdige netwerkconnecties aan. Dit is afhankelijk van de kracht van de server en de service die gehanteerd wordt.<br>Ook is het vaak nodig om een server redundant uit te voeren terwijl hier geen clusteringtechniek voor toegepast kan worden door beperkingen en gedrag van deze techniek. Door een load balancer functionaliteit vóór deze server te plaatsen kan dit opgelost worden. De load balancer presenteert een virtual IP-adres in het netwerk welke opgenomen wordt in de DNS functionaliteit waarna de load balancer de sessies verdeeld over een aantal echte servers. De load balancer kan verschillende technieken aanwenden om te load balancen (OSI laag 3, laag 4 en laag 7). Sessies van apparaat A naar service X moeten tijdens de sessie wel bij dezelfde echte server aankomen, hiervoor wordt persistence toegepast. Bijvoorbeeld op basis van het client IP-adres wordt deze altijd naar dezelfde echte server doorverwezen. Dit kan ook door bijvoorbeeld een http cookie weg te schrijven op de client. De load balancer functionaliteit kan 'zien' of een echte server aanwezig is en of de benodigde service (bijvoorbeeld http) actief is. Op de server kan gebruik gemaakt worden van het Simple Network Management Protocol (SNMP), een TCP port check of een banner grab van bijvoorbeeld een http service, deze oplossingen zorgen ervoor dat de beschikbaarheid van de service gemonitored kan worden. |
| 9. Internet Access | Internettoegang verbindt apparatuur zoals een computer, smartphone of thuis- of bedrijfsnetwerk met het internet. Door middel van internettoegang hebben gebruikers toegang tot onder meer diensten als e-mail, webbrowsing en VoIP. Internettoegang is beschikbaar in verschillende technische uitvoeringen en snelheden. |



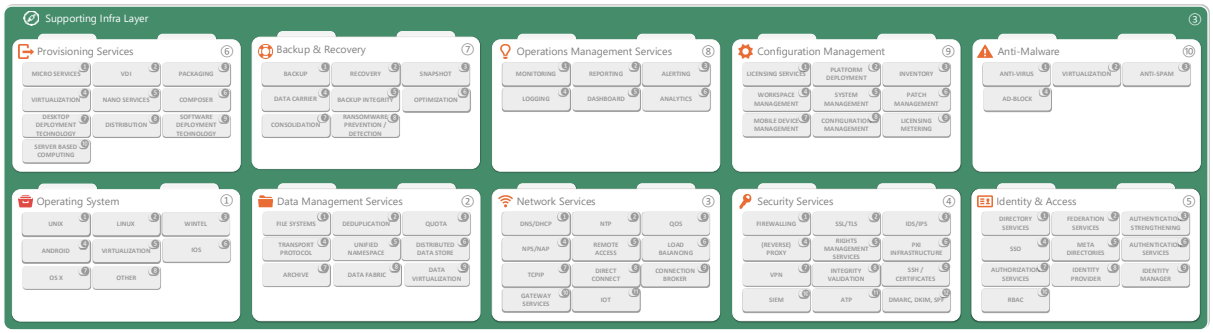


| | |
|---|---|
| 10. Content Delivery Network (CDN) | Een content delivery network is een netwerk van proxyservers die geografisch verspreid zijn over het internet in verschillende datacenters, zodat gebruikers snel en zonder vertraging content kunnen binnenhalen. Dit kan gaan om zowel teksten, documenten, figuren, media, mediastreams, scripten, als applicaties. |
| 11. WAN | Lokale netwerkverbindingen voor binnen een vestiging en Wide Area Networks. Een computernetwerk tussen vestigingen op verschillende locaties. |
| 12. Transport (L1 – L2) | De transportlaag is de vierde laag uit het OSI-model, dat zorgt voor het transport van data voor de applicaties. De meest gebruikte protocollen uit deze laag zijn het Transmission Control Protocol en het User Datagram Protocol, data-eenheden uit deze laag worden meestal segmenten genoemd. |





## 5.3 Supporting Infrastructuur diensten




*Figuur 10 – Supporting Infra layer*

Deze laag beschrijft welke infrastructuur services nodig zijn om de (middleware) applicaties gebruik te kunnen laten maken van de ICT-infrastructuur en de voorzieningen die nodig zijn om beheer uit te kunnen voeren.

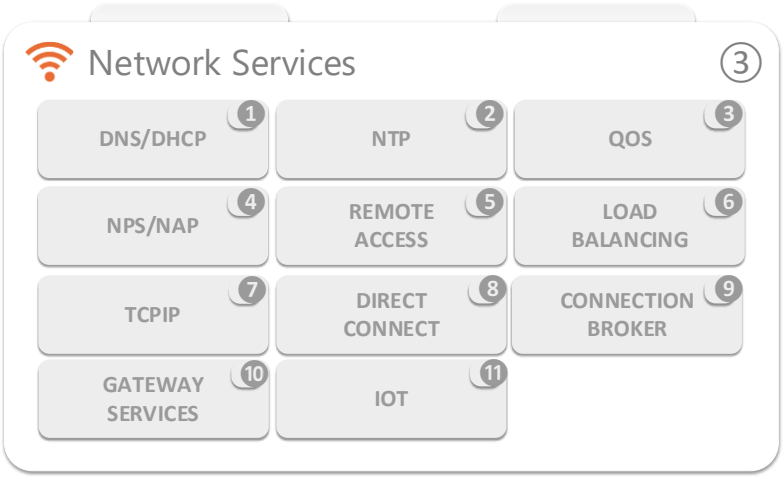
De Infrastructure Services bevat de services die gebaseerd zijn op de core infrastructuur componenten en bieden de mogelijkheden om deze te laten gebruiken door eindgebruikers en applicaties. Dit zijn ook de componenten waarmee operationeel beheer in de meest voorkomende omgevingen vaak op dagelijkse basis mee te maken heeft. De behandeling van deze laag beperkt zich hier tot enkele hoofdcomponenten.

Identity & Access management draait om het toepassen van een of andere vorm van Directory Services - waarin o.a. de gebruikersaccounts opgeslagen worden - en het integreren ervan met andere systemen. Voorbeelden hiervan zijn Microsoft Active Directory en Linux Realms, maar ook het uitvoeren van Role Based Access Control (RBAC). Anti-malware omvat onder andere voorzieningen voor integrale bestrijding van virussen en ongewenste e-mail op desktops, servers, firewalls, document managementsystemen en meer.

OS deployment services zijn ervoor om de geautomatiseerde installatie en inrichting van besturingssystemen op servers en desktops goed te laten verlopen. Daarnaast speelt Application Deployment, of tegenwoordig liever Application Delivery, een belangrijke rol om de gebruikers te laten beschikken over de door hen benodigde applicaties, afgestemd op het end user device van hun keuze. Hierin is applicatie-virtualisatie belangrijk, maar ook desktop-virtualisatie – het ontkoppelen van de visuele desktop van het onderliggende end user device – en de beschikbaarheid van webbrowser gebaseerde applicaties. Ook vinden we hier de hulpmiddelen voor Workspace management ten behoeve van een consistente gebruikerservaring, ongeacht het endpoint device, gekoppeld aan eenvoud van beheer. Direct gerelateerd aan OS deployment en Application Delivery zijn de Configuration Management Services waarmee een configuratie baseline ingericht en bewaakt kan worden op consistentie en afwijkingen en patches worden toegepast.

De integrale bewaking van ICT-componenten op alle lagen is een taak voor Monitoring services. Door al of niet visuele gezondheidsdiagrammen wordt inzichtelijk of de infrastructuur en applicaties naar behoren functioneert en presteert. Er worden in meer of mindere mate geautomatiseerde acties uitgevoerd bij afwijkingen of een event afgetrapt in het incident managementproces en gerapporteerd over het nakomen van Service Level Agreements (SLA). Met data protection & recovery services wordt de back-up en herstel acties op de core infrastructuur laag aangestuurd en de archivering van informatie geregeld. File & Print services zorgen ervoor dat gebruikers hun bestanden kunnen opslaan op de opslagruimte en documenten kunnen afdrukken. Remote Access services zorgen ervoor dat gebruikers ook buiten de kantoormuren gebruik kunnen maken van de geboden voorzieningen, bijvoorbeeld door middel van een veilige portal of gebruikersvriendelijke VPN-verbindingen. Met Licensing worden services ingericht die grenzen stelt aan het gebruik van software om in compliance te blijven met afgenomen licenties en/of rapporteert over gebruik van software. De network services tenslotte zorgen er onder andere voor dat netwerkadressen automatisch worden toegekend en dat computernamen in adressen worden vertaald. Hier horen ook de componenten thuis waarmee het netwerk (verkeer) verder geoptimaliseerd wordt, de zogenaamde traffic managers en - shapers.

### 5.3.1 (ABB) Architectuur Bouwblok Network Services




*Figuur 11 - Architectuur Bouwblok Network Services*

In onderstaand overzicht worden alle elementen met betrekking tot bouwblok Network Services nader beschreven.

| Element | Beschrijving |
|---|---|
| 1. DNS/DHCP | Het Domain Name System (DNS) is het systeem en netwerkprotocol dat op het Internet gebruikt wordt om namen van computers naar numerieke adressen (IP-adressen) te vertalen en omgekeerd. Hoewel dit "vertalen" genoemd wordt gaat het gewoon om opzoeken in tabellen, waarin namen aan nummers gekoppeld zijn.<br><br>Een methodiek voor het automatisch configureren van de netwerkinstellingen van een PC. De DHCP server deelt bijvoorbeeld IP-adressen uit voor het TCP-IP interface van een PC die DHCP ondersteund. |
| 2. NTP | Het Network Time Protocol (NTP) is een protocol waarmee computers die onderling met elkaar in verbinding staan, hun interne klok kunnen synchroniseren met andere computers. |
| 3. QoS | Quality of Service (of QoS) is een algemene term die wordt gebruikt om uit te drukken wat de specifieke eisen zijn voor een bepaalde dienst. Dit kan gaan van snelheid tot de overdracht van computerbestanden. |
| 4. NPS/NAP | Gebruikers met laptops en smartphones hebben een WiFi-verbinding nodig; gebruikers met een desktop een vaste verbinding met de switch. Op alle laptops en desktops is end-point security functionaliteit toegepast. Deze functionaliteit wordt technisch als Network Access Control (NAC) of Network Access Protection (NAP) aangeduid. Naast end-point security wordt door middel van 802.1x authenticatie bepaald of de gebruiker met zijn of haar credentials verbinding mag maken met het netwerk (zowel wireless als wired). Een firewall en een IDP/IDS functionaliteit is geplaatst tussen het gebruikers netwerk en het datacenter netwerk om het security risico verder te verkleinen. |
| 5. Remote Access | Een Remote Access oplossing geeft de mogelijkheid om op afstand andere computers c.q. systemen in te loggen vanaf bijvoorbeeld één beheerserver en deze te beheren. |
| 6. Load Balacing | Een server kan maar een bepaald aantal gelijktijdige netwerk connecties aan. Dit is afhankelijk van de kracht van de server en de service die gehanteerd wordt. Ook is het vaak nodig om een server redundant uit te voeren terwijl hier geen |

| | |
|---|---|
| | clusteringtechniek voor toegepast kan worden door beperkingen en gedrag van deze techniek. Door load balancer functionaliteit vóór deze server te plaatsen kan dit opgelost worden. De load balancer presenteert een virtual IP-adres in het netwerk welke opgenomen wordt in de DNS functionaliteit waarna de load balancer de sessies verdeeld over een aantal echte servers. De load balancer kan verschillende technieken aanwenden om te load balancen (OSI laag 3, laag 4 en laag 7). Sessies van apparaat A naar service X moeten tijdens de sessie wel bij dezelfde echte server aankomen, hiervoor wordt persistence toegepast. Bijvoorbeeld op basis van het client IP-adres wordt deze altijd naar dezelfde echte server doorverwezen. Dit kan ook door bijvoorbeeld een http cookie weg te schrijven op de client. De load balancer functionaliteit kan 'zien' of een echte server aanwezig is en of de benodigde service (bijvoorbeeld http) actief is. Op de server kan gebruik gemaakt worden van het Simple Network Management Protocol (SNMP), een TCP port check of een banner grab van bijvoorbeeld een http service, deze oplossingen zorgen ervoor dat de beschikbaarheid van de service gemonitored kan worden. |
| 7. TCP/IP | TCP/IP is een verzamelnaam voor een reeks netwerkprotocollen die gebruikt worden voor het grootste deel van de netwerkcommunicatie tussen computers. |
| 8. Direct Connect | cloud direct connect is een verbinding tussen een privaat netwerk en een publieke cloud. In het verleden gingen alle verbindingen met de cloud van een openbaar netwerk naar een openbare cloud, maar met de opkomst van nieuwe technologieën zijn er verschillende soorten clouds beschikbaar gekomen, waaronder public, private en hybride. |
| 9. Connection Broker | De connection broker bepaalt welke 'Server hosted remote' desktop aan de client ter beschikking wordt gesteld. Hierbij is het mogelijk bij gebruik van een Server hosted Virtuele Desktop Infrastructuur dedicated of een pool van remote desktops beschikbaar te stellen. Het automatisch aanmaken, verwijderen, of pauzeren van remote desktops is een functionaliteit waarin een desktop broker voorziet. Er zijn verschillende leveranciers van connection brokers. Citrix met XenDektop, Microsoft met Remote Desktop Services en VMware met View zijn de meest bekende totaaloplossingen. Afhankelijk van leverancier kan de connection broker additionele functies hebben, zoals een webinterface die veilige (SSL) en eenvoudige toegang tot de remote desktops verzorgt, maar ook Directory Services integratie, Full USB support, ondersteuning van verschillende display protocollen en integratie met Terminal Services. Afhankelijk van regels is het mogelijk om applicaties centraal op een Server hosted VDI of op een Terminal Server uit te voeren. |
| 10. Gateway Services | Een gateway is een netwerkknooppunt die twee netwerken met verschillende protocollen aan elkaar verbindt. Terwijl een brug wordt gebruikt om twee vergelijkbare typen netwerken te verbinden, wordt een gateway gebruikt om twee ongelijke netwerken samen te voegen.<br>De meest gebruikelijke gateway is een router die een thuis- of bedrijfsnetwerk met internet verbindt. In de meeste op IP gebaseerde netwerken, is het enige verkeer dat niet door minstens één gateway loopt, verkeer dat tussen knooppunten op hetzelfde LAN-segment (local area network) stroomt, bijvoorbeeld computers die op dezelfde switch zijn aangesloten.<br>Gateways kunnen verschillende vormen aannemen en verschillende taken uitvoeren |
| 11. IoT | Het internet der dingen is het geheel aan apparaten die via internetverbindingen met andere apparaten of systemen in contact staan en daarmee gegevens uitwisselen. |





### 5.3.2 (ABB) Architectuur Bouwblok Security Services


*Figuur 12 - Architectuur Bouwblok Security Services*

In onderstaand overzicht worden alle elementen met betrekking tot bouwblok Security Services nader beschreven.

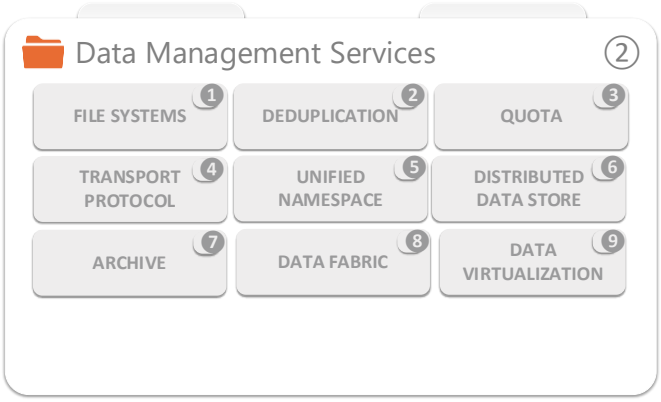
| Element | Beschrijving |
|---|---|
| 1. Firewalling | Een firewall is een systeem dat de middelen van een netwerk of computer kan beschermen tegen misbruik van buitenaf. |
| 2. SSL/TLS | SSL staat voor Secure Sockets Layer, wat ervoor zorgt dat verbindingen met het internet versleuteld worden. SSL brengt een versleutelde verbinding tot stand tussen gebruiker en het internet. |
| 3. IDS/IPS | Intrusion detectionsystemen (IDS) detecteren de typische handelingen van digitale inbrekers of inbraken, en slaan vervolgens alarm. Flink wat gecamoufleerde inbraakpogingen ontsnappen immers aan de aandacht van andere beveiligingssystemen zoals antivirus of firewall.<br>Een intrusion prevention system, kortweg IPS, gaat anders te werk: het onderschept een bedreiging nog voor ze het netwerk kan bereiken en werkt op die manier veel proactiever. In tegenstelling tot een IDS gaat het onmiddellijk over tot actie. |
| 4. (Reverse) Proxy | een reverse proxy de applicatie die zich voor back-end-applicaties bevindt en clientverzoeken naar die applicaties doorstuurt. Reverse proxy's helpen de schaalbaarheid, prestaties, veerkracht en beveiliging te vergroten. |
| 5. Rights Management Services | Right Management Services is een Enterprise digital rights management system van Microsoft. RMS werkt alleen met programma's die het ondersteunen zoals Microsoft office. Het grote verschil met een standaard E-DRM systeem is dat de rechten rechtstreeks via een publicatielicentie aan het document verbonden zijn. |
| 6. PKI Infrastructure | Een public key infrastructure (PKI) is een systeem waarmee uitgiften en beheer van digitale certificaten kan worden gerealiseerd.<br>Door de toepassing van een deugdelijke PKI is het mogelijk dat een certificaat dat door een certificaatautoriteit (CA) wordt beheerd. De CA waarborgt de integriteit en authenticiteit van het certificaat en staat dus in voor de identiteit van de certificaatbezitter. |

| | |
|---|---|
| 7. VPN | Om via een onbeheerde en onveilige verbinding zoals het internet connectie te maken met het datacenter is een encrypted sessie nodig. Door een Virtual Private Network (VPN) te gebruiken wordt dit gerealiseerd. Er wordt een encrypted authenticatie gedaan waarna al het verkeer van de client naar het datacenter encrypted is. Voorheen werd een client gebruikt welke een VPN-verbinding maakt met de firewall (IPSEC VPN). Hiermee wordt een netwerkverbinding gemaakt op laag drie waarna de firewall zo nodig verkeer kan toestaan of weigeren. Bij een SSL VPN wordt de authenticatie en het verkeer versleuteld door middel van een SSL certificaat dat op een appliance staat (of op een gecombineerd apparaat zoals een firewall). Aan de gebruiker wordt een portal gepresenteerd met daarop de applicaties en resources welke voor de gebruiker relevant zijn. Er kan hier op basis van gebruiker bepaald worden waar de gebruiker bij kan komen. Indien nodig kan ook met een SSL VPN oplossing een netwerkverbinding opgezet worden. |
| 8. Integrity Validation | Data (Integriteit) Validatie is het proces van het analyseren van een dataset om bepaalde aspecten van datakwaliteit vast te stellen en te beslissen over mogelijke herstelstappen. |
| 9. SSH/Certificates | SSH-certificaten worden gebouwd met openbare sleutels en bieden niets extra's vanuit het oogpunt van cryptografie-engineering. Een certificeringsinstantie (CA) is een vertrouwde partij die zijn eigen openbare en privésleutelpaar heeft. SSH CA-sleutels worden gebruikt om gebruikers- en host-SSH-certificaten te ondertekenen. |
| 10. SIEM | Beveiligingsinformatie en gebeurtenisbeheer is een gebied op het gebied van computerbeveiliging, waar softwareproducten en -services beheer van beveiligingsinformatie en beheer van beveiligingsgebeurtenissen combineren. |
| 11. ATP | Advanced Threat Protection (ATP) is een reeks analysetools die is ontworpen om te beschermen tegen geavanceerde bedreigingen die bekende en onbekende aanvalsvectoren gebruiken. ATP vormt een aanvulling op meer gebruikelijke beveiligingsoplossingen die zijn gericht op het afweren van bekende intrusion strategieën. |
| 12. DMARC, DKIM, SPF | SPF DKIM en DMARC zijn eenvoudigweg een reeks e-mailverificatiemethoden om aan ISP's en e-mailservices te bewijzen dat afzenders echt geautoriseerd zijn om e-mail te verzenden vanaf een bepaald domein en zijn een manier om te verifiëren dat uw e-mailverzendserver e-mails verzendt via uw domein. |





