SIDN'S SOURCING STRATEGY

Explanatory information

Date (last modified) 19 April 2024

Contents

1 Introduction

This memo provides explanatory information regarding SIDN's sourcing strategy. It describes Eraneos's involvement in a consultancy capacity, the stability and security assessment, SIDN's requirements and Eraneos's sourcing strategy advice.

The English-language version of this memo is a translation of an original Dutch-language text. In the event of any discrepancy between the two, the Dutch version will prevail.

2 About Eraneos

Eraneos (previously known as Quint) is a global Management & Technology Consultancy group that shapes the digital future of organizations. With our services and our industry leading experts, we help customers remain one step ahead with their digital challenges.
Sourcing advice is one of Eraneos's core services. We oversee more than 60 sourcing projects a year, focusing on sourcing strategy, selection, contracting and the implementation of sourcing governance. With a track record extending more than 25 years, we now have a team of roughly 100 expert sourcing and governance consultants active in the Netherlands. Eraneos advices independent of IT vendors and provides independent advice guided solely by the interests of its clients. Eraneos undertakes an annual survey of roughly 220 consumers, and is in continuous contact with roughly 40 IT vendors regarding current trends and market developments.

3 Background to the relationship between SIDN and Eraneos

3.1 Stability and security assessment

At the end of 2022, Eraneos (then known as Quint) carried out an assessment for SIDN with a view to advising on the technological status and currency of SIDN's core ICT systems. The main conclusions of that assessment are included in SIDN's 2022 Annual Report. The DNS systems are up-to-date, but the DRS registration system and the associated complex infrastructure are aging and approaching the stage where they should be replaced. Although reports show that the registration system delivers good uptime and performance to registrars, the associated administrative burden is high. As a result, teams are experiencing increased workloads and are unable to devote sufficient time to innovation. Moreover, the complexity of the environment implies a risk of over-dependence on individual knowledge-holders (key person risk).

3.2 Transition programme

On the basis of the assessment findings, Eraneos helped SIDN to set up and implement a transition programme aimed at providing a sound base for the organisational and technological changes necessary and appropriate for SIDN as an ‘Aanbieder Essentiële Diensten (AED)’ (‘essential service operator’).

The programme included the following elements:

- Formulation of an ICT strategy
- Formulation of architectural principles
- Exploration of DRS renewal options
- Formulation of a sourcing strategy
- Design of a communication and HR enablement work stream

This memo relates to the sourcing strategy formulation process. The associated report sets out Eraneos's advice to SIDN, for use in the context of vision formation and decision-making. Decision-making responsibility lies with SIDN.

4 SIDN's sourcing strategy

4.1 Scope: guidance of service landing zones

The purpose of a sourcing strategy is the formulation and maintenance of an optimal mix of internal and external services aligned with the organisation's objectives.
There are various generic sourcing models, including outsourcing, insourcing, external hire, shared service centre use and strategic collaboration. Like any strategy, a sourcing strategy serves as a guide, indicating how an optimal mix can support the realisation of objectives. As such, a sourcing strategy is more than a standalone set of (system) requirements: it embraces matters such as the implications for the organisation's working methods and structure.

The scope of SIDN's sourcing strategy was defined as the landing zones for the hosting of the DRS and associated applications, such as the Whois/RDAP and BrandGuard. In line with the stability and security assessment, it is appropriate that the DRS takes priority in that context. The examples given in this document therefore all relate to the DRS.

4.2 Approach: scenarios, requirements and vendors

The adopted approach involved the definition of 3 **scenarios** for the realisation of SIDN's objectives within the defined scope: public cloud, private cloud and on-premises. The scenarios were assessed in relation to SIDN's strategic requirements, leading to the identification of a preferred scenario. For each scenario, a number of vendors were assessed in relation to the functional and security requirements.

The **strategic criteria** are:

- Further enhancement of the resilience, availability and security of SIDN's services, and the reduction of latency
- Creation of space for the development of new services in the field of internet infrastructure security and data
- Contribution to Dutch and European digital autonomy and counteraction of internet centralisation (NL/EU-first sourcing strategy)
- Retention of SIDN's ability to attract the next generation of technical personnel, and to provide them with training in the field of internet infrastructure
- Enhancement of SIDN's agility and flexibility, and thus the organisation's capacity for innovation
- Assurance of SIDN's ongoing ability to use state-of-the-art ICT solutions
- Improvement of cost-efficiency

The **functional requirements** include:

- Managed databases, with the vendor assuring matters such as high DRS availability by means of the automatic replication of synchronised database copies and automatic generation of backups. This is required to enable SIDN to reduce its database management workload while assuring a suitably high level of availability.
- Strong support for everything as code, such as DRS documentation and configuration files for the automatic rollout of DRS components such as load balancers. The use of reproducible code will reduce the risk of errors and of dependence on individual knowledge-holders.
- Managed container orchestration (containerised/serverless computing) to give SIDN greater flexibility in terms of DRS workload start-up and transfer between environments and the ability to reserve resources (CPU, memory, etc) within environments to match variables such as the number of incoming EPP requests. This will enhance SIDN's ability to roll out DRS updates for registrars.
- Data encryption at rest and in transit. This is required for securing data in the DRS, both in storage and during transport across the internet or within a cloud or other environment.
- Managed observability: the ability to automatically monitor all activity from, to and within the DRS by means of services provided by the vendor,

and thus maintain a clear view of DRS performance. This will allow SIDN to further enhance the security and stability of the DRS and of the entire pathway from the registration to the publication of a domain name.