### 5.3.3 (ABB) Architectuur Bouwblok Data Management Services



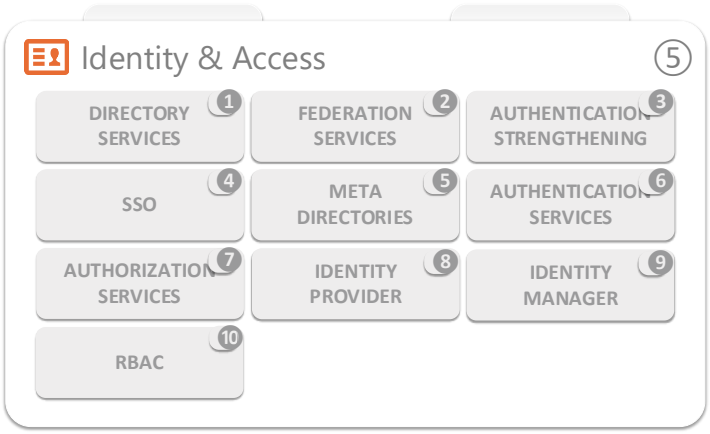

*Figuur 13 - Architectuur Bouwblok Data Management Services*

In onderstaand overzicht worden alle elementen met betrekking tot bouwblok Data Management Services nader beschreven.

| Element | Beschrijving |
|---|---|
| 1. File systems | Een bestandssysteem is een door het besturingssysteem verzorgde, softwarematige indeling van een opslagmedium (zoals een harde schijf). Het besturingssysteem (bijvoorbeeld van de computer of smartphone) gebruikt deze indeling om toegang tot een opslagmedium te verzorgen voor applicaties en zijn eigen gebruik, zodat data in de vorm van bestanden op het opslagmedium weggeschreven kan worden en ook weer teruggelezen.<br><br>Sommige bestandssystemen kunnen door meerdere besturingssystemen gebruikt worden, terwijl andere alleen in bepaalde (spel)computers gebruikt worden. Er zijn meer dan 100 verschillende bestandssystemen. FAT32, NTFS en ext4 zijn vaak gebruikte bestandssystemen. Mac OS X gebruikt HFS+. |
| 2. Deduplication | gegevensdeduplicatie is een techniek om dubbele kopieën van herhalende gegevens te elimineren. |
| 3. Quota | Instellen van een harde limiet op basis van capaciteit. |
| 4. Transport protocol | File Transfer Protocol (FTP) is een protocol dat uitwisseling van bestanden tussen computers vergemakkelijkt. Het standaardiseert een aantal handelingen die tussen besturingssystemen vaak verschillen.<br><br>Een FTP-client (zoals FileZilla) start een verbinding met een FTP-server standaard via TCP-poort 21. |
| 5. Unified Namepace | Een uniforme naamruimte is een softwareoplossing die fungeert als een gecentraliseerde opslagplaats van gegevens, informatie en context waar elke toepassing of elk apparaat gegevens kan gebruiken of publiceren die nodig zijn voor een specifieke actie. |
| 6. Distributed Datastore | Een Distributed Data Store is een computernetwerk waarbij informatie wordt opgeslagen op meer dan één server (knooppunt), vaak op een gerepliceerde manier. Het wordt meestal specifiek gebruikt om te verwijzen naar een gedistribueerde database waarin gebruikers informatie op een aantal servers (knooppunten) opslaan. |

| | |
|---|---|
| 7. Archive | Een digitaal archiefsysteem (ook wel E-depot, elektronisch depot van digitaal depot) is een systeem voor het elektronische verwerken en beheren van statistische documenten. Het gaat om alle soorten en formaten van elektronische documenten: gescande papieren documenten, kantoor-documenten, zoals tekstverwerking, rekenschema's, presentaties, etc., foto's, tekeningen, multimedia, kortom alles wat als een digitaal object opgeslagen kan worden. Dit systeem is inherent virtueel, en bestaat uit hardware en software, voor de duurzame bewaring en beschikbaarheid van onveranderlijke digitale informatie, zowel digitaal geboren als gedigitaliseerd. Het gaat hier niet alleen om geheugenruimte maar om het samenspel van speciaal voor archiefbeheer ontwikkelde software en speciaal voor archiefopslag ontwikkelde hardware. |
| 8. Data Fabric | Een datafabric is een architectuurbenadering om de toegang tot gegevens in een organisatie te vereenvoudigen en selfservice-gegevensverbruik te vergemakkelijken. Deze architectuur is agnostisch voor data-omgevingen, processen, hulpprogramma's en geografie, en integreert end-to-end mogelijkheden voor databeheer. |
| 9. Data virtualization | Datavirtualisatie is een benadering van databeheer waarmee een toepassing gegevens kan ophalen en manipuleren zonder technische details over de gegevens te vereisen, zoals hoe ze bij de bron zijn opgemaakt of waar ze fysiek zijn gelokaliseerd, en die een enkel klantbeeld van de algemene gegevens. |

### 5.3.4 (ABB) Architectuur Bouwblok Identity & Access Services




*Figuur 14 - Architectuur Bouwblok Identity & Access Services*

In onderstaand overzicht worden alle elementen met betrekking tot bouwblok Identity & Access Services nader beschreven.

| Element | Beschrijving |
|---|---|
| 1. Directory Services | Een directoryservice is een dienst (één of meerdere toepassingen) die het mogelijk maakt om toegang te krijgen tot hiërarchisch georganiseerde gegevens die eventueel verspreid zijn opgeslagen in een computernetwerk. De directoryservice beheert de gegevens en de relatie tussen gegevensbronnen. Toegang tot gegevens geschiedt volgens het client-serverprincipe. |

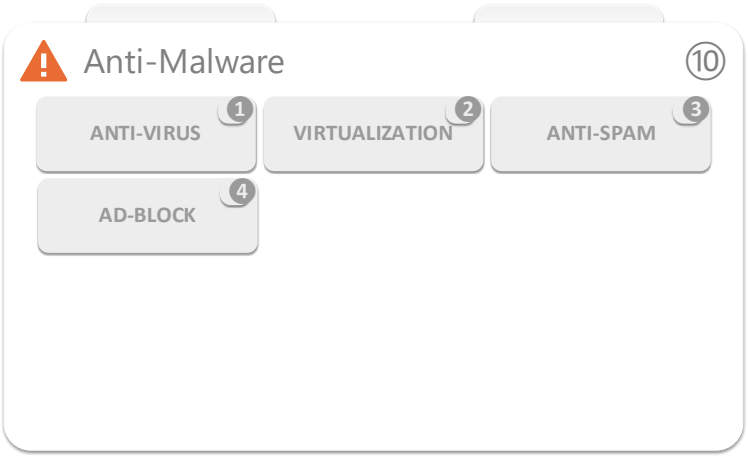
| | |
|---|---|
| 2. Federation Services | Active Directory Federation Services (AD FS), een softwarecomponent dat is ontwikkeld door Microsoft, kan op Windows Server-besturingssystemen worden uitgevoerd om gebruikers met eenmalige aanmelding toegang te verlenen tot systemen en toepassingen die zich over de grenzen van de organisatie bevinden. Het maakt gebruik van een op claims gebaseerd autorisatie-model voor toegangscontrole om de applicatiebeveiliging te behouden en om federatieve identiteit te implementeren. Op claims gebaseerde authenticatie houdt in dat een gebruiker wordt geverifieerd op basis van een reeks claims over de identiteit van die gebruiker in een vertrouwd token. Een dergelijk token wordt vaak uitgegeven en ondertekend door een entiteit die in staat is om de gebruiker op andere manieren te authenticeren, en die wordt vertrouwd door de entiteit die de op claims gebaseerde authenticatie uitvoert. Het maakt deel uit van de Active Directory Services.<br><br>In AD FS wordt identiteitsfederatie tussen twee organisaties tot stand gebracht door vertrouwen te vestigen tussen twee beveiligingsdomeinen. Een federatieserver aan de ene kant (de accountkant) authenticeert de gebruiker via de standaardmiddelen in Active Directory Domain Services en geeft vervolgens een token uit dat een reeks claims over de gebruiker bevat, inclusief de identiteit ervan. Aan de andere kant, de Resources-kant, valideert een andere federatieserver het token en geeft een ander token uit voor de lokale servers om de geclaimde identiteit te accepteren. Hierdoor kan een systeem gecontroleerde toegang tot zijn bronnen of services bieden aan een gebruiker die tot een ander beveiligingsrealm behoort zonder dat de gebruiker zich rechtstreeks bij het systeem hoeft te verifiëren en zonder dat de twee systemen een database met gebruikersidentiteiten of wachtwoorden delen. |
| 3. Authentication strengthening | Om de betrouwbaarheid van de authenticatie te vergroten, wordt authenticatie afgedwongen door toepassing van multifactor authenticatie. Daarbij worden minimaal twee van de bovenstaande authenticatievormen gelijktijdig toegepast. Te denken valt aan het gebruik van een token met een PINcode. Een aanvaller dient nu niet alleen het kenniskenmerk te kraken, maar ook het token te bezitten. Een Eenmalig wachtwoord wordt veel gebruikt door internetdiensten als manier om naast een wachtwoord een tweede factor toe te voegen. |
| 4. SSO | Single sign-on (SSO) is een authenticatieproces waarmee een gebruiker toegang heeft tot meerdere applicaties met één set inloggegevens. SSO is een gangbare procedure, waar een client toegang heeft tot meerdere bronnen. SSO verbetert de bruikbaarheid door het verminderen van wachtwoordmoeheid. Het biedt ook een betere beveiliging door het potentiële aanvalsoppervlak te verkleinen. |
| 5. Meta Directories | Een metadirectorysysteem zorgt voor de gegevensstroom tussen een of meer directoryservices en databases, om de synchronisatie van die gegevens te behouden, en is een belangrijk onderdeel van identiteitsbeheersystemen. De gegevens die worden gesynchroniseerd, zijn doorgaans verzamelingen vermeldingen die gebruikersprofielen en mogelijk authenticatie- of beleidsinformatie bevatten. De meeste metadirectory-implementaties synchroniseren gegevens naar ten minste één op LDAP gebaseerde directoryserver, om ervoor te zorgen dat op LDAP gebaseerde toepassingen zoals eenmalige aanmelding en portalservers toegang hebben tot recente gegevens, zelfs als de gegevens worden beheerd in een niet-LDAP-gegevensbron .<br><br>Metadirectory-producten ondersteunen het filteren en transformeren van gegevens in transit. |
| 6. Authentication Services | Authenticatie is het proces waarbij iemand nagaat of een gebruiker, een andere computer of applicatie daadwerkelijk is wie hij beweert te zijn. Bij de authenticatie wordt gecontroleerd of een opgegeven bewijs van identiteit overeenkomt met echtheidskenmerken, bijvoorbeeld een in het systeem geregistreerd bewijs. Er zijn verschillende vormen van authenticatie die eventueel gecombineerd kunnen worden om een hoger of lager niveau van beveiliging op te leveren. Daarbij zijn drie vormen van bewijs bruikbaar: iets wat je weet (kennis), iets wat je hebt (bezit) of iets wat je bent (persoonlijke eigenschap). |
| 7. Authorization services | Autorisatie is het verlenen van een geverifieerde (authenticatie) partijmachtiging om iets te doen. Hiermee geeft u op welke gegevens u toegang hebt en wat u met die gegevens kunt doen. Autorisatie |





| | |
|---|---|
| | wordt soms ingekort tot AuthZ. Het Microsoft Identity Platform maakt gebruik van het OAuth 2.0-protocol voor het afhandelen van autorisatie. |
| 8. Identity Provider | Een identiteitsprovider (afgekort als IdP) is een systeementiteit die identiteitsinformatie voor opdrachtgevers maakt, onderhoudt en beheert, terwijl hij verificatieservices levert aan afhankelijke partijtoepassingen binnen een federatie of gedistribueerd netwerk.<br>Een identiteitsprovider biedt gebruikersauthenticatie als een service. Vertrouwende partijtoepassingen, zoals webtoepassingen, besteden de stap van de gebruikersauthenticatie uit aan een vertrouwde identiteitsprovider. Een dergelijke afhankelijke partijtoepassing zou federatief zijn, dat wil zeggen dat het federatieve identiteit verbruikt.<br>Een identiteitsprovider is "een vertrouwde provider waarmee u single sign-on (SSO) kunt gebruiken om toegang te krijgen tot andere websites." |
| 9. Identity Manager | Identity en Access Management (IAM of IdM) is een overkoepelende term voor het ontwikkelen en beheersen van gebruikers en middelen in het netwerk met de toegangscontrole van de applicaties en systemen. |
| 10. RBAC | Role-based access control is een methode waarmee op een effectieve en efficiënte wijze toegangscontrole voor informatiesystemen kan worden ingericht. |

## 5.3.5 (ABB) Architectuur Bouwblok Anti-Malware Services



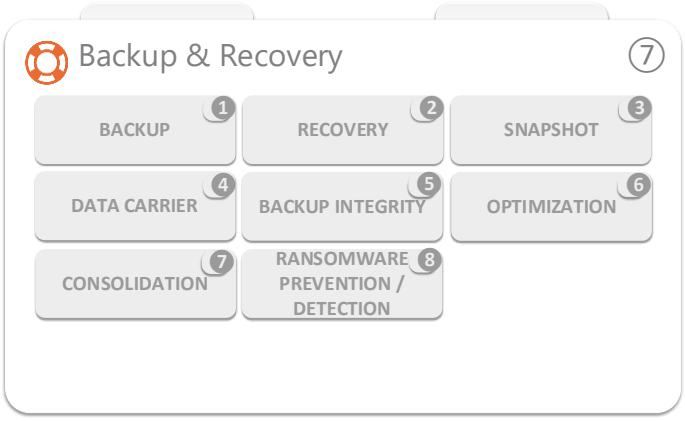

*Figuur 15 - Architectuur Bouwblok Anti-Malware Services*

In onderstaand overzicht worden alle elementen met betrekking tot bouwblok Anti-Malware Services nader beschreven.

| Element | Beschrijving |
|---|---|
| 1. Anti-Virus | Antivirussoftware is programmatuur die probeert om computervirussen te identificeren, tegen te houden en te verwijderen. Antivirussoftware gebruikt daarvoor twee verschillende technieken: |

| | |
|---|---|
| | • Onderzoeken (scannen) van bestanden om te zoeken naar virussen die overeenkomen met de definities uit een lijst van bekende virussen.<br>• Identificeren van verdacht gedrag door eender welk computerprogramma, wat op een besmetting kan wijzen.<br><br>De meeste antivirusprogramma's gebruiken beide technieken, met de nadruk op de eerste aanpak. Er zijn ook programma's beschikbaar die enkel de eerste techniek gebruiken. |
| 2. Virtualization | Gevirtualiseerde anti-malware oplossing is een "agentless" antivirus-/beveiligingsplatform die heeft een andere benadering voor het bieden van beveiliging in een gevirtualiseerde omgeving. In plaats van een kopie van de beveiligingssoftware op elke VM binnen het besturingssysteem te installeren, is een afzonderlijke virtuele appliance bestemd voor het uitvoeren van beveiligingssoftware.<br><br>Verschillende agentloze oplossingen kunnen verschillende methoden gebruiken om het doel van het handhaven van de beveiliging voor de gevirtualiseerde hostomgeving te bereiken |
| 3. Anti-Spam | Een spamfilter is een stuk software dat spam en computervirussen te snel te herkennen en te verwijderen uit een set e-mails. Normaal gezien detecteert een spamfilter de e-mail in, besluit het of er sprake is van spam en onderneemt het op basis daarvan actie.<br><br>Spam wordt ook wel 'ongevraagde bulk e-mail' (UBE) genoemd: ongevraagde (ongevraagde) e-mail die in grote hoeveelheden (bulk) wordt verstuurd. Het criterium voor de omgang met 'spam' te spreken. |
| 4. AD-Block | Blokkeert webpagina's die malware bevatten, stopt in-browser cryptojackers (ongewenste cryptovaluta-mijnwerkers) en laat andere kwaadaardige inhoud opstarten. |

## 5.3.6 (ABB) Architectuur Bouwblok Backup & Recovery




*Figuur 16 - Architectuur Bouwblok Backup & Recovery*

In onderstaand overzicht worden alle elementen met betrekking tot bouwblok Backup & Recovery nader beschreven.