- Integrated security and compliance, enabling the vendor to provide SIDN with reports on DRS-related system events automatically and in real time. This capability is required to enable SIDN to meet increasingly exacting compliance requirements arising out of, for example, NIS2 and the Government Information Security Baseline.

Best practices must be supported to achieve and maintain compliance with such requirements. Best practices are specific, proven configuration guidelines and recommendations regarding architectural design, operational process design and security risk prevention. The availability of such information facilitates the swift and controlled initiation of appropriate change.

The **security requirements** that we apply to vendors relate to compliance with the following standards:

- EU Cloud CoC, EU Cloud Code of Conduct
- EU GDPR, EU General Data Protection Regulation (GDPR)
- EU Model Clauses, clauses relating to personal data associated with the GDPR
- ISO 27001, international information security management standard
- ISO 27017, Guidelines for information security controls applicable to the provision and use of cloud services
- ISO 27018, Guidelines for information security controls applicable to privacy in cloud services
- ISO 27701, Privacy extension to ISO/IEC 27001

SIDN wishes any vendor it uses to be demonstrably compliant with the main standards on (information) security and privacy. SIDN has ultimate responsibility for the provision of essential services and must therefore manage the risks associated with any party in the supply chain from whom services are procured or to whom services are outsourced.

The vendor list was drawn up over a number of review rounds and in accordance with SIDN's express wish that an adequate number of Dutch and other European vendors should be included:

- Public cloud: hyper-scalers and European variants. Within this scenario, there are no Dutch providers that satisfy the requirements to a sufficient extent to warrant inclusion.
- Private cloud: mix of Dutch and other European providers.

Assessment of the strategic requirements was made on the basis of Eraneos's knowledge of the scenarios, in dialogue with SIDN regarding applicability to the objectives. Assessment of the functional and security requirements was made on the basis of knowledge publicly available from websites or product/service catalogues, knowledge available within Eraneos, and targeted enquiries to vendors made by Eraneos.

4.3 Recommendation: public cloud is preferred scenario for the DRS

The advice given by Eraneos on the basis of the assessment is summarised below.

The **public cloud** scenario is the best means of enabling SIDN to meet its strategic objectives. A public cloud solution will give SIDN access to off-the-shelf, managed services, with the result that SIDN has to devote less time to the technical management of the DRS and is therefore able to focus on innovation. Public cloud providers provide extensive sets of best practices and make use of associated checklists and implementation blueprints. On the highly competitive technical labour market, the use of modern technology will help SIDN to remain attractive to upcoming talent.

Within the public cloud scenario, **Amazon Web Services (AWS)** is the best candidate. In view of the status of its existing ICT environment, SIDN requires a platform that is available immediately and offers extensive off-the-shelf functionalities, security and compliance.

Eraneos and SIDN discussed Eraneos's advice in depth, because following the advice will imply a major concession in relation to SIDN's objectives of contributing to the digital autonomy of the Netherlands and the EU and counteracting internet centralisation.

However, no Dutch or other European provider can satisfy a similar number of SIDN's requirements:

- Managed databases: available from some vendors, while others offer no specific solution or do not provide any relevant information.
- Strong support for everything as code: no specific solution available or offered only on a bespoke basis.
- Managed container/serverless: offered only on a bespoke basis or no service description available.
- Data encryption at rest and in transit: not available from all vendors or not of a comparable standard.
- Managed observability: depends on what services are procured and requires a bespoke service element.

- Integrated security: usually requires third-party involvement and bespoke services to enable integrated security for all services.

If SIDN chooses to use a Dutch or other European vendor or an on-premises solution, SIDN will remain dependent on a bespoke set-up and/or on the use of integration partners to connect the various services. In that case, some of the technical management of the generic infrastructure of the DRS and the related application would very probably have to remain in house, and SIDN will have to maintain direct oversight of multiple vendors.

Hence, while the scenario is not completely unviable, its adoption would require SIDN to make concessions on the majority of its objectives. Moreover, the lead times for change and innovation would be undesirably long.

SIDN Sourcing Strategy – landing zones

19 July 2023

Version 1.0

Contents

The English-language version of this report is a translation of an original Dutch-language text. In the event of any discrepancy between the two, the Dutch version will prevail.

Management summary

SIDN wants the technology that best fits its ambitions

ICT vision 2025
In 2023, SIDN formulated an ambitious ICT strategy and associated target architecture. The main strategic themes for ICT are (see slide 6): agility, modern technology, engineering culture and security by design. With a view to realising those objectives, SIDN wishes to make a number of key decisions in the period ahead regarding its organisational structure and the landing zones, i.e. the target platforms for landing the various applications. Each platform must enable the corresponding product team to quickly and easily test and develop existing and new applications. SIDN is committed to adopting proven, widely accepted products, tools and methods from the technology sector wherever possible.

From Ist to Soll landing zones
The current situation has been described largely on a schematic basis to provide a starting point for roadmaps aligned with the target architecture. The choice of appropriate landing zones involves strategic decision-making as to the extent to which SIDN should undertake its own technical management in the future. The considerations influencing the choice are set out in this sourcing strategy.

Possible scenarios
The sourcing strategy addresses the following 3 possible scenarios:

1. Public cloud
2. Private cloud
3. On-premises

The 3 scenarios have been assessed against a number of strategic criteria. In addition, an assessment has been made of the functionalities and security features provided by various public and private cloud vendors. Finally, supporting general information is provided regarding the public cloud vendors.