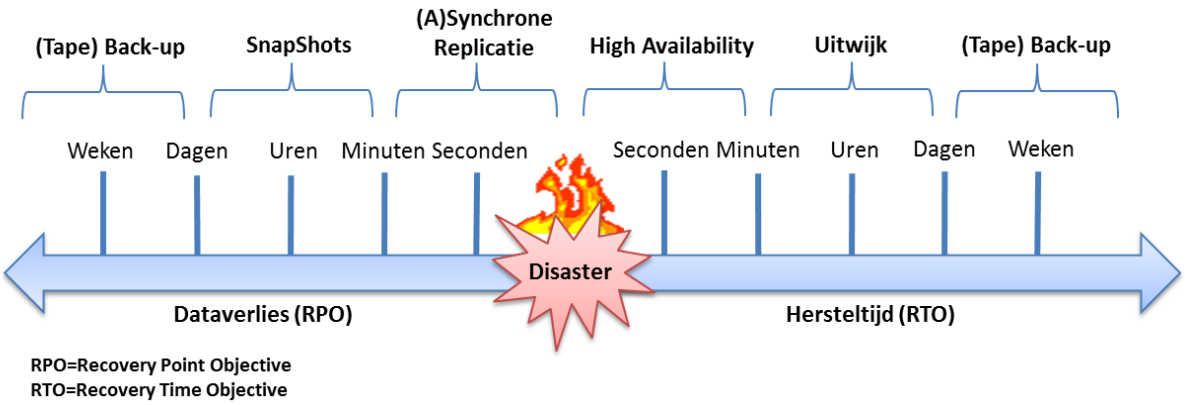
| Element | Beschrijving |
|---|---|
| 1. Backup | Back-up en Recovery verwijst naar het proces van back-up van gegevens in geval van verlies en het opzetten van systemen die gegevensherstel mogelijk maken als gevolg van gegevensverlies. Het maken van back-ups van gegevens vereist het kopiëren en archiveren van computergegevens, zodat deze toegankelijk zijn in het geval van verwijdering van gegevens of corruptie. Gegevens uit een eerdere tijd kunnen alleen worden hersteld als er een back-up van is gemaakt.<br><br>Gegevensback-up is een vorm van disaster recovery en moet deel uitmaken van elk DR plan. |
| 2. Recovery | Onlosmakend verbonden met Backup, waarbij het kunnen herstellen van een backup een belangrijk onderdeel is van het doel om te komen tot terughalen van data. Het herstellen c.q. een recovery kunnen doen, zou ook regelmatig getest moeten worden, dat inderdaad de backup hersteld kan worden. |
| 3. Snapshot | Een snapshot is een reeks van referentiemarkeringen van data op een bepaald tijdstip. Een snapshot werkt als een gedetailleerde inhoudsopgave en biedt de gebruiker toegankelijke kopieën van gegevens waarnaar ze kunnen teruggaan c.q. herstellen. |
| 4. Data Carrier | Een opslag voorziening, zoals een optische schijf, USB-flashstation of een Disk, dat wordt gebruikt om gegevens te transporteren. |
| 5. Backup integrity | De back-upintegriteitscontrole zorgt voor een goede werking van back-uptaken en de consistentie tussen de back-upgegevens en bronbestanden tot het volledige herstel van back-upgegevens |
| 6. Optimization | Backup opmimalisatie biedt mechanismen voor datacompressie en deduplicatie. Met gegevenscompressie en deduplicatie wordt het verkeer dat over het netwerk gaat en schijfruimte die nodig is voor het opslaan van back-up bestanden en VM-replica's verlaagd. |
| 7. Consoldation | Middels consolidatie reduceren we het aantal backup oplossingen die nodig zijn. |
| 8. Ransomware prevention / detection | Beveiligings voorzieningen om de backup veilig te houden tegen ransomware. Een voorbeeld hiervan is Write once read many (WORM) beschrijft een gegevensopslagapparaat waarin informatie, eenmaal geschreven, niet kan worden gewijzigd. Deze schrijfbeveiliging biedt de zekerheid dat er niet met de gegevens kan worden geknoeid zodra ze naar het apparaat zijn geschreven. |

**Backup**

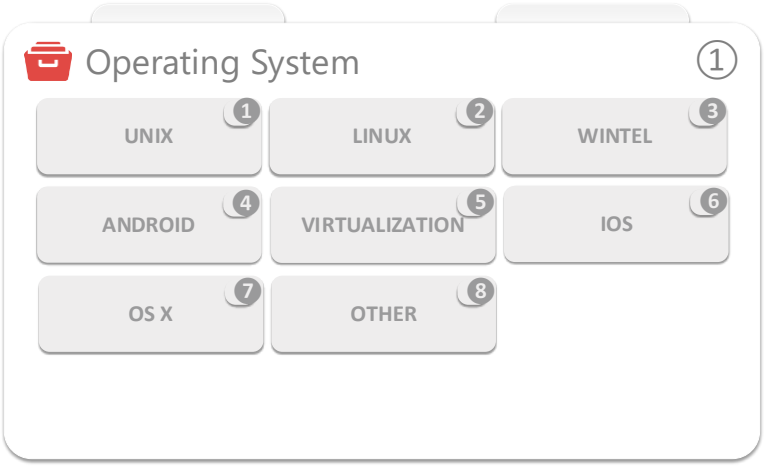
Met een traditionele back-up van slechts één maal per dag bestaat de kans dat er 24 uur dataverlies (RPO) optreed (mits de back-up succesvol was verlopen). Het herstellen van een traditionele back-up kost circa twee keer de tijd van het maken van een back-up. Als het huidige back-up window (tijd die het kost om een back-up te maken) circa acht (8) uur bedraagt, zal de hersteltijd (RTO) circa 16 uur bedragen.

Hierbij is nog geen rekening gehouden met eventuele tijd die nodig is om een defect systeem te herstellen. In een gunstig geval is een defect systeem door middel van een onderhoudscontract of reserveonderdelen binnen acht (8) uur hersteld. De hersteltijd van een defect systeem (acht (8) uur) plus de hersteltijd van het terugzetten van de back-up (16 uur) maken samen de hersteltijd (RTO) van de dienst, welke in dit voorbeeld 24 uur bedraagt.

Om betere bescherming te bieden tegen dit realistische voorbeeld zijn diverse maatregelen mogelijk. Onderstaande afbeelding geeft een voorbeeld aan van tegenmaatregelen die genomen kunnen worden om het dataverlies (RPO) en hersteltijd (RTO) aanzienlijk te reduceren.




## 5.3.7 (ABB) Architectuur Bouwblok Operating System



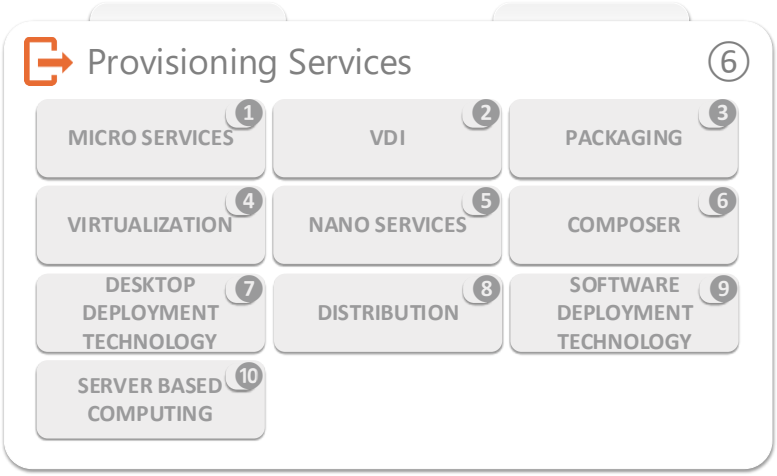

*Figuur 17 - Architectuur Bouwblok Operating System*

In onderstaand overzicht worden alle elementen met betrekking tot bouwblok Operating System nader beschreven.

| Element | Beschrijving |
|---|---|
| 1. Unix | Unix besturingssysteem |
| 2. Linux | Linux is een open-source-, Unix-achtig besturingssysteem gebaseerd op de Linuxkernel. |
| 3. Wintel | Microsoft Windows het meest gebruikte operating systeem voor servers. |

| | |
|---|---|
| 4. Android | Android besturingssysteem |
| 5. Virtualization | Het stelt gebruikers in staat om VM's rechtstreeks op een enkele Windows- of Linux-desktop of laptop te maken en uit te voeren. Die VM's draaien gelijktijdig met de fysieke machine. Elke VM heeft zijn eigen besturingssysteem, zoals Windows of Linux. VMware Workstation is een voorbeeld hiervan. |
| 6. iOS | iOS besturingssysteem |
| 7. OS X | OS X besturingssysteem |
| 8. Other | Een ander besturingssysteem |

### 5.3.8 (ABB) Architectuur Bouwblok Provisoning Services




*Figuur 18 - Architectuur Bouwblok Provisoning Services*

In onderstaand overzicht worden alle elementen met betrekking tot bouwblok Provisoning Services nader beschreven.

| Element | Beschrijving |
|---|---|
| 1. Micro Services | Een microservice-architectuur - een variant van de structuurstijl van de servicegerichte architectuur - ordent een applicatie als een verzameling losjes gekoppelde services. In een microservices-architectuur zijn services fijnkorrelig en zijn de protocollen lichtgewicht. |
| 2. VDI | Desktopvirtualisatie is een softwaretechnologie die de desktopomgeving en de bijbehorende applicatiesoftware scheidt van het fysieke clientapparaat dat wordt gebruikt om er toegang toe te krijgen. |

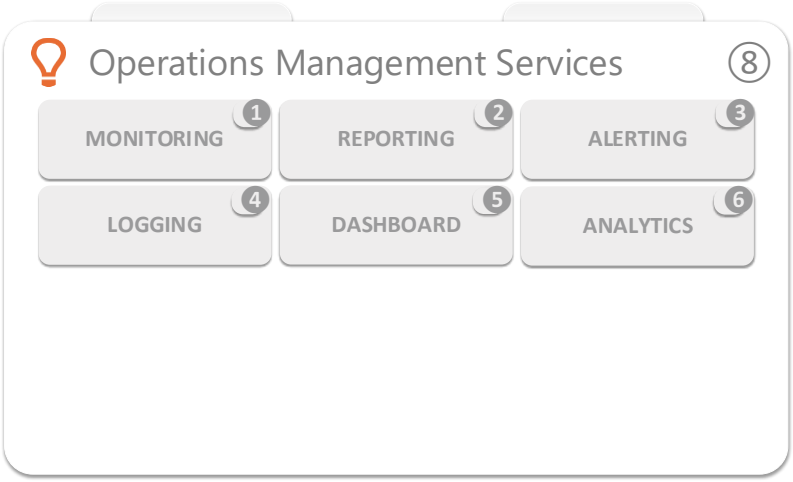
| | |
|---|---|
| 3. Packaging | Packaging of re-packaging van applicaties, ook wel software packaging genoemd, is het aanpassen of converteren van de installer van bestaande applicaties zodat deze geschikt wordt voor software distributie. Het is een specialisme dat ontstaan is vanuit de behoefte om applicaties automatisch te kunnen installeren. Van oorsprong werd dit gerealiseerd door het maken van scripts die, bijvoorbeeld, vanuit het aanmeld script uitgevoerd werden. |
| 4. Virtualization | Met behulp van Applicatie streaming en Virtualisatie kunnen Microsoft Windows applicaties gebruikt worden zonder dat er iets aan het lokale besturingssysteem wordt gewijzigd, laat staan dat er applicatiesoftware op een werkplek wordt geïnstalleerd. Met andere woorden: de applicatie wordt uitgevoerd, slaat gegevens op en print alsof het lokaal aanwezig is, zonder enige aanpassing van de lokale client. Resources zoals CPU, geheugen, harddisk en netwerkkaart zorgen voor de uitvoering van deze applicaties. Applicatie Streaming en Virtualisatie verzorgen het beschikbaar stellen van applicaties aan desktop, laptop, Server hosted VDI en Terminal Services platformen. De applicatie wordt uitgevoerd op het 'client' platform zonder dat er aanpassingen aan het platform gemaakt wordt. Een aantal voordelen voor Applicatie Virtualisatie zijn: installatie, upgrade, roll-back en het gemak van ondersteuning van applicaties (beheer). Installatie van applicaties is hiermee veleden tijd; conflicten zijn niet meer mogelijk. Het creëert een dynamische application delivery infrastructuur. |
| 5. Nano Services | Nanoservices zijn ontworpen om een enkele functie uit te voeren, waarvan de uitvoer wordt weergegeven via een specifiek API-eindpunt (opdracht). Nanoservices zijn onderling volledig vindbaar. Elk kan worden gekoppeld aan andere services om extra acties uit te voeren en functionaliteit uit te breiden. Door hun ontwerp zijn nanoservices: Op zichzelf staand. |
| 6. Composer | Composer is een functie die beheerders de mogelijkheid biedt om pools van desktops te beheren die een gemeenschappelijke virtuele schijf delen. Een beheerder kan de master-image bijwerken, waarna alle desktops die gekoppelde klonen van die master-image gebruiken ook kunnen worden gepatcht. |
| 7. Desktop Deployment Technology | Desktop Deployment Technology is een oplossing voor het makkelijk uitrollen van Microsoft besturingssystemen en configuratie middels Microsoft deployment toolkit (MDT) op verschillende type hardware en tevens de implementatie van toepassingen afhankelijk van profielen.<br><br>De meeste organisaties zullen een scala aan software beschikbaar hebben. Dit kan onder meer uit het besturingssysteem, hardware drivers, software patches of updates, en natuurlijk, toepassingen bestaan. Met MDT, kunt u al deze onderdelen toevoegen aan de collectie van beschikbare software - of distributiepakketten.<br><br>De netwerk, USB, ISO of DVD uitrol van image en applicaties kan volledig of semi automatisch (Zero Touch Installation / Lite Touch Installation) ingeregeld worden waarbij afhankelijk van bijvoorbeeld de situatie (schone installatie of her uitrol van een bestaande pc) het type hardware (laptop, desktop, server, bitness etc.), locatie of gekozen profiel de verschillende, drivers, naconfiguratie of applicaties geinstalleerd worden. |
| 8. Distribution | De verzameling van functionaliteiten en hulpmiddelen die ervoor zorgen dat nieuwe software geautomatiseerd, snel en uniform kan worden geïnstalleerd.<br><br>Het distribueren van applicaties middels een centrale voorziening. |
| 9. Software Deployment Techmology | De verzameling van functionaliteiten en hulpmiddelen die ervoor zorgen OS en software updates vlot en betrouwbaar worden gedistribueerd. |
| 10. Server Based Computing | Server Based Computing, ook wel aangeduid als RDS = 'Shared Remote Desktop'. SBC is een oplossing voor remote toegang tot desktops en applicaties die op een SBC in het datacenter worden uitgevoerd waarbij elke gebruiker zijn eigen unieke SBC sessie heeft. Toegang tot de desktop of applicatie is niet gebonden aan een locatie of eindgebruikerapparaat en programma-uitvoering vinden centraal plaats |





op de SBC Server. De informatie verschijnt op het clientscherm via een remote display protocol zoals Microsoft RDS of Citrix ICA. SBC bestaan uit verschillende infrastructuurcomponenten voor beheer, load balancing, sessiecontrole en ondersteuning. Enkele voordelen van SBC zijn het snel en veilig beschikbaar stellen van applicaties, lage TCO, locatie en werkplek onafhankelijke applicatie toegang.

### 5.3.9 (ABB) Architectuur Bouwblok Operations Management Services



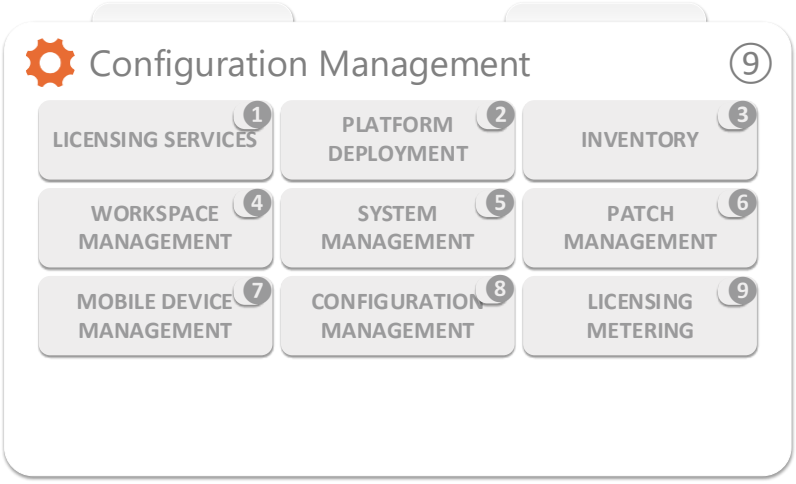

*Figuur 19 - Architectuur Bouwblok Operations Management Services*

In onderstaand overzicht worden alle elementen met betrekking tot bouwblok Operations Management Services nader beschreven.

| Element | Beschrijving |
|---|---|
| 1. Monitoring | Monitoring is het geheel van applicaties dat wordt gebruikt voor het 'in de gaten houden' van o.a. de gezondheid, beschikbaarheid en belasting van infrastructuur componenten en ketens. Middels geautomatiseerde processen in specialistische software worden periodiek de beschikbaarheid en waarden van verschillende parameters van infrastructuur componenten gecontroleerd en geregistreerd. |
| 2. Reporting | Reporting betreft alle zoek- en (geautomatiseerde) rapportage functies over de middels monitoring verzamelde gegevens. Onder andere beschikbaarheidspercentages, resourcegebruik en bijzondere meldingen kunnen per gewenst tijdsbestek beschikbaar worden gesteld. Reporting is vaak vanuit de SLA een vereiste om aan te tonen dat aan de afgesproken resultaatverplichtingen is voldaan. |
| 3. Alerting | Bij afwijking van vooraf gestelde monitoring parameters vindt signalering/alerting plaats, zowel binnen de monitoring applicaties als via externe media zoals bijvoorbeeld email/SMS naar betreffende verantwoordelijke personen en/of afdelingen. Binnen de alerting vindt meestal nog classificatie plaats van meldingen die de ernst van de geconstateerd situatie aangeeft. |
| 4. Logging | Logging is het centraal registreren van alle relevante gebeurtenissen die plaatsvinden op infrastructuur componenten. Deze componenten versturen de platte meldingen voorzien van een tijdsstempel naar de centrale log voorziening welke het vervolgens opslaat, er vindt geen intelligente verwerking van de data plaats. Logging is bedoeld als registratiemechanisme en als extra informatiebron voor het analyseren van bepaalde situaties/gebeurtenissen. |

| | |
|---|---|
| 5. Dashboard | Een dashboard geeft een geaggregeerd overzicht van de 'gezondheid' van een specifieke omgeving, dienst of groep infrastructuur componenten, zodat in één oogopslag zichtbaar wordt als zich ergens een foutsituatie voordoet. Het dashboard is hierin een verlengstuk van de monitoring dienst. |
| 6. Analytics | Operationele analyse verwijst naar de categorie bedrijfsanalyses die zich richt op het meten van de bestaande en realtime activiteiten van het bedrijf. Het maakt gebruik van data-analyse en business intelligence om de efficiëntie te verbeteren en de dagelijkse activiteiten in realtime te stroomlijnen. |

## 5.3.10(ABB) Architectuur Bouwblok Configuration Management




*Figuur 20 - Architectuur Bouwblok Configuration Management*

In onderstaand overzicht worden alle elementen met betrekking tot bouwblok Configuration Management nader beschreven.

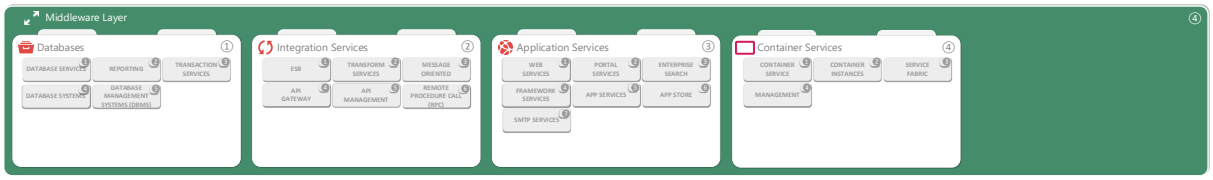
| Element | Beschrijving |
|---|---|
| 1. Licensing Services | Dit betreft de voorzieningen die zijn getroffen door software vendoren of organisaties van eindgebruikers om controle te hebben over waar en hoe software producten worden gebruikt. Enerzijds worden vendoren beschermd tegen illegaal gebruik van hun software producten, tegelijkertijd houden organisaties grip op hun compliancy met licentie overeenkomsten en de kosten van software gebruik. |
| 2. Platform deployment | Platform Deployment Services gives administrators the ability to deploy operating systems remotely. |
| 3. Inventory | De inventory is de centrale opslagplaats voor alle configuration management informatie. Deze wordt gebruikt voor het vastleggen van historische wijzigingen maar bijvoorbeeld ook voor het draaien van rapportages. Tot de inventory behoort vaak een database, maar bijvoorbeeld ook een verzameling van relevante documenten. |
| 4. Workspace management | De verzameling van software tooling en overige voorzieningen die helpen bij het beheer van de werkplekomgeving van eindgebruikers noemen we workspace management. De workspace kan in velerlei vormen bestaan, van fat clients met lokaal geïnstalleerde applicaties en tablets tot thin clients en |

| | |
|---|---|
| | gevirtualiseerde en gecentraliseerde Server Based Computing oplossingen. Iedere variant vergt zijn eigen specifieke beheerinstrumenten. |
| 5. System management | Systems management is de bedrijfsbrede administratie van computersystemen. Maximale productiviteit kan worden bereikt door correlatie van events, system automation en voorspellende analyses. Systems management kan uit onder ander de volgende processen bestaan: hardware inventories, server availability monitoring en metrics, software inventory en installatie, anti-virus en anti-malware management, monitoring van gebruikersactiviteit, capacity monitoring, security management, storage management, monitoring van netwerkcapaciteit en –belasting, anti-manipulation management. |
| 6. Patch Management | Een patch is een stuk(je) software bedoeld om een computerprogramma of de ondersteunende data aan te passen, met als doel deze te repareren of verbeteren. Hieronder vallen beveiligings kwetsbaarheden en bugs, zulke patches heten dan ook vaak bug fixes, die de bruikbaarheid en/of performance verbeteren. Hoewel ze zijn ontworpen om problemen te verhelpen, kunnen patches soms ook nieuwe introduceren. Het proces rondom de distributie van patches wordt patch management genoemd. Het is onderdeel van lifecycle management, en planning van welke patches wanneer op welke systemen moeten worden uitgerold. |
| 7. Mobile device management | Mobile device management (MDM) is een branchterm voor het beheer van mobiele devices, zoals smartphones, tablet computers, laptops en desktop computers. MDM wordt meestal geïmplementeerd met behulp van een third party product met beheerkenmerken voor specifieke vendoren of typen mobiele devices. MDM is een manier om te waarborgen dat medewerkers productief kunnen blijven en niet in strijd handelen met het bedrijfsbeleid. Veel organisaties maken dan ook gebruik van MDM producten/diensten om controle te houden over hun medewerkers. MDM houdt zich met name bezig op afscherming/scheiding van bedrijfsdata, beveiligen van email, afschermen van bedrijfsinformatie op devices, het afdwingen van policies, en integratie en beheer van mobiele devices inclusief laptops en handhelds in allerlei categorieën. MDM implementaties kunnen zowel on-premise als cloud based zijn. |
| 8. Configuration Management | Configuratiemanagement is een systems engineering proces voor het vaststellen en onderhouden van een product of object, waarbij men functionele en fysieke kenmerken kan aangeven met vereisten en operationele informatie gedurende de levenscyclus. |
| 9. Licensing metering | Licensing metering bestaat uit een aantal aspecten, te beginnen met het meten en onderhouden van software licenties. Het is van belang dat niet meer dan het maximum aantal licenties van een bepaald pakket in gebruik is, en dat er voldoende licenties zijn voor iedereen die dat nodig heeft. Dit houdt dan ook in monitoring van concurrent software gebruik, en real-time afdwingen van licentie beperkingen. Een tweede aspect is het monitoren op gebruik van ongeregistreerde en/of ongelicenseerde software. Een alternatieve methode voor software licensering is automatische registratie van het aantal malen en hoe lang een of meerdere functies van software gebruikt wordt, en facturatie vindt plaats op daadwerkelijk gebruik (ook bekend als 'pay-per-use'). |





## 5.4 Middleware diensten



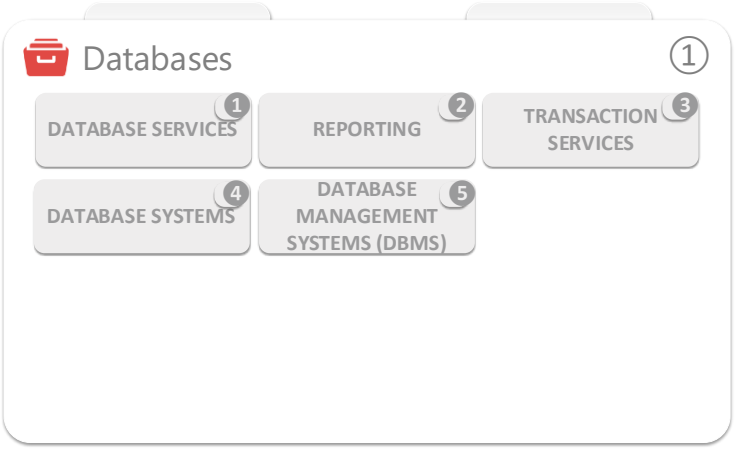

*Figuur 21 – Middleware layer*

Deze laag beschrijft welke middleware applicaties gebruikmaken van de ICT-infrastructuur en welke bovenliggende applicaties weer gebruik maken van de middleware laag

De Middleware laag bevat de bouwblokken die gebaseerd zijn op infrastructuur componenten en bieden de mogelijkheden om deze te laten gebruiken door eindgebruikers en applicaties. Dit zijn ook de componenten waarmee operationeel beheer in de meest voorkomende omgevingen vaak op dagelijkse basis mee te maken heeft. De behandeling van deze laag beperkt zich hier tot enkele hoofdcomponenten.

Databases bevat de gestructureerde opslag van data in de vorm van databases en database services om die data te ontsluiten aan applicaties. Er wordt doorgaans onderscheid gemaakt tussen database inrichting voor infrastructurele applicaties (alle infrastructure services die een database nodig hebben) en Line Of Business applicaties. In het laatste geval fungeert database vaak als een hoeksteen voor de Enterprise Service Bus.

### 5.4.1 (ABB) Databases



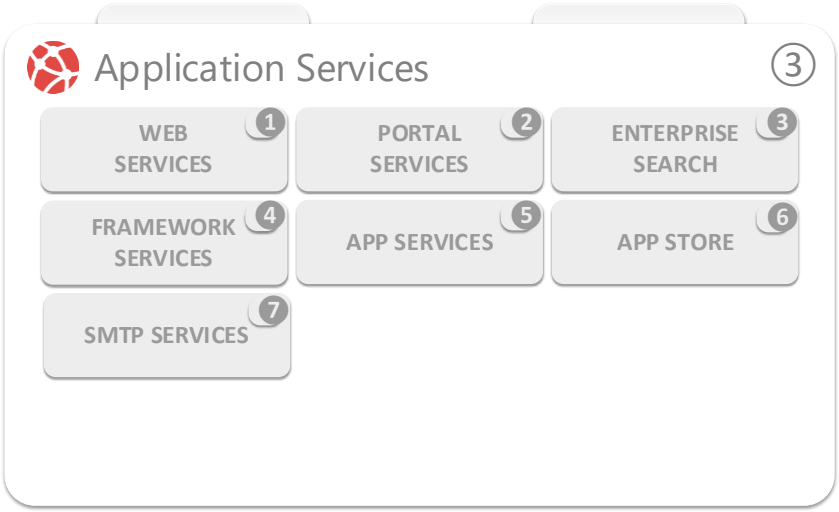

*Figuur 22 - Architectuur Bouwblok Databases*

In onderstaand overzicht worden alle elementen met betrekking tot bouwblok Databases nader beschreven.

| Element | Beschrijving |
|---|---|
| 1. Database Services | Database-services zorgen voor schaalbaarheid en een hoge beschikbaarheid van de database. Database-services maken de onderliggende softwarestack transparant voor de gebruiker. |
| 2. Reporting | Database reporting is het geformatteerde resultaat van database queries en bevat nuttige data voor analyses en besluitvorming. De meeste kwalitatieve business applicaties bevatten ingebouwde |

| | |
|---|---|
| | rapportage tools, enkele database platformen hebben zelf reporting componenten die door applicaties kunnen worden aangesproken. Dit is vaak een front-end interface die back-end database queries draait of aanroept, welke vervolgens worden geformateerd voor eenvoudige applicatie toepassing. |
| 3. Transaction Services | Een transactie sympoliseert een werkhoeveelheid binnen een database management systeem voor een database, en wordt in een consistente en betrouwbare wijze onafhankelijk van andere transacties verwerkt. Een transactie omvat feitelijk iedere wijziging binnen een database. Transaction services zijn ontworpen om de integriteit van een system te bewaken in een bekende, consistente staat, door ervoor te zorgen dat alle van elkaar afhankelijk zijnde acties ofwel allen succesvol worden afgehandeld, dan wel allen succesvol worden afgewezen. Indien enkele acties zijn uitgevoerd maar er ontstaan fouten bij een of meerdere volgende, dan zal de transaction service alle acties binnen de transactie terugdraaien, inclusief de succesvolle. Hierdoor komt de database weer in de vorige, consistente status terecht. Als alle acties binnen een transactie eenmaal succesvol zijn uitgevoerd, wordt de transactie bevestigd door het system, en alle wijzigingen aan de database worden permanent. De transactie kan hierna niet meer worden teruggedraaid. |
| 4. Database Systems | Databasesystemen of DBMS is software die geschikt is voor het verzamelen van elektronische en digitale records om nuttige informatie te extraheren en die informatie op te slaan, bekend als databasesystemen/databasebeheersystemen of DBMS. Het doel van een standaarddatabase is het opslaan en ophalen van gegevens. |
| 5. Database Management Systems | Met een databasemanagementsysteem (dbms) wordt een systeem aangeduid dat als database opgeslagen gegevens ontsluit, bewaakt en beheert. Een database bestaat soms uit drie onderdelen: de opgeslagen gegevens (in één of meer bestanden), het programma waarmee de gegevens worden onderhouden (DBMS) en eventueel de gebruikersomgeving (client) die het gebruikers mogelijk maakt om de gegevens te behandelen. Meestal is er één DBMS actief voor meer dan een gebruiker. Bekende en veelgebruikte programma's zijn relationele dbms'en (afgekort tot rdbms) zoals MySQL, Microsoft SQL Server en Oracle Database. |

## 5.4.2 (ABB) Architectuur Bouwblok Application Services

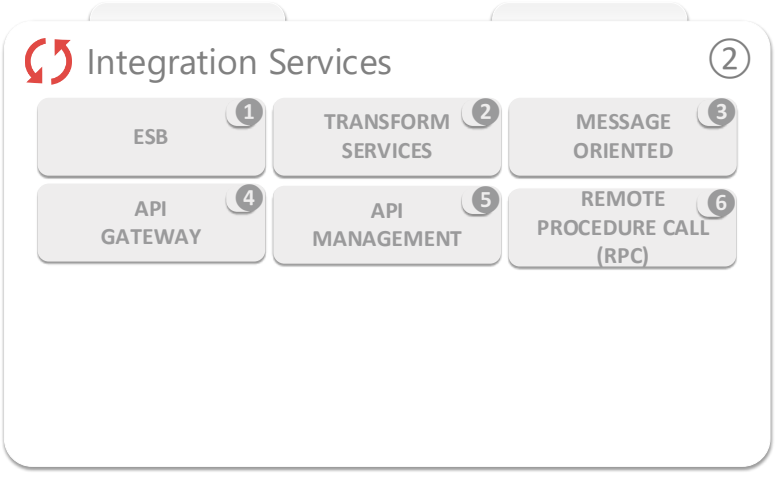



*Figuur 23 - Architectuur Bouwblok Application Services*

In onderstaand overzicht worden alle elementen met betrekking tot bouwblok Application Services nader beschreven.

| Element | Beschrijving |
|---|---|
| 1. Web Services | Webservices zijn op zichzelf staande, modulaire toepassingen die kunnen worden beschreven, gepubliceerd, gelokaliseerd en aangeroepen via een netwerk. Ze implementeren een services-georiënteerde architectuur (SOA), die het verbinden of delen van resources en data op een zeer flexibele en gestandaardiseerde manier ondersteunt. |
| 2. Portal Services | (Web) Portals zijn er in twee smaken - intern en extern. Interne portals zijn ontworpen om services binnen een organisatie te bieden, terwijl externe portals als startpunt dienen voor het surfen op internet. |
| 3. Enterprise Search | Enterprise Search is het doorzoekbaar maken van inhoud uit meerdere bronnen van het bedrijfstype, zoals databases en intranetten, voor een bepaald publiek. "Enterprise search" wordt gebruikt om de software van zoekinformatie binnen een onderneming te beschrijven (hoewel de zoekfunctie en de resultaten ervan nog steeds openbaar kunnen zijn). |
| 4. Framework Services | Het Service Application Framework biedt een platform waarmee ontwikkelaars schaalbare middle-tier-applicaties kunnen bouwen. Deze services kunnen gegevens of verwerkingsbronnen leveren aan andere applicaties. |
| 5. App Services | App Service is een Platform as a Service (PaaS)-aanbod van Microsoft. We gebruiken het om webapplicaties, REST API's en backend-services voor mobiele applicaties te hosten. |
| 6. App Store | Een app store (application store) is een online portal waarmee softwareprogramma's beschikbaar worden gesteld voor aanschaf en download. |
| 7. SMTP Services | Een eenvoudige mailtransferprotocol-relay (SMTP-relay) is een service die wordt gebruikt als een middel om e-mailberichten te transporteren tussen verschillende e-mailhostingservices, servers en / of domeinen. |

### 5.4.3 (ABB) Architectuur Bouwblok Integration Services




*Figuur 24 - Architectuur Bouwblok Integration Services*

In onderstaand overzicht worden alle elementen met betrekking tot bouwblok Integration Services nader beschreven.

| Element | Beschrijving |
|---|---|
| 1. ESB | Een enterprise service bus is een architecturale softwareconstructie waarmee de communicatie tussen de afnemers van diensten en aanbieders hiervan, vereenvoudigd wordt. |
| 2. Transform Services | Transformatiediensten vormen de reeks technologiegerichte diensten die een bedrijf helpen zijn producten, dienstverlening, ontwikkeling en aanpak te verbeteren. Een transformatiedienstverlener kan klanten adviseren over verschillende benaderingen, waaronder: Agile softwareontwikkeling. Bedrijfsanalyse. |
| 3. Message Oriented | Berichtgeoriënteerde middleware is een software- of hardware-infrastructuur die het verzenden en ontvangen van berichten tussen gedistribueerde systemen ondersteunt. |
| 4. API Gateway | Een API-gateway is een API-beheertool die zich tussen een client en een verzameling back-endservices bevindt. Een API-gateway fungeert als een omgekeerde proxy om alle API-aanroepen (Application Programming Interface) te accepteren, de verschillende services die nodig zijn om ze te vervullen samen te voegen en het juiste resultaat te retourneren. |
| 5. API Management | API-beheer is het proces van het maken en publiceren van programmeerinterfaces voor webtoepassingen, het afdwingen van hun gebruiksbeleid, het controleren van de toegang, het koesteren van de abonneegemeenschap, het verzamelen en analyseren van gebruiksstatistieken en het rapporteren over de prestaties |
| 6. Remote Procedure Call (RPC) | Een remote procedure call, kortweg RPC, is een technologie die een computerprogramma op één bepaalde computer toestaat om code uit te voeren op een andere machine zonder dat de programmeur de code expliciet hiervoor geschreven heeft. |

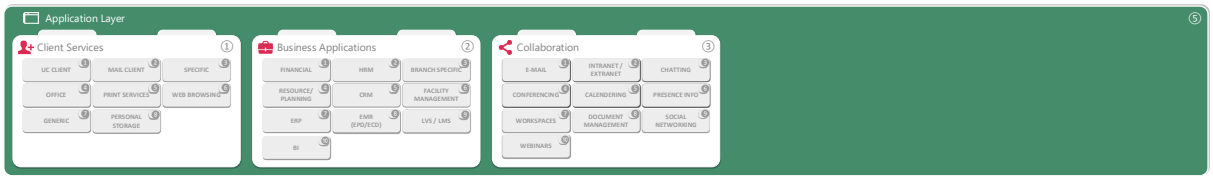
## 5.4.4 (ABB) Architectuur Bouwblok Container Services


*Figuur 25 - Architectuur Bouwblok Container Services*

In onderstaand overzicht worden alle elementen met betrekking tot bouwblok Container Services nader beschreven.

| Element | Beschrijving |
|---|---|
| 1. Container Service | Containers as a Service ( CaaS ) is een cloudgebaseerde service waarmee softwareontwikkelaars en IT-afdelingen containers kunnen uploaden, organiseren, uitvoeren, schalen en beheren met behulp van op containers gebaseerde virtualisatie. |
| 2. Container Instances | Container Instances is een beheerde service waarmee u containers rechtstreeks op de public-cloud kunt uitvoeren, zonder dat u virtuele machines (VM's) hoeft te gebruiken. |
| 3. Service Fabric | Een containerservices-fabric is een raamwerk van applicatieservices die nodig zijn om een gecontaineriseerde applicatie te implementeren, beheren en beveiligen op basis van microservices-architectuur. |
| 4. Management | Containerbeheer is een proces voor het automatiseren van het maken, inzetten en schalen van containers. Containermanagement faciliteert het op grote schaal toevoegen, vervangen en organiseren van containers. |

## 5.5 Applicatie diensten




*Figuur 26 – Application layer*

Deze laag beschrijft welke applicaties gebruikmaken van de ICT-infrastructuur (infrastructuur applicaties, kantoorautomatisering en Business applicaties).