Eraneos advises carefully considered migration to the public cloud

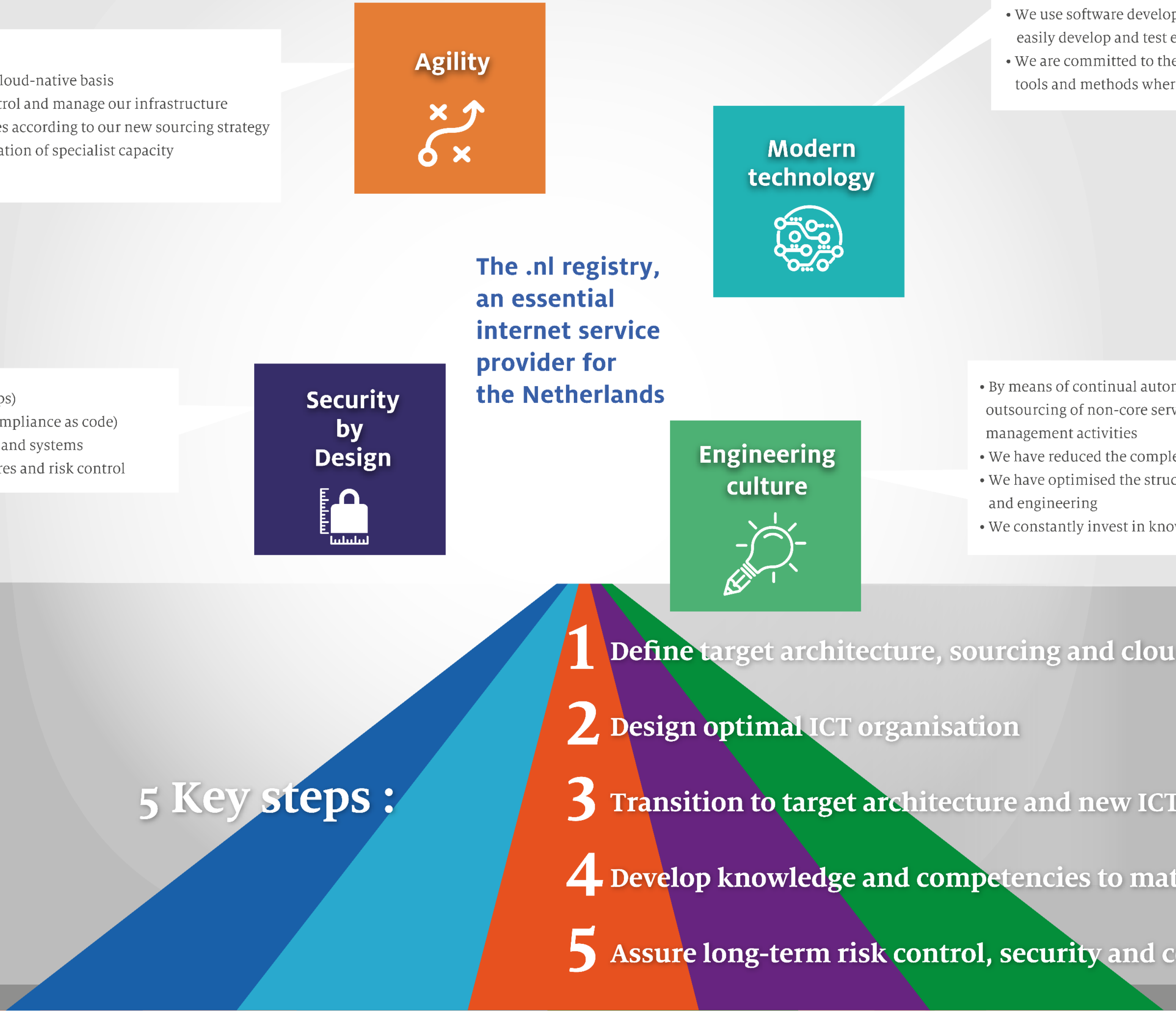
Public cloud is preferable
The strategic assessment identified the public cloud scenario as preferable. The large number of services available from public cloud vendors will relieve SIDN's technical management burden, thus enabling it to focus on innovation. The one trade-off for SIDN is compromising on its desire to play exemplary role in relation to the NL/EU-first strategy. SIDN might therefore consider the possibility of contributing to the further development of EU cloud initiatives, such as Gaia-X.

AWS is the best candidate, but not without risk
Within the public cloud domain, AWS is the best candidate. Although the differences are not enormous, AWS is the market leader and, as such, has the widest palette of services and the highest level of innovation. However, the use of AWS would not be without risk. SIDN currently lacks technical personnel familiar with the platform. External support will therefore be necessary for landing zone design and acquisition of the knowledge required to implement migration.

Careful consideration required
In this sourcing strategy, we present a cloud model for SIDN that is more than simply a cloud-first approach. We assume a 'PaaS-unless' approach for core and ambition, and an 'SaaS-unless' approach for all supporting applications. However, in every instance, the decision to use the cloud must be tested against: (a) the results of the business impact analysis (BIA) covering matters such as availability, (b) all relevant non-functional requirements such as performance and latency requirements, and (c) the generic sourcing principles guiding the choice between insourcing and outsourcing.

Roadmap to implementation
This sourcing strategy provides SIDN with a starting point for further development of a roadmap for all SIDN's ICT services and for implementation preparations. In that context, it is important not only to develop an architectural design, but also to build up internal knowledge and competences, so that SIDN has both appropriate technological expertise in house to maintain control of landscape operation, and the control competences required to, for example, manage the complex financial models in the cloud. Finally, it is advisable to develop the sourcing strategy further, to cover the management and implementation of other services, such as office IT, printing and telephony. That will provide structure and direction for the period ahead.