Op de applicatie laag van de PICRA (figuur 41) komen we een driedeling van applicaties tegen die allen gebruikmaken van de onderliggende lagen. Grofweg behelst de driedeling die van:

- de typische business applicaties die elke organisatie uniek maakt;
- front-end applicaties die op iedere desktop moeten voorkomen met een look and feel van een lokale implementatie (office applicaties zoals een rekenblad, presentatiesoftware, webbrowser, e-mail etc.), kortweg de Kantoorautomatisering (KA) genoemd;
- de generieke applicaties die in bijna elke organisatie voorkomen, maar waarvoor het niet praktisch is een business eigenaar aan te wijzen als eigenaar (e-mail service, document management, telefonie en conferencing service etc.).

Er zijn altijd wel een aantal herkenbare business applicaties zoals een HRM systeem, financieel systeem of branche specifiek informatiesysteem. Anders dan 2 en 3 is dit echter volledig het domein van de informatie & applicatie architectuur, kortweg informatisering. De opname hiervan op deze plek is meer uit oogpunt van kennis nemen van het applicatielandschap met het oog op gemeenschappelijk gebruik, capaciteitsplanning en toe te passen standaarden in de infrastructuur zoals databases. Op dat punt hebben infrastructuur en informatisering gemeenschappelijke belangen. Vanzelfsprekend is er vaak ook een front-end gedeelte van business applicaties die beschikbaar worden gemaakt door de infrastructuur adequaat in te richten, zie Deployment Services en Application Delivery op de Supporting Infra Services laag.

De client services is juist wel weer volledig onderdeel van de infrastructuur. Het betreft hier de relatief eenvoudige applicaties zoals eerder genoemd. Wie echter al eens een poging heeft ondernomen om te migreren van de ene office suite naar de andere (MS Office naar Open Office en vice versa) of een upgrade van een of meer versies weet als geen ander hoe lastig en complex dat kan zijn. Dat komt omdat de KA applicaties vaak heel veel relaties hebben met andere applicaties en men ook meteen de productiviteit van eindgebruikers aantast en de beschikbaarheid van informatie in het geding komt.

De laatste categorie is Collaboration. Deze backend applicaties zijn de toepassingen die typisch door grote delen van de organisatie gebruikt worden en nodig zijn om medewerkers in staat stellen om goed samen te werken, zoals e-mail en portals. Een relatief nieuwe verzamelnaam voor enkele collaboration toepassingen is Unified Communications. Dit laat e-mail en voicemail bij elkaar komen, maakt onderling chatten mogelijk als tussenvorm tussen bellen en mailen. Het toont presence informatie en stelt gebruikers op eenvoudige wijze in staat zelf voice en video conferencing te starten. Door al deze middelen te integreren met vaste telefonie, Voice over IP en mobiele telefonie ontstaan nieuw mogelijkheden die de productiviteit een boost geven. Veelal zijn dit de technologie bouwstenen voor het moderne leren, ontdekken, leiden, innoveren en samenwerken – of kortweg ‘het flexibel werken’.

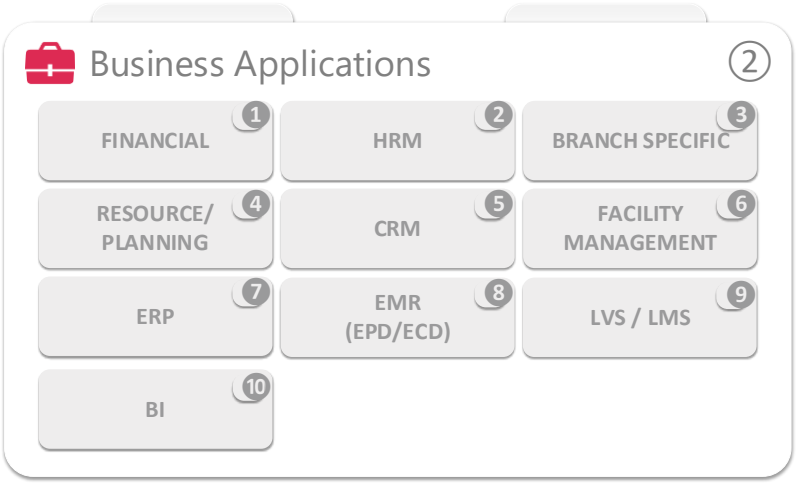
### 5.5.1 (ABB) Architectuur Bouwblok Client Services


*Figuur 27 - Architectuur Bouwblok Client Services*

In onderstaand overzicht worden alle elementen met betrekking tot bouwblok Client Services nader beschreven.

| Element | Beschrijving |
|---|---|
| 1. UC Client | Unified Communications Client zoals Skype for Business, voorheen bekend als Microsoft Lync Server, is een Unified Communications (UC) -platform dat gemeenschappelijke kanalen voor zakelijke communicatie en online vergaderingen integreert, inclusief instant messaging (IM), aanwezigheid, voice over IP (VoIP), voicemail, bestandsoverdrachten , videoconferenties, webconferenties en e-mail. |
| 2. Mail client | Een e-mailclient biedt de gebruiker functies om een e-mail te schrijven, te bewerken en aan te bieden aan een mailserver voor bezorging bij de ontvanger. De e-mailclient kan ook worden gebruikt om e-mail te ontvangen van een mailserver. |
| 3. Specific | Specifieke onderdelen die voor de klant in gebruik zijn genomen voor specifieke doeleinden. |
| 4. Office | Microsoft Office is een suite van desktop productiviteits toepassingen die speciaal is ontworpen voor gebruik op kantoor of in het bedrijfsleven. Het is een eigen product van Microsoft Corporation en werd voor het eerst uitgebracht in 1990 |
| 5. Print Services | Print voorzieningen voor de KA omgeving |
| 6. Web browsing | Internet browsers die gebruikt worden om te kunnen internet surfen, |
| 7. Generic | Generieke onderdelen die voor de klant in gebruik zijn genomen. |
| 8. Personal Storage | OneDrive for Business is personal online storage space, much like your My Documents folder or Home Drive, but in the cloud and provided to you by your company. Use it to store your work files across multiple devices with ease and security. Share your files with business colleagues as needed, and edit Office documents together in real time with Office Online. Sync files to your local computer using the OneDrive for Business sync app. |

### 5.5.2 (ABB) Architectuur Bouwblok Business Applications



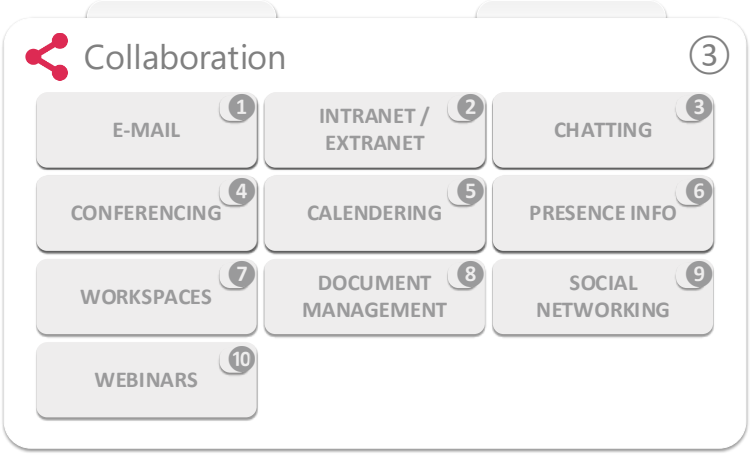

*Figuur 28 - Architectuur Bouwblok Business Applications*

In onderstaand overzicht worden alle elementen met betrekking tot bouwblok Client Services nader beschreven.

| Element | Beschrijving |
|---|---|
| 1. Financial | Financiële applicaties |
| 2. HRM | HR Applicaties |
| 3. Branch Specific | Specifieke onderdelen die voor de klant in gebruik zijn genomen voor specifieke doeleinden. |
| 4. Resource / Planning | Planning applicaties |
| 5. CRM | Customer relationship management oftewel crm is een Engelstalige benaming voor klantrelatiebeheer, soms ook relatiemarketing of verkoopbeheersysteem genoemd. |
| 6. Facility Management | Facilitair management kan worden gedefinieerd als de tools en diensten die de functionaliteit, veiligheid en duurzaamheid van gebouwen, terreinen, infrastructuur en onroerend goed ondersteunen. Facilitair beheer omvat: Leasebeheer, inclusief huuradministratie en boekhouding. |
| 7. ERP | Enterprise resource planning staat voor een computerprogramma gebruikt binnen organisaties ter ondersteuning van alle processen binnen het bedrijf. Een ERP-programma bestaat meestal uit kleine deelprogramma's die allemaal een specifieke taak ondersteunen |
| 8. EMR (EPD / ECD) | Elektronisch patiënten dossier / elektronisch cliënten dossier |

| | |
|---|---|
| 9. LVS / LMS | Leerling volg system / Leer management systeem |
| 10. BI | Business intelligence |

### 5.5.3 (ABB) Architectuur Bouwblok Collaboration



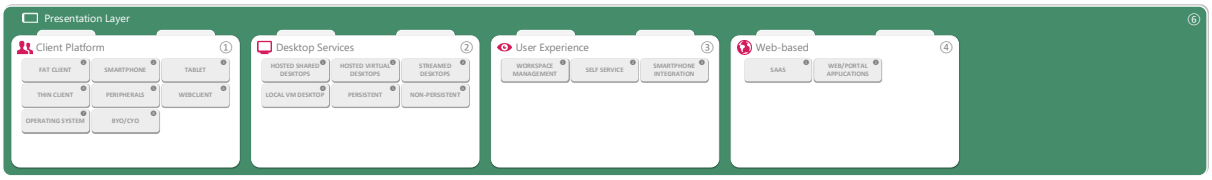

*Figuur 29 - Architectuur Bouwblok Collaboration*

In onderstaand overzicht worden alle elementen met betrekking tot bouwblok Collaboration nader beschreven.

| Element | Beschrijving |
|---|---|
| 1. E-mail | E-mail is de naam van digitaal, elektronisch postverkeer. Zowel het individuele bericht als het onderliggende systeem kunnen met e-mail worden bedoeld. Als synoniemen worden gebruikt: mail, e-post, e-brief, elektronische post en elektronische brief. |
| 2. Intranet / Extranet | Intranet is een hulpmiddel voor het delen van informatie binnen de organisatie. Terwijl Extranet een hulpmiddel is voor het delen van informatie tussen de interne leden en externe leden. 2. Intranet is eigendom van één organisatie. Hoewel Extranet eigendom is van één of meerdere organisaties |
| 3. Chatting | Chatting, is een benaming voor technologieën waarbij het de bedoeling is dat berichten zeer snel worden overgebracht. Dit in tegenstelling tot e-mail, waarbij de snelheid van overbrengen iets lager kan zijn. |
| 4. Conferencing | Conferencing is een zeer algemene term voor verschillende soorten technologieën waarmee twee of meer mensen van verschillende locaties een liveconferentie over internet of middels telefoon kunnen houden. |
| 5. Calendering | Agenda is de kalender en planningscomponent van Outlook die volledig is geïntegreerd met e-mail, contacten en andere functies. |

| | |
|---|---|
| 6. Presence info | In computer- en telecommunicatienetwerken is aanwezigheidsinformatie een statusindicator van een mede-gebruiker. De client van een gebruiker biedt aanwezigheidsinformatie (aanwezigheidsstatus) via een netwerkverbinding met een aanwezigheidsservice, die wordt opgeslagen in zijn persoonlijke beschikbaarheid. Waarmee andere gebruikers kunnen waarnemen of een mede gebruiker beschikbaar is voor communicatie. |
| 7. Workspaces | Collaborative workspaces zijn kantoren waarin medewerkers van verschillende bedrijven onder één dak werken. Bedrijven die een gezamenlijke werkruimte delen, zijn er in alle soorten en maten, van groeiende startups tot internationale ondernemingen. |
| 8. Document management | Document Management is het proces van het opslaan, lokaliseren, bijwerken en delen van gegevens met het oog op workflow-voortgang en bedrijfsresultaten. Gecentraliseerd delen en gegevensopslag binnen specifieke servers helpen organisaties om informatie efficiënt en effectief toegang te krijgen tot informatie, samen met het beveiligen van beschermde gegevens. Programma's en servers worden gebruikt in het proces van documentbeheer. Belangrijke metadata is gecentraliseerd, in tegenstelling tot gedecentraliseerd of moeilijk te lokaliseren. |
| 9. Social Networking | Een sociaalnetwerksite of een online sociaal netwerk is een internetdienst waarmee gebruikers een sociaal netwerk kunnen creëren en onderhouden. Meestal gebeurt dit door het aanmaken van een online profiel, dat ze vervolgens kunnen koppelen aan de profielen van anderen. |
| 10. Webinars | Een webinar is een lezing, workshop, college of soortgelijke presentatie of vorm van kennisoverdracht die plaatsvindt via het internet. Het neologisme "webinar" is een porte-manteau van de woorden "web" en "seminar". Webinars worden doorgaans live uitgezonden |

## 5.6 Presentation (Werkplek) diensten




Deze laag beschrijft de architectuur waarop applicaties aan de gebruikers beschikbaar worden gesteld.

De Presentation Layer is de laag die applicaties zichtbaar maakt voor gebruikers en hier vindt dan ook de interactie met gebruikers plaats. Key point is dus de hedendaagse enorme hoeveelheid aan endpoint devices die al dan niet ondersteund of zelfs beheerd moeten worden.

Als een endpoint device wordt verstrekt door de organisatie en locked down beheerd wordt is er sprake van een trusted endpoint. Organisaties die kiezen voor een Bring Your Own Device (BYOD) beleid of onbeheerde thuiswerkplekken, werken in principe met untrusted endpoints. Daarnaast zijn nog andere, hybride, vormen denkbaar. De keuzes (of requirements) die organisaties hierin maken (of hebben), hebben vergaande consequenties voor de manier waarop ‘de werkplek’ wordt aangeboden op ‘het device’. Dit geldt, zoals al blijkt, niet in de laatste plaats voor de informatiebeveiligingsaspecten die samenhangen met de manier van werken.

Gelukkig maakt virtualisatie het mogelijk om de functionaliteit los te koppelen van de onderliggende hardware. Met desktopvirtualisatie in de vorm van Server Based Computing (SBC) t.b.v. desktop- of application publishing is al veel ervaring opgedaan in menig organisatie. Relatief nieuw zijn de individueel gevirtualiseerde desktop besturingssystemen, VDI (Virtual Desktop Interface), die veilig in het datacenter draaien en meer te personaliseren zijn. Daarmee is echter niet ineens een zaligmakende oplossing geboren. VDI is een goede uitkomst voor een kantoor waar gebruikers beschikken over een toetsenbord + muis + beeldscherm of rondreizende medewerkers met een laptop met een dataverbinding. Maar op een smartphone of tablet scoort de gebruikerservaring hierbij onvoldoende. De infrastructuur dient dus bij voorkeur in staat te zijn om te detecteren met welk apparaat de medewerker zich aanmeldt en op basis daarvan de technologie te gebruiken om een daarbij passende weergave van de applicatie te tonen. Op een smartphone is dat wellicht een web gebaseerde App of een browser gebaseerde applicatie, maar die zijn vaak (nog) niet of onvoldoende voorhanden. Belangrijk is het om eerst in te schatten met welk type gebruikers en hun mobiliteit de organisatie te maken heeft en de keuze van ondersteunde devices daaropaf te stemmen, te standaardiseren of te beperken.

Organisaties die te lichtzinnig kiezen voor diverse hybride vormen van Presentation Services zullen dat merken aan hun budget: het aantal licenties dat afgetikt moet worden maakt een dergelijk aanpak vanuit TCO-standpunt voorlopig niet economisch haalbaar, mede dankzij diverse aanvullende tooling om die vormen op elkaar aan te sluiten. Organisaties die weloverwogen hybride vormen kiezen zullen zich nadrukkelijk bewust zijn van de voordelen die het hen oplevert en de prijs die daarvoor betaald wordt.