ICT strategy 2023-2025



Agility

- Our ICT systems support agile working
- We design and develop our applications on a modular, cloud-native basis
- We use the infrastructure-as-code (IaC) principle to control and manage our infrastructure
- We select and procure our ICT infrastructure and services according to our new sourcing strategy
- We take a dynamic, team-based approach to the organisation of specialist capacity
- The technology stack is further standardised

Modern technology

- We use software development and release platforms that enable us to quickly and easily develop and test existing and new applications
- We are committed to the use of proven, widely accepted technology sector products, tools and methods wherever possible

The .nl registry, an essential internet service provider for the Netherlands

Security by Design

- Responsibility for security lies with the teams (DevSecOps)
- We invest in process automation and IT controls (e.g. compliance as code)
- We make maximum use of intrinsically secure products and systems
- We have an organisation-wide focus on security, measures and risk control

Engineering culture

- By means of continual automation and maximum use of cloud services and the outsourcing of non-core service where possible, we have greatly reduced our management activities
- We have reduced the complexity and diversity of our IT landscape
- We have optimised the structure of our ICT organisation for product development and engineering
- We constantly invest in knowledge and culture through recruitment and training

5 Key steps :

1 Define target architecture, sourcing and cloud strategy

2 Design optimal ICT organisation

3 Transition to target architecture and new ICT organisation

4 Develop knowledge and competencies to match objectives

5 Assure long-term risk control, security and compliance within ICT

Scope

Scope

Landing zones and additional services

The scope of this sourcing strategy is landing zones and additional services:

- Landing zones are environments in which applications are hosted (on-site, IaaS, PaaS, SaaS), also referred to as target platforms.
- Additional services are management services for such environments (security, database management, disaster recovery, etc).

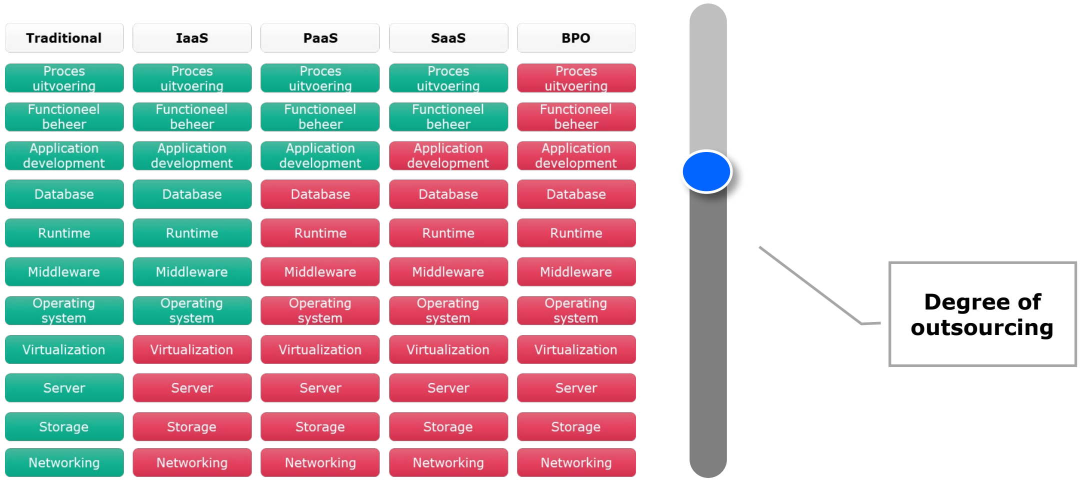
The primary focus of the sourcing strategy is the landing zone for the DRS. The document also provides generic advice regarding landing zones for other applications.

The following services and activities are out of scope:

- Execution of business processes
- Functional application management
- Landing zone(s) for services in the SIDN Labs and SOC domains
- All other IT management services for office ICT systems (e.g. printing, telephony, workplace management).

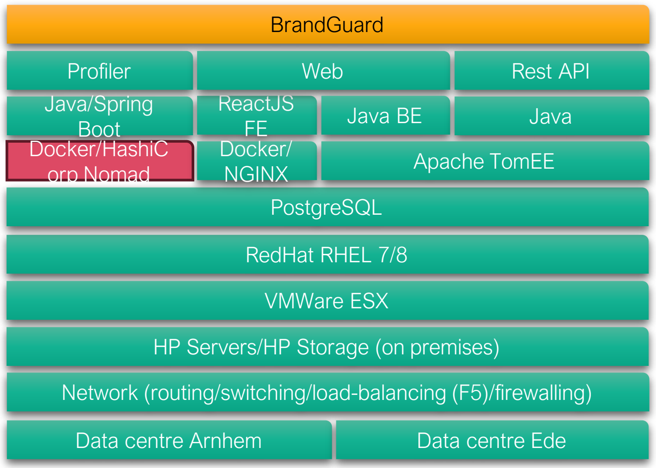
The diagrams opposite provide a general impression of the extent of outsourcing (top) and an illustrative example of the current make-up of an SIDN service (below). See appendix for additional detail.

The diagram on the following slide provides a full sourcing overview of SIDS's IT environment and the associated scope.



Traditional	IaaS	PaaS	SaaS	BPO
🟩 Proces uitvoering	🟩 Proces uitvoering	🟩 Proces uitvoering	🟩 Proces uitvoering	🟥 Proces uitvoering
🟩 Functioneel beheer	🟩 Functioneel beheer	🟩 Functioneel beheer	🟩 Functioneel beheer	🟥 Functioneel beheer
🟩 Application development	🟩 Application development	🟩 Application development	🟥 Application development	🟥 Application development
🟩 Database	🟩 Database	🟥 Database	🟥 Database	🟥 Database
🟩 Runtime	🟩 Runtime	🟥 Runtime	🟥 Runtime	🟥 Runtime
🟩 Middleware	🟩 Middleware	🟥 Middleware	🟥 Middleware	🟥 Middleware
🟩 Operating system	🟩 Operating system	🟥 Operating system	🟥 Operating system	🟥 Operating system
🟩 Virtualization	🟥 Virtualization	🟥 Virtualization	🟥 Virtualization	🟥 Virtualization
🟩 Server	🟥 Server	🟥 Server	🟥 Server	🟥 Server
🟩 Storage	🟥 Storage	🟥 Storage	🟥 Storage	🟥 Storage
🟩 Networking	🟥 Networking	🟥 Networking	🟥 Networking	🟥 Networking

Degree of outsourcing



BrandGuard

Profiler | Web | Rest API

Java/Spring Boot | ReactJS FE | Java BE | Java

🟥 Docker/HashiCorp Nomad | Docker/ NGINX | Apache TomEE

PostgreSQL

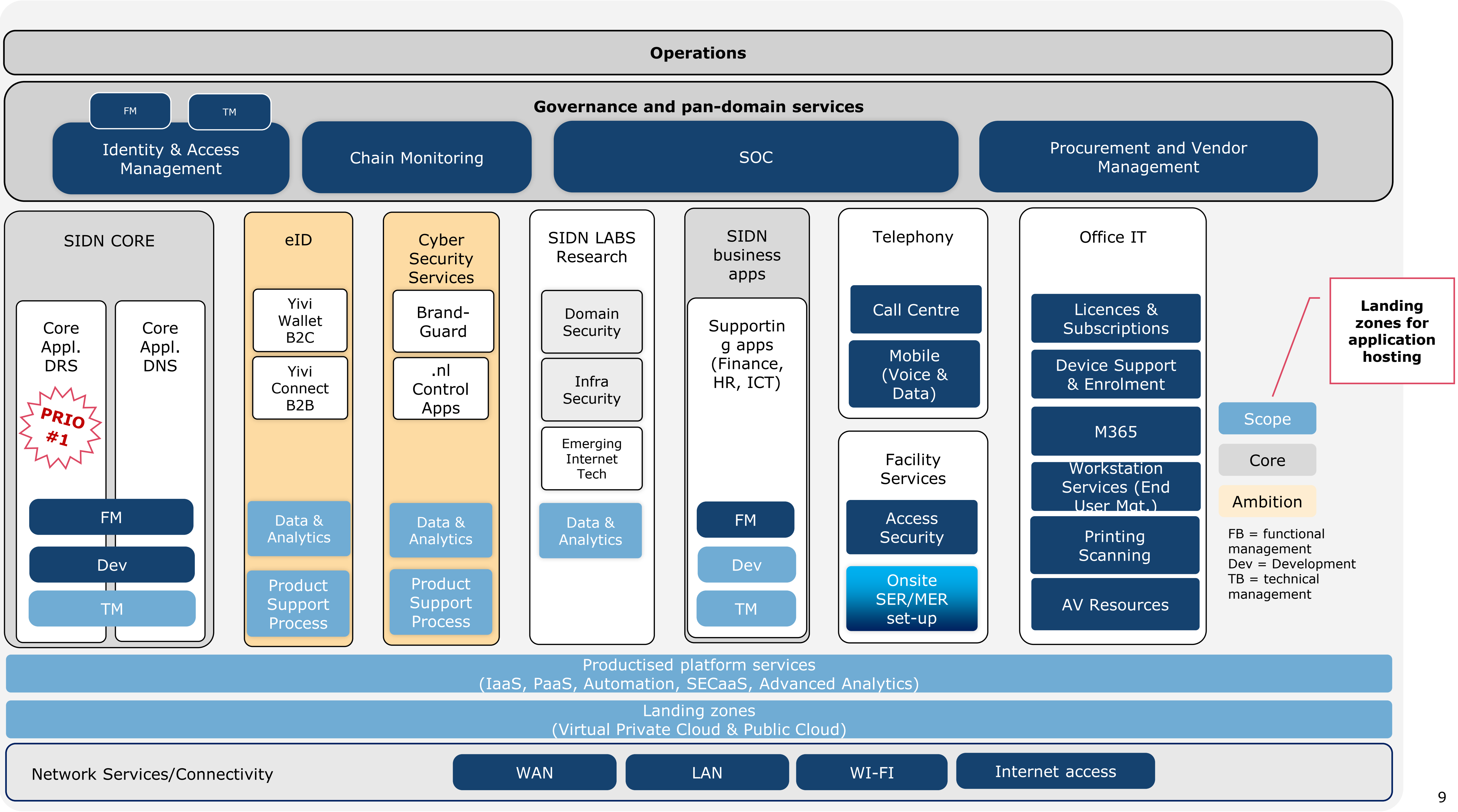
RedHat RHEL 7/8

VMWare ESX

HP Servers/HP Storage (on premises)

Network (routing/switching/load-balancing (F5)/firewalling)

Data centre Arnhem | Data centre Ede



Operations

Governance and pan-domain services

FM

TM

Identity & Access Management

Chain Monitoring

SOC

Procurement and Vendor Management

SIDN CORE

Core Appl. DRS

PRIO #1

Core Appl. DNS

FM

Dev

TM

eID

Yivi Wallet B2C

Yivi Connect B2B

Data & Analytics

Product Support Process

Cyber Security Services

Brand-Guard

.nl Control Apps

Data & Analytics

Product Support Process

SIDN LABS Research

Domain Security

Infra Security

Emerging Internet Tech

Data & Analytics

SIDN business apps

Supporting apps (Finance, HR, ICT)

FM

Dev

TM

Telephony

Call Centre

Mobile (Voice & Data)

Facility Services

Access Security

Onsite SER/MER set-up

Office IT

Licences & Subscriptions

Device Support & Enrolment

M365

Workstation Services (End User Mgt.)