### 5.6.1 (ABB) Architectuur Bouwblok Client Platform

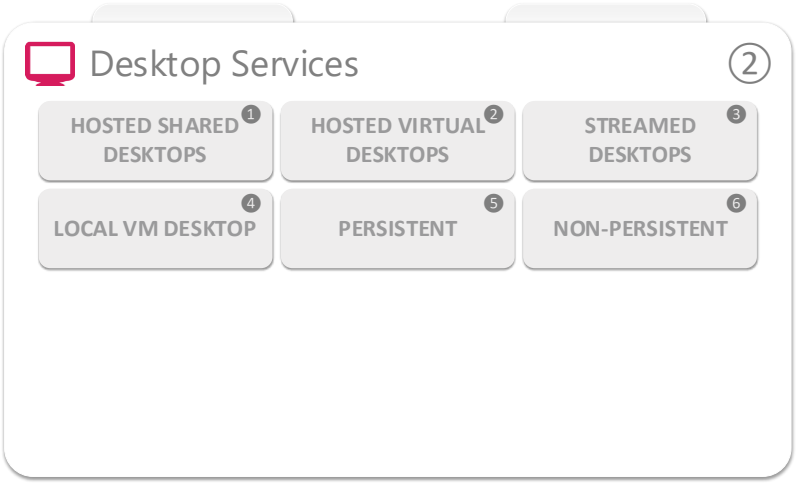

*Figuur 30 - Architectuur Bouwblok Client Platform*

In onderstaand overzicht worden alle elementen met betrekking tot bouwblok Client Platform nader beschreven.

| Element | Beschrijving |
|---|---|
| 1. FAT Client | Een FAT Client is een volwaardige computer voorzien van alle aspecten |
| 2. Smartphone | Smartphone is een een mobiele telefoon die veel van de functies van een computer uitvoert, meestal met een touchscreeninterface, internettoegang en een besturingssysteem waarmee gedownloade apps kunnen worden uitgevoerd. |
| 3. Tablet | Een tablet is een personal computer met een draadloos touchscreen (pc) die kleiner is dan een notebook, maar groter is dan een smartphone. Moderne tablets zijn gebouwd met draadloos internet of lokale netwerken (LAN) en een verscheidenheid aan softwaretoepassingen, waaronder bedrijfstoepassingen, webbrowsers en games. |
| 4. Thin Client | Een Thin Client is een afgeslankte computer voorzien van alleen de noodzakelijke componenten |
| 5. Peripherals | Randapparatuur van computers. |
| 6. Web client | Web client based applicaties. |
| 7. Operating System | Het besturings systeem van een computer. |

| | |
|---|---|
| 8. BYO / CYO | Bring-Your-Own en Choose-Your-Own is een concept waarbij de gebruiker zelf zijn aparatuur mag inbrengen om te gebruiken op het werk. |

### 5.6.2 (ABB) Architectuur Bouwblok Desktop Services



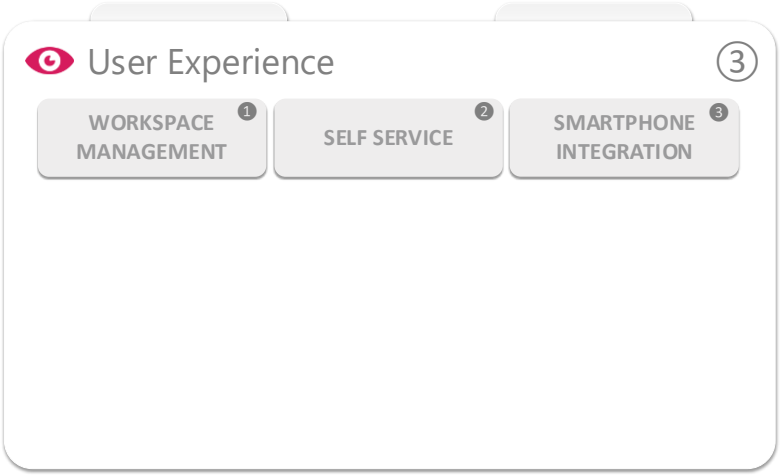

*Figuur 31 - Architectuur Bouwblok Desktop Services Services*

In onderstaand overzicht worden alle elementen met betrekking tot bouwblok Desktop Services nader beschreven.

| Element | Beschrijving |
|---|---|
| 1. Hosted shared desktops | Een gehoste desktop is een product dat is ingesteld in de grotere cloud computing-omgeving en dat over het algemeen wordt geleverd met een combinatie van technologieën, waaronder hardware virtualisatie en een of andere vorm van externe verbindingssoftware. Citrix XenApp of Microsoft Remote Desktop Services zijn twee van de meest voorkomende. De verwerking vindt plaats in de datacenteromgeving.<br><br>Een gehoste desktop heeft meestal een browsergebaseerde verbinding met een desktopomgeving met een kantoorproductiviteitssuite naast andere bureaubladtoepassingen. De desktop wordt gehost, uitgevoerd, geleverd en ondersteund vanaf een centrale locatie, meestal een beveiligd datacenter met hoogwaardige en veerkrachtige verbindingen met internet / cloud. Cloud Desktop is een term die vaak wordt gebruikt om te verwijzen naar een container van een verzameling virtuele objecten, software, hardware, configuraties enz. Die zich in de cloud bevinden, die door een client worden gebruikt om te communiceren met externe services en computergerelateerde taken uit te voeren.<br><br>Verbindende clients hebben vooraf geïnstalleerde of gedownloade viewertoepassingen via een van de vele externe desktopprotocollen. Klanten kunnen thin clients, pc's, werkstations, mobiele en handheld-apparaten met verschillende besturingssystemen, zoals Windows, Mac OS X, Linux. |
| 2. Hosted Virtual Desktops | Een gehoste virtuele desktop (HVD) is een volledige, thick-client gebruikersomgeving, die wordt uitgevoerd als een virtuele machine (VM) op een server en op afstand toegankelijk is. |
| 3. Streamed Desktops | Applicatiestreaming creëert een gevirtualiseerde desktop die centraal kan worden beheerd, maar toch de snelheid van lokale uitvoering biedt |

| | |
|---|---|
| 4. Local VM Desktop | Desktop draait op het lokale apparaat van de gebruiker op een virtuele machine (VM). Hierdoor kan een gebruiker meerdere desktops op dezelfde fysieke computer gebruiken en kan IT de zakelijke omgeving op één desktop vergrendelen terwijl de gebruikers nog steeds persoonlijk gebruik kunnen maken van hun pc. |
| 5. Persistent | Een permanente desktop is een desktop waarop aan het einde van de gebruikerssessie alles wordt opgeslagen. Alle bestanden die zijn opgeslagen op het bureaublad, instellingen of snelkoppelingen zijn blijven allemaal bewaard aan het einde van de session. |
| 6. Non-persistent | Een niet-permanente desktop is een desktop waarop aan het einde van de gebruikerssessie niets wordt opgeslagen. Alle bestanden die zijn opgeslagen op het bureaublad, instellingen of snelkoppelingen zijn allemaal verloren aan het einde van de session. |

### 5.6.3 (ABB) Architectuur Bouwblok User Experience

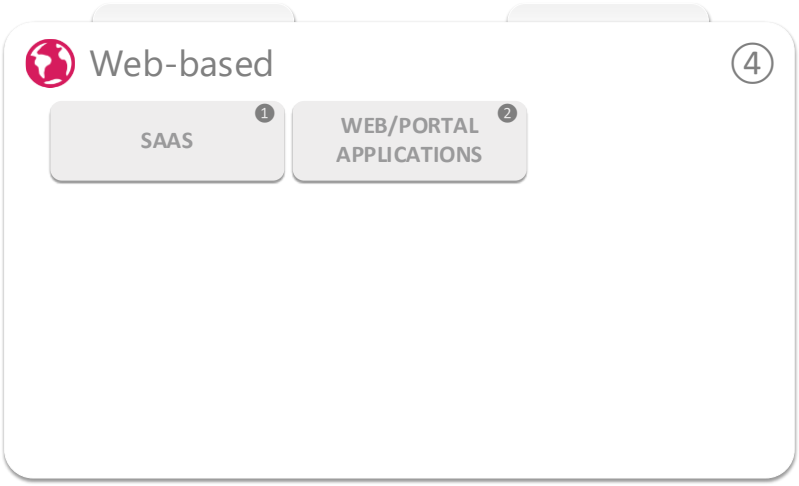



*Figuur 32 - Architectuur Bouwblok User Experience Services*

In onderstaand overzicht worden alle elementen met betrekking tot bouwblok User Experience nader beschreven.

| Element | Beschrijving |
|---|---|
| 1. Workspace Management | De verzameling van software tooling en overige voorzieningen die helpen bij het beheer van de werkplekomgeving van eindgebruikers noemen we workspace management. De workspace kan in velerlei vormen bestaan, van fat clients met lokaal geïnstalleerde applicaties en tablets tot thin clients en gevirtualiseerde en gecentraliseerde Server Based Computing oplossingen. Iedere variant vergt zijn eigen specifieke beheerinstrumenten. |
| 2. Self Service | Een zelf bedienings portaal voor eind gebruikers waarmee ze zelf redzaam worden voor bepaalde zaken die door de IT afdeling beschikbaar worden gesteld, zoals het zelf resetten van een wachtwoord. |
| 3. Smartphone Integration | Integratie van Smartphone met de KA omgeving, waarbij de Apps die op de Smartphone beschikbaar worden gesteld worden ontsloten voor overige Apps op de Smartphone. |

### 5.6.4 (ABB) Architectuur Bouwblok Web Based




*Figuur 33 - Architectuur Bouwblok Web Based Services*

In onderstaand overzicht worden alle elementen met betrekking tot bouwblok Web Based nader beschreven.

| Element | Beschrijving |
|---|---|
| 1. SaaS | Software-as-a-Service voorzieningen |
| 2. Web/Portal Applications | Web en Portaal applicaties |

## 5.7 Compliance & Control diensten


Deze laag geeft kaders en context in relatie tot informatiebeveiliging waaraan de overige lagen moeten voldoen qua Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV) en de kwaliteit eisen.

De Security Services zijn gebaseerd op de beginselen van informatiebeveiliging en de daaruit voortkomende aspecten Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV, of in het Engels CIA). Vanzelfsprekend is deze plaat het domein van informatiebeveiliging. De vraag of er een separate beveiligingsarchitectuur opgesteld moet worden of dat informatiebeveiliging een onderdeel is van iedere laag laat zich echter niet eenvoudig beantwoorden.

Zoals ook al uit de beschrijving van onderliggende lagen (Datacenter, Platform en Infrastructure Services) blijkt, is met name ‘beschikbaarheid’ een onderwerp dat grotendeels direct vanuit de infrastructuur opgepakt moet worden. De genoemde RPO en RTO zijn hierin belangrijke uitgangspunten.

Wat deze plaat met name wil uitdrukken is dat er verantwoordelijke stakeholders zijn die iets te zeggen hebben of beleid hebben over de afgebeelde onderwerpen m.b.t. informatiebeveiliging. En daarmee aanzienlijke invloed uitoefenen op de infrastructuur. Want hoe vaak ook geprobeerd wordt een beveiligingsmaatregel te treffen op een business- of applicatielaag, de maatregel moet uiteindelijk vaak geheel of gedeeltelijk worden geïmplementeerd op de infrastructuur laag.

Het gaat immers niet om het vermijden van risico’s, maar om het managen van risico’s. Een BIV-analyse vooraf kan de organisatie veel opleveren, omdat beveiligingsmaatregelen achteraf ingrijpend en dus vaak kostbaar uitpakken. Vragen die bij een BIV-analyse aan de orde komen zijn onder andere: Welke schade zou ontstaan indien informatiesystemen niet

beschikbaar zouden zijn voor een uur, een dag, een week etc.? Zouden er verkeerde managementbeslissingen genomen worden indien informatiesystemen niet beschikbaar zouden zijn voor een uur, een dag etc. en wat is de schade daarvan? Daarnaast is er vaak sprake van imagoschade (waarde?) en herstelschade (kosten?).

Om de beschrijving van de Cloud & Infrastructuur Architectuur kort te houden wordt voor een meer gedetailleerde beschrijving van dit gedeelte verwezen naar het domein informatiebeveiliging.

### 5.7.1 (ABB) Architectuur Bouwblok Availability


*Figuur 34 - Architectuur Bouwblok Availability*

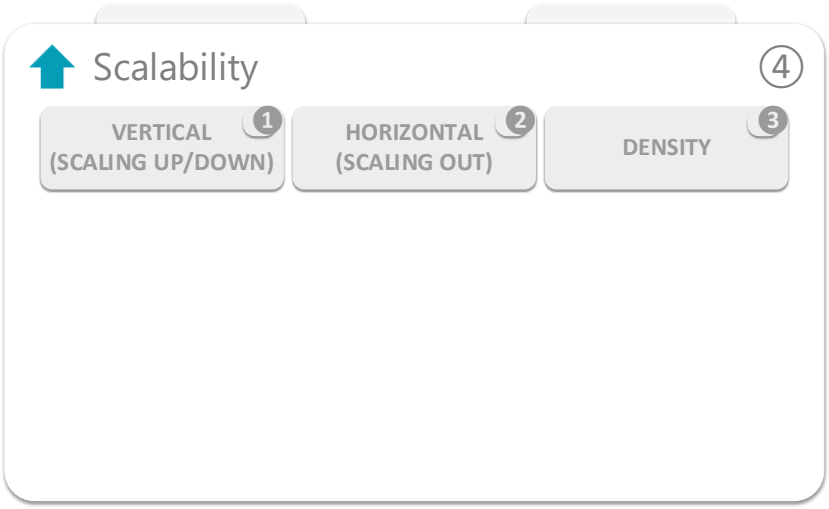
In onderstaand overzicht worden alle elementen met betrekking tot bouwblok Availability nader beschreven.

| Element | Beschrijving |
|---|---|
| 1. Tier Level (0-4) | Beschikbaarheid van het datacenter |
| 2. Fault Tolerant | Een fouttolerant ontwerp maakt het mogelijk dat een systeem doorgaat met de beoogde werking, mogelijk op een verlaagd niveau, in plaats van volledig te falen, wanneer een deel van het systeem uitvalt. De term wordt meestal gebruikt om computersystemen te beschrijven die zijn ontworpen om min of meer volledig operationeel te blijven, met misschien een vermindering van de doorvoer of een toename van de responstijd in het geval van een gedeeltelijke uitval. Dat wil zeggen, het systeem als geheel wordt niet gestopt vanwege problemen in de hardware of de software. |
| 3. Clustering | Een cluster bestaat uit een aantal computers die zijn verbonden aan een LAN omgeving en die als één computer fungeren en acties uitvoeren. |
| 4. RPO/RTO | Recovery Point Objective (RPO) geeft herstelpuntdoelstelling en is een begrip uit de wereld van de informatietechnologie. RPO is the job of the best-of-the-art, of the computer of the ICT and / of een ICT-dienstverlener. RPO is verwant aan RTO.<br>Recovery Time Objective (RTO) betekent hersteltijddoelstelling en is een begrip uit de wereld van de informatietechnologie. RTO is het streven om te voldoen aan de afgesproken hersteltijd na een computercrash, door de afdeling ICT en/of een ICT dienstverlener. RTO is verwant aan RPO. |

| | |
|---|---|
| 5. Archiving | Archiveren is een bijzondere vorm van documenteren, te weten het vastleggen van informatie voor later (her)gebruik |
| 6. Replication | Replicatie is het continu kopiëren van gegevenswijzigingen. De twee locaties bevinden zich over het algemeen op verschillende fysieke servers. |
| 7. High Availability | Hoge beschikbaarheid verwijst naar systemen die duurzaam zijn en waarschijnlijk langdurig zonder storing zullen werken. De term impliceert dat delen van een systeem volledig zijn getest en dat er in veel gevallen accommodatie is voor mislukking in de vorm van overtollige componenten. |
| 8. OTA | Ontwikkeling, Test, Acceptatie en Productie, afgekort OTAP is de naam van een methodiek die wordt gebruikt in de ICT. De hoofdwoorden in de naam geven de fases aan die onder andere in de softwareontwikkeling doorlopen worden. Het Nederlandse begrip is afgeleid van het Engelse DTAP: Development, Testing, Acceptance and Production.<br><br>Het pad dat wordt doorlopen is als volgt:<br><br>O: Een programma of component wordt eerst ontwikkeld in de ontwikkelomgeving, hierin bevindt zich veelal een of meerdere personen in een ontwikkelteam die ieder op een ontwikkelwerkplek werken aan 1 gezamenlijke versie, die aan het einde van elke dag wordt gekopieerd ofwel 'ingecheckt' in het versiebeheerprogramma op de ontwikkelserver.<br><br>T: Deze gezamenlijke versie wordt dan 's nachts automatisch van programmacode naar een draaibaar programma omgezet, ofwel 'gebuild' en eventueel doorgezet naar de testserver. Op de testserver kan er met deeltest, ofwel ´unittests´ automatisch technisch en functioneel getest worden, waarvan de resultaten de volgende dag klaarliggen voor het ontwikkelteam. Als er na een ontwikkelperiode een functionele samengestelde versie ofwel een ´release´ wordt gestabiliseerd, kan deze release volledig doorgetest worden met alle voor de software gekozen testgevallen door alle betrokken partijen, personen en gebruikers.<br><br>A: Na goedkeuring kan de versie worden geïnstalleerd in de acceptatieomgeving. Het installatieproces wordt gedocumenteerd in een productiegang draaiboek. De acceptatie-omgeving is qua software en hardware zo veel mogelijk gelijk aan de productieomgeving. De klant kan hier alvast zien hoe de release er functioneel en qua performance uit gaat zien in productie. Dit, zonder dat de dagelijkse productie onderbroken wordt.<br><br>P: Indien de klant accepteert in de acceptatie-omgeving, wordt het programma geïnstalleerd op de productieomgeving, zoals gedocumenteerd toen de release naar de acceptatie-omgeving ging. Tevens moet er een terugdraaiplan zijn om bij verrassingen toch de productie-installatie ongedaan te maken en door te gaan in productie met de oude versie. |




## 5.7.2 (ABB) Architectuur Bouwblok Scalability

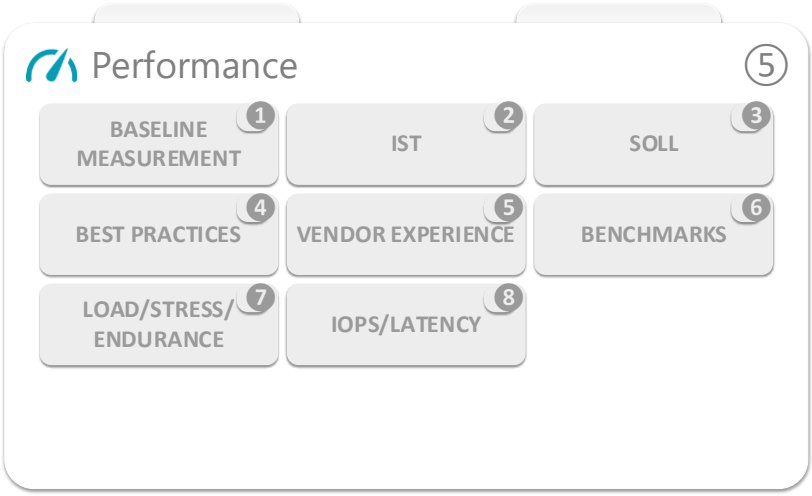



*Figuur 35 - Architectuur Bouwblok Scalability*

In onderstaand overzicht worden alle elementen met betrekking tot bouwblok Scalability nader beschreven.

| Element | Beschrijving |
|---|---|
| 1. Vertical (Scaling-up) | De term 'verticale schaalverdeling' zoals deze in het algemeen wordt toegepast in IT, verwijst naar het opbouwen van resources, in tegenstelling tot de term 'horizontal scaling', wat betekent dat er moet worden gebouwd. Deze twee verschillende soorten schaalverkleining werken anders op basis van de hardware en software die hierbij betrokken zijn. |
| 2. Horizontal (Scaling-out) | Horizontaal schalen is een term die in veel verschillende soorten IT-opstellingen wordt gebruikt. De basisbetekenis van horizontaal schalen is dat systemen worden "uitgebouwd" met behulp van extra componenten. De term 'verticale schaalverdeling' betekent daarentegen dat extra capaciteit en bronnen aan één enkele component worden toegevoegd. |
| 3. Density | Meer ruimte creëren met bestaande middelen. |

### 5.7.3 (ABB) Architectuur Bouwblok Performance




*Figuur 36 - Architectuur Bouwblok Performance*

In onderstaand overzicht worden alle elementen met betrekking tot bouwblok Performance nader beschreven.

| Element | Beschrijving |
|---|---|
| 1. Baseline measurement | In IT-beheer is een baseline de verwachte waarden of condities waartegen alle uitvoeringen worden vergeleken. Een basislijn is een vast referentiepunt. Vanuit het oogpunt van projectbeheer wordt het creëren van basislijnen beschouwd als het officiële einde van de projectplanning en het begin van de uitvoering en controle van het project. Controle van baselines is cruciaal voor project- en IT-management. |
| 2. IST | De IST-situatie beschrijft de huidige stand van zaken waarbij kan worden aangegeven wat er in de huidige situatie wel en niet beschikbaar is en nodig is om hetgeen men wenst te bereiken te realiseren. |
| 3. SOLL | De SOLL-situatie beschrijft de stand van zaken wat men wenst te bereiken en te realiseren. Één van de doelarchitecturen is opgezet conform het TOGAF Architecture Development Model. |
| 4. Best practices | Een best practice is een sectorbrede overeenkomst die de meest efficiënte en effectieve manier standaardiseert om een gewenste uitkomst te bereiken. Een best practice bestaat over het algemeen uit een techniek, methode of proces. Het concept houdt in dat als een organisatie de beste werkwijzen volgt, een geleverde uitkomst met minimale problemen of complicaties zal worden verzekerd. Best practices worden vaak gebruikt voor benchmarking en zijn het resultaat van herhaalde en contextuele gebruikersacties. |
| 5. Vendor experience | Ervaringen van vendoren en leveranciers zijn zeer waardevol om vooraf mee te nemen in de ontwerp fase, zodat oplossingen worden ontworpen waar goede ervaringen mee zijn. |
| 6. Benchmarks | Benchmarking is het maken van een vergelijking. Maar iemand die gaat benchmarken, vergelijkt niet zomaar twee situaties of prestaties. Bij een benchmark vergelijk je altijd iets met een 'ideale situatie'. Bijvoorbeeld met een best presterende concurrent of andere |

| | |
|---|---|
| | toonaangevende bedrijven. Ook je eigen prestaties kun je benchmarken of afzetten tegen de markt. |
| 7. Load/stress/endurance | Prestatietests zijn de tests die worden uitgevoerd om na te gaan hoe de componenten van een systeem presteren in een bepaalde situatie. Gebruik van hulpbronnen, schaalbaarheid en betrouwbaarheid van het product worden ook gevalideerd onder deze test. Deze test is de subset van prestatie-engineering, die is gericht op het aanpakken van prestatieproblemen in het ontwerp en de architectuur van softwareproducten.<br>Het primaire doel van prestatietests is het vaststellen van het benchmarkgedrag van het systeem. Er zijn een aantal branchegerichte benchmarks waaraan moet worden voldaan tijdens prestatietests. |
| 8. IOPS/latency | Invoer / uitvoerbewerkingen per seconde (IOPS, uitgesproken als eye-operatoren) is een invoer / uitvoer-prestatiemeting die wordt gebruikt voor het karakteriseren van computeropslagapparaten zoals harde schijven (HDD), solid-state schijven (SSD) en SAN's (storage area networks). Net als benchmarks hebben IOPS-nummers die door fabrikanten van opslagapparaten worden gepubliceerd, geen directe relatie met praktijktoepassingen in de praktijk |

### 5.7.4 (ABB) Architectuur Bouwblok Contracts


*Figuur 37 - Architectuur Bouwblok Contracts*

In onderstaand overzicht worden alle elementen met betrekking tot bouwblok Contracts nader beschreven.

| Element | Beschrijving |
|---|---|
| 1. Hardware | Hardware onderhoudscontracten |
| 2. Software | Software onderhoudscontracten |
| 3. UC / OLA / SLA | Het Ondersteuningscontract (UC) is een contract tussen een IT-serviceprovider en een derde partij. De derde partij biedt ondersteunende diensten waarmee de serviceprovider een service aan een klant kan leveren.<br><br>Een operational level agreement/OLA (SLM) is een overeenkomst tussen een it-serviceprovider en een ander onderdeel van dezelfde organisatie. Een OLA ondersteunt de levering door de it-serviceprovider van it-services aan de klanten.<br><br>Een service level agreement (SLA) is een afspraak tussen leverancier en klant over de beschikbaarheid en ondersteuning van een product of dienst. SLA's komen eigenlijk alleen voor bij dienstverlening tussen bedrijven. Een SLA geeft de afnemer zekerheid over de bruikbaarheid van een product of dienst. |
| 4. Licenses | Software licenties |
| 5. DAP | staat voor Daily Agreed Procedures. Het betreft een dossier waarin operationele werkafspraken tussen aanbieder en gebruiker staan omschreven. Een DAP dient geen beschrijving van de kwaliteit van de service, dit hoort thuis in de SLA. Vaak is een DAP wel een bijlage van de SLA |

### 5.7.5 (ABB) Architectuur Bouwblok Security

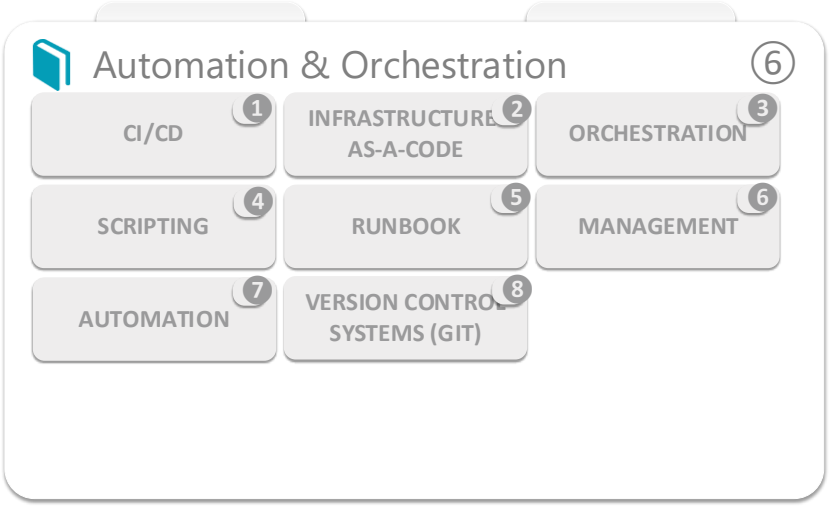

*Figuur 38 - Architectuur Bouwblok Security*

In onderstaand overzicht worden alle elementen met betrekking tot bouwblok Security nader beschreven.

| Element | Beschrijving |
|---|---|
| 1. ISO | ISO, de internationale organisatie voor standaardisatie. ISO ontwikkeld en publiceerd de internationale normen. |
| 2. NEN | NEN onderzoekt in hoeverre normalisatie mogelijk is en er interesse voor bestaat. Zij nodigen vervolgens alle belanghebbende partijen uit om deel te nemen. Een breed draagvlak is randvoorwaarde. De afspraken komen op basis van consensus tot stand en worden vastgelegd in een document. Dit is meestal een norm. |
| 3. ISAE | ISAE 3402 is een internationale standaard waarin richtlijnen zijn opgenomen die auditoren gebruiken voor het beoordelen van leveranciers (serviceorganisaties) van organisaties (gebruikersorganisaties). Tijdens deze audit beoordeelt een auditor de kwaliteit van de leveranciers en de uitbestede processen. |
| 4. (Company) Guidelines | Richtlijnen zoals deze zijn opgesteld door Cloud & Infrastructuur Architectuur. |
| 5. GDPR | GDPR (of AVG) is de Europese nieuwe regelgeving die de rechten van een individu voorschrijft alsook voorschriften oplegt welke maatregelen bedrijven/instanties dienen te nemen om de bescherming van de gegevens die zij in hun bezit hebben, te beschermen. |
| 6. Alerting | Welke vorm van Alering is vanuit Informatie Beveiliging benodigd en waar moet aan worden voldaan. |
| 7. Auditing | Welke vorm van Auditing is vanuit Informatie Beveiliging benodigd en waar moet aan worden voldaan. |

| | |
|---|---|
| 8. Hardening | verharding is het proces van het beveiligen van een systeem door het kwetsbaarheidsoppervlak te verkleinen, dat groter is wanneer een systeem meer functies vervult; in principe is een systeem met één functie veiliger dan een systeem voor meerdere doeleinden<br>Welke vorm van 'verharden' van OS en applicaties is vanuit Informatie Beveiliging benodigd en waar moet aan worden voldaan. |
| 9. SOC | Een security operations center is een centrale eenheid die zich bezighoudt met beveiligingsvraagstukken op organisatorisch en technisch niveau. Het omvat de drie bouwstenen voor het beheren en verbeteren van de beveiligingshouding van een organisatie: mensen, processen en technologie. |
| 10. ISMS | Informatiebeveiligingsbeheer definieert en beheert controles die een organisatie moet implementeren om ervoor te zorgen dat het de vertrouwelijkheid, beschikbaarheid en integriteit van activa op een verstandige manier beschermt tegen bedreigingen en kwetsbaarheden. |
| 11. NOC | Een Network Operations Center (NOC) is een centrale locatie van waaruit netwerkbeheerders een of meer netwerken beheren, besturen en bewaken. De algemene functie is het handhaven van optimale netwerkactiviteiten op verschillende platforms, media en communicatiekanalen.<br>Grote netwerkserviceproviders worden geassocieerd met netwerkoperatiecentra, die een visuele weergave bieden van de bewaakte netwerken en werkstations waar gedetailleerde netwerkstatus wordt bewaakt. Software wordt gebruikt om de netwerken te helpen beheren. Telecommunicatie, televisie-uitzendingen en computernetwerken worden beheerd via netwerkoperatiecentra. |
| 12. BIO | De Baseline informatiebeveiliging Overheid (BIO) is het basisnormenkader voor informatiebeveiliging binnen alle overheidslagen (Rijk, gemeenten, provincies en waterschappen). Had voorheen iedere overheidslaag zijn eigen baseline, nu is er met gezamenlijke inspanning één BIO voor de gehele overheid. |

## 5.7.6 (ABB) Architectuur Bouwblok Automation & Orchestration




*Figuur 39 - Architectuur Bouwblok Automation & Orchestration*

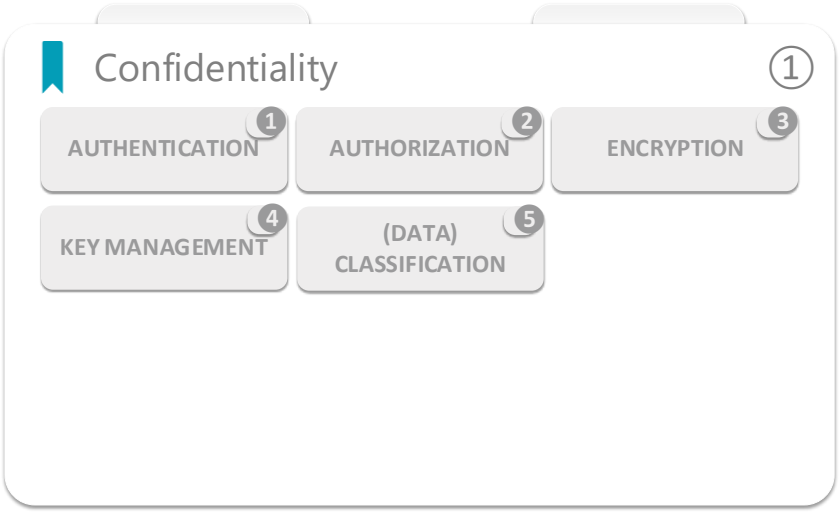
In onderstaand overzicht worden alle elementen met betrekking tot bouwblok Automation & Orchestration nader beschreven.

| Element | Beschrijving |
|---|---|
| 1. CI/CD | In software-engineering is CI/CD of CICD de gecombineerde praktijk van continue integratie en continue levering of continue implementatie. CI/CD overbrugt de kloof tussen ontwikkelings- en operationele activiteiten en teams door automatisering af te dwingen bij het bouwen, testen en implementeren van applicaties. |
| 2. Infrastructure-as-a-Code | Als software bedrijf ben je afhankelijk van IT-infrastructuur en de software zal op hardware moeten draaien. Software wordt gemaakt met code. Hardware draait tegenwoordig veelal in de cloud. Dat is vaak zelfs virtueel. Dit opent deuren, want de infrastructuur wordt zo programmeerbaar. Dat wordt een hele belangrijke manier van werken omdat diverse redenen die we in dit artikel toelichten.<br><br>Infrastructure as Code (IaC) of programmeerbare infrastructuur betekent het definiëren en beheren van infrastructuur door middel van code. Zo'n infrastructuur wordt beschreven als objecten met eigenschappen. Vaak worden deze objecten omschreven in YAML, XML of JSON, maar vaak is er ook ondersteuning om dit in je favoriete programmeertaal te doen als Kotlin, Python etc.<br><br>De objecten worden vervolgens tegen een omgeving aangehouden en de state wordt dan gesynchroniseerd. Op deze manier worden IT componenten aangemaakt, ge-update of verwijderd. Je programmeert dus wat je wilt en synchroniseert dat naar de omgeving, bijvoorbeeld AWS, Google Cloud of Microsoft Azure. |
| 3. Orchestration | Orchestration, specifiek in de informatica, is de geautomatiseerde configuratie, coördinatie en het beheer van computersystemen en software. Om Orchestration uit te kunnen voeren bestaan diverse toepassingen en hulpmiddelen. Enkele voorbeelden hiervan zijn Azure Bicep, Ansible, Puppet, Salt, Terraform en AWS CloudFormation. |
| 4. Scripting | Een scripttaal is een programmeertaal die geschikt is voor het schrijven van scripts, kleine programmaatjes om veel voorkomende taken pragmatisch te automatiseren, of om een langdurige maar eenmalige taak te verrichten |
| 5. Runbook | In een computersysteem of netwerk is een runbook een compilatie van routineprocedures en -bewerkingen die de systeembeheerder of -operator uitvoert. Systeembeheerders in IT-afdelingen en NOC's gebruiken runbooks als referentie. Runbooks kunnen in elektronische of in fysieke boekvorm zijn. |
| 6. Management | Management oplossingen van Orchestration tooling. Bijvoorbeeld met container orchestration kan het DevOps-team de gewenste status van het cluster als een configuratie vertegenwoordigen. Een engine voor container indeling dwingt de gewenste configuratie af en automatiseert alle beheertaken. |
| 7. Automation | Automatiseren van IT taken, zoals aanmaken van een account of uitgeven van rechten. |
| 8. version control systems (Git) | Het doel van versiebeheer is om softwareteams wijzigingen in de code te laten volgen, terwijl de communicatie en samenwerking tussen teamleden wordt verbeterd. |





### 5.7.7 (ABB) Architectuur Bouwblok Confidentiality




*Figuur 40 - Architectuur Bouwblok Confidentiality*

In onderstaand overzicht worden alle elementen met betrekking tot bouwblok Confidentiality nader beschreven.

| Element | Beschrijving |
|---|---|
| 1. Authentication | Authenticatie is het proces waarbij iemand nagaat of een gebruiker, een andere computer of applicatie daadwerkelijk is wie hij beweert te zijn. Bij de authenticatie wordt gecontroleerd of een opgegeven bewijs van identiteit overeenkomt met echtheidskenmerken, bijvoorbeeld een in het systeem geregistreerd bewijs. |
| 2. Authorization | Autorisatie in de informatica is het proces waarin een subject rechten krijgt op het benaderen van een object. De autorisatie wordt toegekend door de eigenaar van het object. Het meest gebruikte principe daarbij is need-to-know: je mag alleen zien wat je voor je functie nodig hebt. |
| 3. Encryption | Encryption is de kunst van het versleutelen van te verzenden data zodat deze niet leesbaar is. Door het versleutelen van data hou je de data geheim en ben je in staat de integriteit van de data en de identificatie van de zender te garanderen. |
| 4. Key Management | Sleutelbeheer verwijst naar het beheer van cryptografische sleutels in een cryptosysteem. Dit omvat het omgaan met het genereren, uitwisselen, opslaan, gebruiken, crypto-versnipperen en vervangen van sleutels. |
| 5. (Data) Classification | Gegevensclassificatie tagt gegevens op basis van het type, de gevoeligheid en de waarde voor de organisatie als ze worden gewijzigd, gestolen of vernietigd. Het helpt een organisatie de waarde van haar gegevens te begrijpen, te bepalen of de gegevens risico lopen en controles te implementeren om risico's te beperken. Gegevensclassificatie helpt een organisatie ook om te voldoen aan relevante branchespecifieke regelgeving zoals BIO en AVG.<br>Gegevens worden geclassificeerd op basis van hun gevoeligheidsniveau: hoog, gemiddeld of laag.<br>**Hooggevoelige gegevens** - als ze worden aangetast of vernietigd in een ongeautoriseerde transactie, zouden ze een catastrofale impact hebben op de organisatie of individuen. Bijvoorbeeld financiële gegevens, intellectueel eigendom, authenticatiegegevens. |

**Gegevens met gemiddelde gevoeligheid**: alleen bedoeld voor intern gebruik, maar als ze worden gecompromitteerd of vernietigd, hebben ze geen catastrofale gevolgen voor de organisatie of individuen. Bijvoorbeeld e-mails en documenten zonder vertrouwelijke gegevens.

**Gegevens met een lage gevoeligheid**: bedoeld voor openbaar gebruik. Bijvoorbeeld inhoud van openbare websites.

### 5.7.8 (ABB) Architectuur Bouwblok Integrity


*Figuur 41 - Architectuur Bouwblok Integrity*

In onderstaand overzicht worden alle elementen met betrekking tot bouwblok Integrity nader beschreven.

| Element | Beschrijving |
|---|---|
| 1. Integrity | Het begrip integriteit is een kwaliteitskenmerk van gegevens in het kader van de informatiebeveiliging. Het is een synoniem voor betrouwbaarheid. Een betrouwbaar gegeven is Juist Volledig Tijdig Geautoriseerd. |
| 2. Data | De juistheid van de gegevens moet worden gewaarborgd; tijdens het bewerken van de gegevens kunnen storingen optreden en gebruikers kunnen tegelijkertijd dezelfde gegevens muteren. Gelijktijdig muteren kan worden voorkomen door record- of filelocking toe te passen. |

## 5.8 Governance & Management diensten


Deze laag geeft kaders en context in relatie tot Governance voor sturing en management op het gebruik van nu en in de toekomst. Hoe gaan we om met veranderingen, verbeteringen en incidenten (beheersing).

Hoewel hier met name ITIL v3 zaken op afgebeeld staan zouden dit net zo goed ITIL v2 zaken kunnen zijn. Waar deze plaat de aandacht op wil vestigen is dat een goed werkende infrastructuur niet alleen afhankelijk is van technologie. Het gaat om de balans tussen Mensen, Processen en Technologie.

Al is de technologie nog zo goed voor elkaar, als er geen afspraken worden gemaakt en vastgelegd in processen waarin mensen samenwerken dan zal het niet gaan functioneren. Evengoed geldt dat als je afspraken en technologie goed zijn je niet buiten de mensen en hun expertise kunt om de technologie te bedienen. Vrijwel ieder onderdeel heeft een beslag in de infrastructuur.