Printing Scanning

AV Resources

Landing zones for application hosting

Scope

Core

Ambition

FB = functional management
Dev = Development
TB = technical management

Productised platform services
(IaaS, PaaS, Automation, SECaaS, Advanced Analytics)

Landing zones
(Virtual Private Cloud & Public Cloud)

Network Services/Connectivity

WAN

LAN

WI-FI

Internet access

Current sourcing model

Current sourcing model

In-house technical management

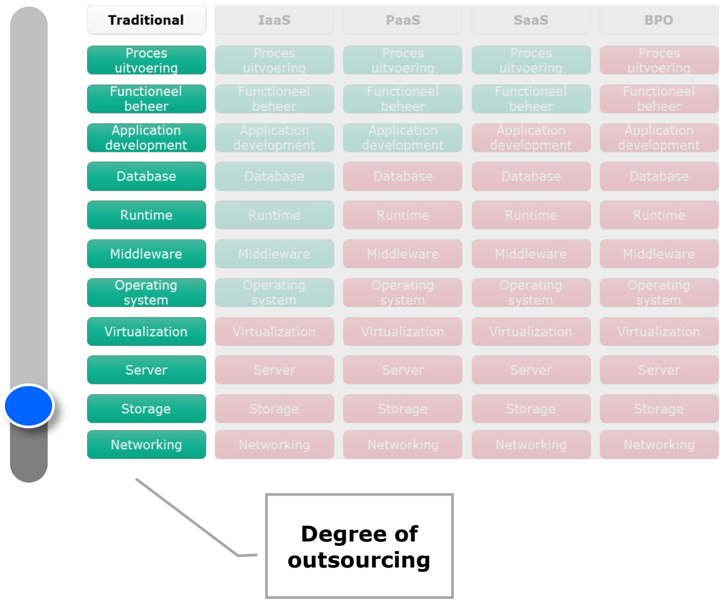
SIDN currently manages most of the technology stack for the DRS and the majority of supporting services in house. In practice, that broadly implies undertaking the following activities:

- Contracting co-location at data centres
- Managing network layer to the data centres
- Procurement of server hardware and licences, e.g. for virtualisation and databases
- Technical management of environments (servers, databases, etc)
- Technical management of applications (patches, releases, etc)
- All service management tasks, e.g. incident, problem, change, capacity and financial management

Some as-a-service procurement

SIDN procures certain things on an as-a-service basis, including Microsoft 365 office software (SaaS), DNS anycast landing zone (BMaaS*), data platform (Azure Datafactory), logo detection for BrandGuard (GPC).

The use of outsourcing in such cases is not based on a pre-defined sourcing strategy or outsourcing policy.



Traditional	IaaS	PaaS	SaaS	BPO
Proces uitvoering	Proces uitvoering	Proces uitvoering	Proces uitvoering	Proces uitvoering
Functioneel beheer	Functioneel beheer	Functioneel beheer	Functioneel beheer	Functioneel beheer
Application development	Application development	Application development	Application development	Application development
Database	Database	Database	Database	Database
Runtime	Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware	Middleware
Operating system	Operating system	Operating system	Operating system	Operating system
Virtualization	Virtualization	Virtualization	Virtualization	Virtualization
Server	Server	Server	Server	Server
Storage	Storage	Storage	Storage	Storage
Networking	Networking	Networking	Networking	Networking

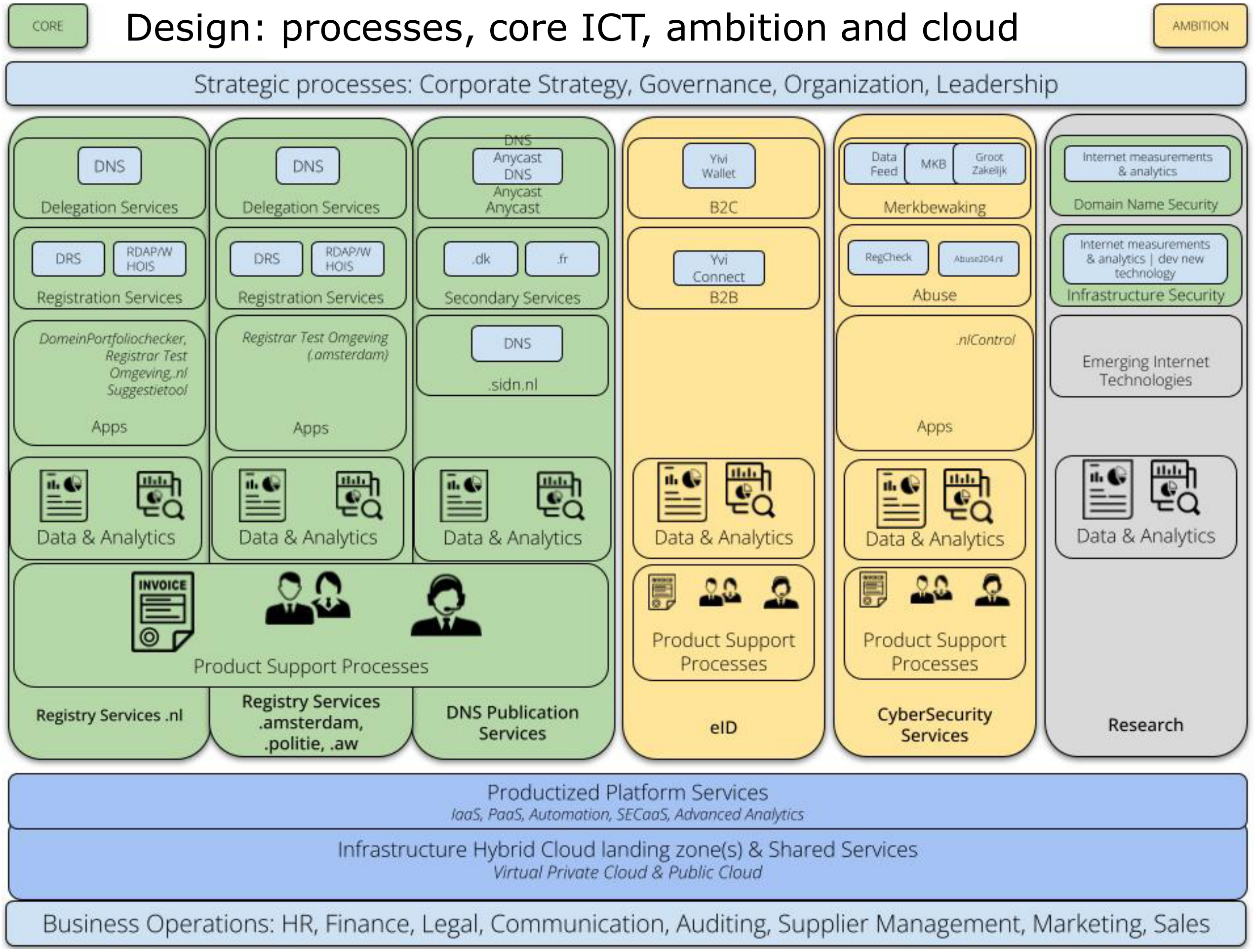
Degree of outsourcing

*Bare metal as a service for extremely critical DNS processes

Sourcing principles

Core, ambition and supporting applications
Criticality and non-functional requirements
Generic sourcing principles

Core, ambition and supporting applications



CORE

Design: processes, core ICT, ambition and cloud

AMBITION

Strategic processes: Corporate Strategy, Governance, Organization, Leadership

Registry Services .nl: DNS — Delegation Services; DRS, RDAP/WHOIS — Registration Services; *DomeinPortfoliochecker, Registrar Test Omgeving,.nl Suggestietool* — Apps; Data & Analytics

Registry Services .amsterdam, .politie, .aw: DNS — Delegation Services; DRS, RDAP/WHOIS — Registration Services; *Registrar Test Omgeving (.amsterdam)* — Apps; Data & Analytics

DNS Publication Services: DNS Anycast DNS Anycast — Anycast; .dk, .fr — Secondary Services; DNS — .sidn.nl; Data & Analytics

INVOICE — Product Support Processes

eID: Yivi Wallet — B2C; Yivi Connect — B2B; Data & Analytics; Product Support Processes

CyberSecurity Services: Data Feed, MKB, Groot Zakelijk — Merkbewaking; RegCheck, Abuse204.nl — Abuse; *.nlControl* — Apps; Data & Analytics; Product Support Processes

Research: Internet measurements & analytics — Domain Name Security; Internet measurements & analytics | dev new technology — Infrastructure Security; Emerging Internet Technologies; Data & Analytics

Productized Platform Services
IaaS, PaaS, Automation, SECaaS, Advanced Analytics

Infrastructure Hybrid Cloud landing zone(s) & Shared Services
Virtual Private Cloud & Public Cloud

Business Operations: HR, Finance, Legal, Communication, Auditing, Supplier Management, Marketing, Sales

Distinction between 'core' and 'ambition'
SIDN's core IT services, labelled 'Core', with the corresponding research fields (Domain Name Security & Infrastructure Security) such as domains, processes and technology are distinguished from eID and cybersecurity services, which are labelled 'Ambition'. Distinction is made so that continuity, availability, innovation and development of core IT services are always assured.

Supporting applications
Supporting applications are business applications used to perform business processes, such as HR, finance, communication, auditing, marketing and sales. The '"IT4IT' tooling for DevOps, productivity and observability fall under this heading as well. Finally, the (planned) data platform, is also a supporting business application. Each of those applications has its own landing zone and sourcing model.

Absolute condition: design a cloud-agnostic transition
SIDN should use a platform services layer to support the cloud technology transition and to enable the use of landing zones on a cloud-agnostic basis as far as possible. That will also enable the possible future migration of SIDN's application landscape from one provider to another.

Criticality and functionality

BIA

The business impact analyse (BIA) provides insight into the criticality of each application. An application's criticality normally forms the basis for the requirements regarding availability, integrity and confidentiality (and sometimes privacy), with maximum data loss as a component. The landing zone must fulfil the BIA-derived requirements.

Non-functional requirements

In addition to the BIA-derived requirements, numerous non-functional requirements may apply. Non-functional requirements relate to the quality of an application, in contrast to functional requirements, which relate to the application's properties and capabilities.

Examples of non-functional requirements include: performance, scalability, convenience, latency, etc. As well as satisfying the BIA-derived requirements, the choice of landing zone for each application must take adequate account of the application-specific non-functional requirements.