### 5.8.1 (ABB) Architectuur Bouwblok Knowledge Retention


*Figuur 42 - Architectuur Bouwblok Knowledge Retention*

In onderstaand overzicht worden alle elementen met betrekking tot bouwblok Knowledge Retention nader beschreven.

| Element | Beschrijving |
|---|---|
| 1. Education | Opdoen van kennis van nieuwe technieken. |
| 2. Documentation | Documenteren is een belangrijk onderdeel van het implementeren van een nieuwe ICT infrastructuur |
| 3. Troubleshooting | Probleemoplossing is een vorm van probleemoplossing, vaak toegepast om defecte producten of processen op een machine of een systeem te repareren. Het is een logische, systematische zoektocht naar de bron van een probleem om het op te lossen en het product of proces weer operationeel te maken. |
| 4. Knowledge base | Een kennisbank is een gespecialiseerde databank voor de opslag en het beheer van 'kennis'. Een kennisbank is de basis voor een collectie van kennis. Normaliter bestaat een kennisbank uit specifieke kennis met betrekking tot een organisatie bijvoorbeeld: artikel troubleshooting white papers gebruikershandleiding |
| 5. Whitepapers | Whitepapers zijn artikelen die alle informatie geven over een specifieke techniek of oplossing |
| 6. Management | Kennismanagement of kennisbeheer is het proces van het creëren, delen, gebruiken en beheren van de kennis en informatie van een organisatie. Het begrip verwijst naar een multidisciplinaire benadering voor het bereiken van organisatiedoelstellingen door kennis optimaal te benutten. |
| 7. Adoption | Een model dat gebruikers van innovaties classificeert op basis van hun mate van bereidheid om nieuwe ideeën te accepteren. Innovatieve adoptiekenmerken worden toegewezen aan groepen om |

| | |
|---|---|
| | aan te tonen dat alle innovaties een voorspelbaar proces doorlopen voordat ze algemeen worden geadopteerd |
| 8. Workshops | Workshops zijn interactieve sessies met projectleden waarin besluitvorming en keuzes gezamelijk worden gemaakt. |

### 5.8.2 (ABB) Architectuur Bouwblok Architecture


*Figuur 43 - Architectuur Bouwblok Architecture*

In onderstaand overzicht worden alle elementen met betrekking tot bouwblok Architecture nader beschreven.

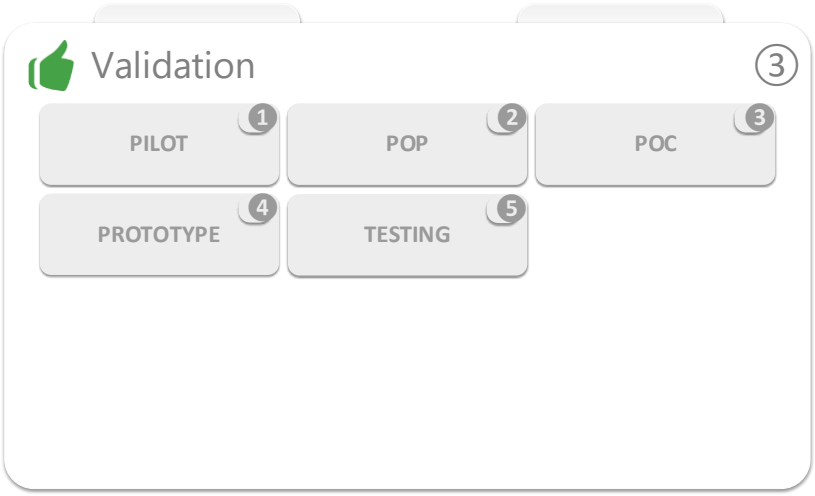
| Element | Beschrijving |
|---|---|
| 1. Business | Het wordt vaak omschreven als een onderdeel van Enterprise architectuur gerelateerd aan de business kant van de organisatie. De formele definitie volgens de Object Management Group's Business Architecture Working Group is als volgt:<br><br>"een blauwdruk van de onderneming die een gemeenschappelijk begrip van de organisatie verschaft en wordt gebruikt om strategische doelstellingen en tactische eisen op elkaar af te stemmen." |
| 2. Information | De informatie-architectuur beschrijft de inhoudelijke relaties en samenhang tussen toepassingen en gegevensverzamelingen onderling. Hiermee worden de relaties met informatie en communicatie als bedrijfsmiddelen/productiefactoren van een organisatie inzichtelijk |
| 3. Technical | Technische architectuur Architectuur die weergeeft wat nodig is om de informatievoorziening te laten werken zoals deze is beschreven in de informatie-architectuur, bijvoorbeeld hardware en netwerk specificaties, overzicht van technische componenten en hun relatie met informatiesystemen. |
| 4. Governance | IT-governance is een raamwerk dat ervoor zorgt dat de IT-infrastructuur van uw organisatie wordt ondersteund en waarmee de bedrijfsstrategieën en -doelstellingen kunnen worden bereikt. |

| | |
|---|---|
| 5. Guiding Principles | Alle principes of voorschriften die een organisatie leiden in alle omstandigheden, ongeacht veranderingen in haar doelen, strategieën, soort werk of het topmanagement. |
| 6. Innovation | Innovatie kan eenvoudig worden gedefinieerd als een "nieuw idee, apparaat, oplossing of methode". Het tegenovergestelde van innovatie is exnovatie. |
| 7. PSA | Een Project StartArchitectuur (PSA) is een document dat als hulpmiddel bij een project wordt ingezet om veranderingen te faciliteren. |
| 8. Quality Aspects | Kwaliteit heeft kenmerken als: beheerbaarheid, beveiliging, bruikbaarheid, continuïteit, controleerbaarheid, duurzaamheid, functionaliteit, gebruikersvriendelijkheid, herbruikbaarheid, inpasbaarheid, onderhoudbaarheid, prestatie, portabiliteit, testbaarheid, zuinigheid. |
| 9. Enterprise | Enterprise-architectuur (EA) is het vakgebied op het snijvlak van Business en IT. Of liever gezegd: tussen bedrijfskunde, informatiekunde en informatica in, met als doel dat de totale organisatie zich in de gewenste richting verder ontwikkelt. |
| 10. Application | De applicatiearchitectuur beschrijft de samenhang van applicaties en informatiesystemen binnen een organisatie. Het is een modelmatige beschrijving van het applicatielandschap, de daadwerkelijk in productie zijnde systemen. De applicatiearchitectuur is een onderdeel van de enterprisearchitectuur. |
| 11. Naming Convention | Naamconventies zijn algemene regels die worden toegepast bij het implementeren van nieuwe services en servers. Ze hebben veel verschillende doelen, zoals het toevoegen van duidelijkheid en uniformiteit aan scripts, leesbaarheid voor toepassingen van derden en functionaliteit en toepassingen. |
| 12. Roadmap | Als duidelijk is wat er moet gebeuren en wat de prioriteiten zijn, dan is de volgende stap het maken van een IT Roadmap. Dit is te vergelijken met een ontwerptekening van een architect, waarbij omschreven staat welke acties en wanneer deze worden uitgevoerd. Een roadmap bevat drie kenmerken: het doel, de tijdslijn en de samenhang tussen de verschillende uit te voeren onderdelen. |





### 5.8.3 (ABB) Architectuur Bouwblok Validation




*Figuur 44 - Architectuur Bouwblok Validation*

In onderstaand overzicht worden alle elementen met betrekking tot bouwblok Validation nader beschreven.

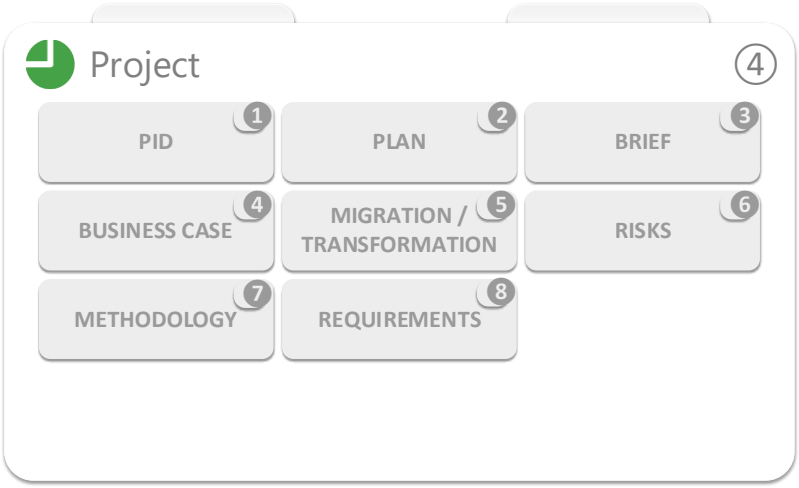
| Element | Beschrijving |
|---|---|
| 1. Pilot | Een pilotstudie, een pilotproject of een pilot-experiment is een kleinschalig vooronderzoek dat is uitgevoerd om de haalbaarheid, tijd, kosten, nadelige gebeurtenissen te evalueren en het ontwerp van de studie te verbeteren voordat een grootschalig onderzoeksproject wordt uitgevoerd. |
| 2. POP | Eén van de belangrijke redenen voor het houden van een PoP is: het kunnen achterhalen van de benodigde (soms verborgen) functionaliteiten die voor jouw organisatie van belang zijn. Veel doorontwikkelde producten zoals enterprise search engine software of document management systemen bestaan tegenwoordig uit 1001 functionaliteiten.<br><br>Bij een PoP kies je uit de functionaliteiten van de applicatie, de voor jouw organisatie belangrijkste onderdelen (knockout criteria en bijzondere features) en zegt tegen de leverancier wat je wilt zien, op welke manier en binnen welke tijd. Liefst doe je dat tegen een aantal leveranciers tegelijkertijd zodat je heel precies kunt zien en meten wat de leveranciers kunnen en doen. Meestal doorkruist dat het 'normale' patroon van de leverancier en komt het voor hen aan op snel creatief kunnen schakelen, je maakt er een soort competitie van tussen de leveranciers. |
| 3. POC | Een Proof of Concept (PoC) is een methode om door middel van een werkend product te demonstreren of een bepaalde IT-oplossing geschikt is voor een bepaald doel. Deze werkwijze is geschikt voor zowel pakketsoftware, een maatwerkproduct of een low-code ontwikkelplatform |
| 4. Prototype | Een prototype is een vroeg model van een product, handgemaakt of via rapid prototyping, waarmee optredende krachten, de werking of passing van onderdelen wordt getest en de productie wordt voorbereid. Prototypen worden in allerlei disciplines toegepast. De eisen aan de prototypen verschillen per productsoort |
| 5. Testing | Doel is om vooraf te weten of de gebruiker ermee wil gaan werken en om te weten te komen welke problemen de gebruiker verwacht. Bijkomend voordeel is dat een gedeelte van de gebruikers al geschoold wordt in het gebruik en dat een eventuele trainingsbehoefte ingeschat kan worden. |

Het doel van de acceptatietest is vast te stellen dat de software/oplossing voldoet aan uw eisen en wensen en dat de software/oplossing geschikt is voor bedrijfsmatige ingebruikname.

Voorbeelden hiervan zijn:

- Technische Acceptatie Tests (TAT)
- Gebruikers Acceptatie Tests (GAT)

### 5.8.4 (ABB) Architectuur Bouwblok Project



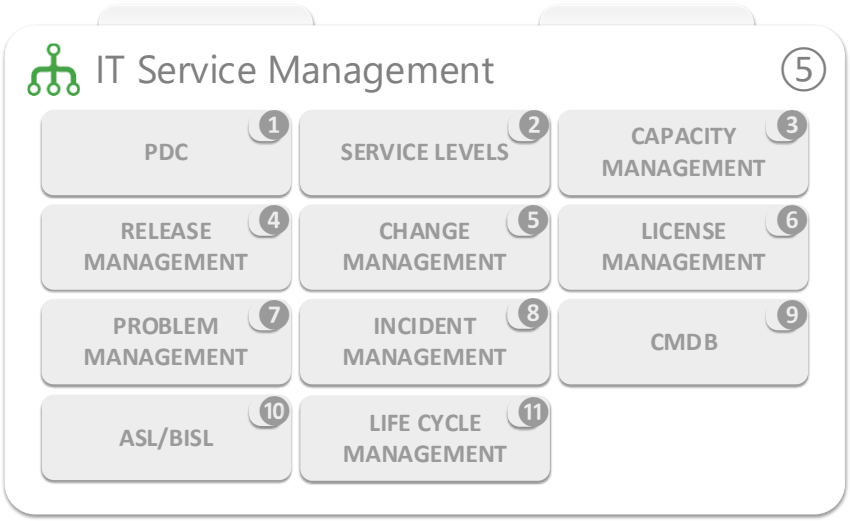

*Figuur 45 - Architectuur Bouwblok Project*

In onderstaand overzicht worden alle elementen met betrekking tot bouwblok Project nader beschreven.

| Element | Beschrijving |
|---|---|
| 1. PID | Een Project Initiation Document (PID) is een van de belangrijkste onderdelen van projectmanagement, die de basis vormt voor een bedrijfsproject. Het is een referentiepunt in het gehele project voor zowel de klant als het projectteam. Daarnaast is het PID een beslisdocument op basis waarvan het mandaat wordt uitgevoerd.<br><br>Een Project Initiation Document bundelt de informatie die is verkregen door het opstarten van een project en initiatieven van een projectproces in een Prince2 gecontroleerde omgeving. Project Initiation Document is een Prince2 term; een projectmanagementmethode die zich richt op de succes- en faalcriteria binnen projecten. |
| 2. Plan | Zo worden in het projectplan afspraken gemaakt tussen de opdrachtgever en de projectleider. De afspraken gaan onder andere over welke feiten, situaties en bovenliggende organisatiedoelen de opdracht te maken heeft (achtergrond), de ongewenste situatie (probleem) en welke uiteindelijk opgelost moet gaan worden (doel). |

| | |
|---|---|
| 3. Brief | De projectbrief helpt om o.a. doelstellingen, randvoorwaarden en projectorganisatie te expliciteren. U kunt deze standaard projectbrief aanpassen voor de situatie bij uw corporatie. Bij kleinere corporaties kan een afgeleide vorm van de projectbrief van toepassing zijn gezien de omvang. |
| 4. Business case | Een businesscase of een haalbaarheidsstudie is een projectmanagement-term waarin de zakelijke afweging om een project of taak te beginnen beschreven wordt. In de businesscase worden de kosten tegen de baten afgewogen, rekening houdend met de risico's |
| 5. Migration / Transformation | Het migratie- , transformatieplan beschrijft het gehele proces van conversie of migratie. Het (geïntegreerde) testplan beschrijft wat en hoe er wordt getest en wat het resultaat moet zijn; de resultaten van de test worden vastgelegd in een testverslag. |
| 6. Risks | Onvoldoende beschikking over middelen (geld, mensen) Geen heldere planning en deadline. Geen duidelijk en compleet projectplan. Het ontbreken van duidelijke resultaten |
| 7. Methodology | Projectmethoden gebaseerd op het 'Waterval' gedachtegoed wordt vaak gezien als het traditionele projectmanagement waarbij eerst een (uitgebreid) plan van aanpak wordt geschreven. Vervolgens wordt het project zo precies mogelijk uitgevoerd zoals staat omschreven in dit plan.<br>IPMA en Prince2 zijn voorbeelden van Project Methodieken. |
| 8. Requirements | De basis is dat goede requirements compleet, correct, realiseerbaar, waardevol, geprioriteerd, ondubbelzinnig en testbaar zijn. Daarbij moet de juiste informatie bij requirements vastgelegd zijn, in de taal van de gebruiker en met een detaillering die aansluit bij het project. |

### 5.8.5 (ABB) Architectuur Bouwblok IT Service Management




*Figuur 46 - Architectuur Bouwblok IT Service Management*

In onderstaand overzicht worden alle elementen met betrekking tot bouwblok IT Service Management nader beschreven.

| Element | Beschrijving |
|---|---|
| 1. PDC | Een Producten- en dienstencatalogus, in het kort een PDC, is een etalage voor jouw diensten. Hier kunnen jouw klanten informatie vinden over de producten en diensten die jouw afdeling aanbiedt. |
| 2. Service Levels | Serviceniveau meet de prestaties van een systeem. Bepaalde doelen zijn gedefinieerd en het serviceniveau geeft het percentage aan waarin die doelen moeten worden bereikt. Opvullingspercentage verschilt van serviceniveau. Voorbeelden van serviceniveau: Percentage oproepen dat is beantwoord in een callcenter |
| 3. Capacity Management | Het doel van capaciteitsbeheer is ervoor te zorgen dat de middelen voor informatietechnologie voldoende zijn om op een kosteneffectieve manier aan de toekomstige zakelijke vereisten te voldoen. Een veelvoorkomende interpretatie van capaciteitsbeheer wordt beschreven in het ITIL-raamwerk. |
| 4. Release Management | Releasemanagement is een proces uit de softwareontwikkeling. Het omvat het plannen, bouwen en testen van gewijzigde en nieuwe onderdelen in de software, vanaf de requirementsanalyse tot het in één keer voor gebruik beschikbaar maken van de verzameling aan onderdelen in een stabiele versie. |
| 5. Change Management | Met change management zorg je ervoor dat de mensen in de organisatie zo snel en soepel mogelijk de transitie doorlopen, waardoor zowel de mensen als de organisatie gebruik kunnen maken van de voordelen die de verandering teweeg moet brengen |
| 6. License Management | Een softwarelicentiemanager is een softwarebeheertool dat wordt gebruikt door onafhankelijke softwareleveranciers of door eindgebruikersorganisaties om te bepalen waar en hoe softwareproducten kunnen worden uitgevoerd. |
| 7. Problem Management | Probleembeheer is het proces dat verantwoordelijk is voor het beheer van de levenscyclus van alle problemen die zich voordoen of kunnen optreden in een IT-service. |
| 8. Incident management | Incidentmanagement is een procesgebied voor IT-servicemanagement (ITSM). Het eerste doel van het incidentbeheerproces is het zo snel mogelijk herstellen van een normale serviceoperatie en het minimaliseren van verstoringen. |
| 9. CMDB | Een database voor configuratiebeheer is een ITIL-term voor een database die door een organisatie wordt gebruikt om informatie over hardware- en softwareactiva op te slaan. Het is handig om configuratie-items op te splitsen in logische lagen. |
| 10. ASL/BISL | ASL en BiSL zijn beide publieke standaarden. ASL staat voor Application Services Library en is een standaard voor de inrichting van Applicatiemanagement. BiSL staat voor Business Information Services Library en is een standaard voor Business Informatiemanagement<br><br>Daar waar ASL gaat over applicatiemanagement zoals beheer, onderhoud en vernieuwing van applicaties, behandelt BiSL onderwerpen op het gebied van functioneel beheer en informatiemanagement. |
| 11. Lifecycle management | Lifecycle Management is het beheren van de verschillende levenscycli waar een product zich in kan bevinden. Voorbeelden van levenscycli zijn onder andere Work-In-Progress (WIP), Review, en Released. |