Criticality levels

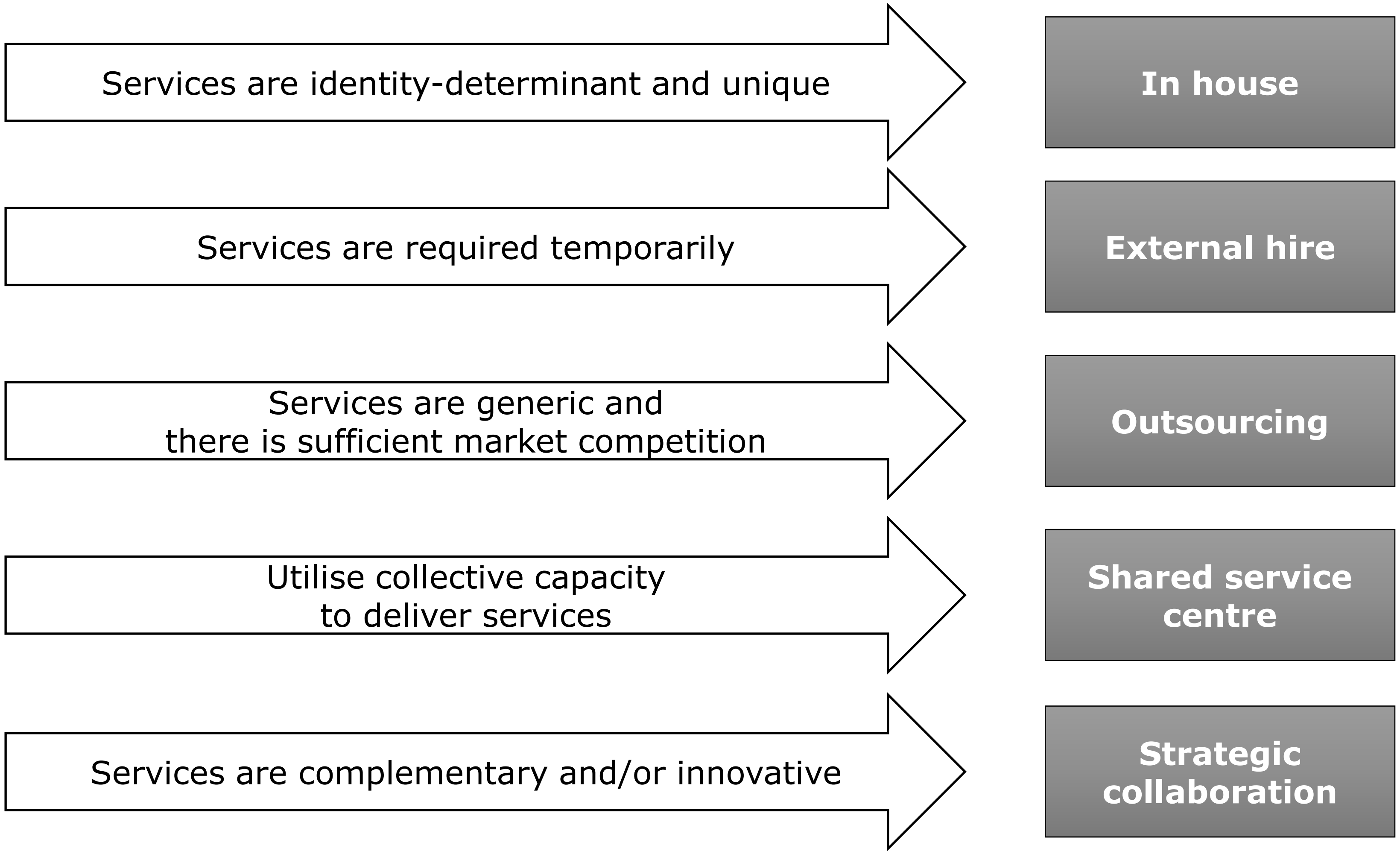
The following summary is an interpretation based on the most recent available BIAs*.

Information system/process	Loss of exclusivity	Loss of integrity	Loss of availability
DNS	E	A	B – 1 hour A – 8 hours
DRS	A	A	C – 8 hours A – 1 week
Whois/public Is	D	C	D – 8 hours C – 1 week B – 1 month
Whois/Registrar Is	C	C	C – 4 hours B – 8 hours A – 1 week
Office automation	C	C	D - 1 hour C – 4 hours B – 8 hours A – 1 week
BrandGuard	B	B	E – 4 hours D – 8 hours C – 1 week B – 1 month
eID	B	C	E – 8 hours C – 1 week B – 1 month

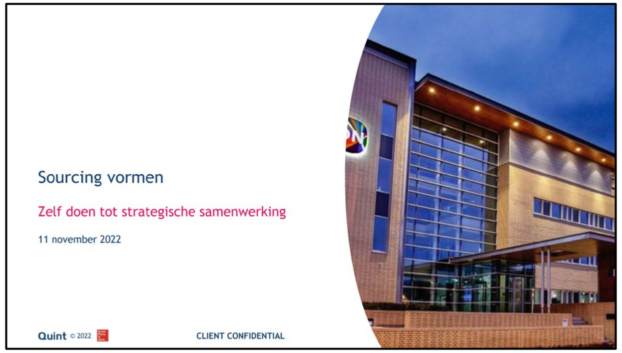
A – Threat to business continuity
B – Very serious impact
C – Significant impact
D – Minor impact
E – Critical impact

*See BIA summary. See also roadmap and other advisory reports on the modernity and market conformity of the existing BIAs.

Generic sourcing principles



Services are identity-determinant and unique	In house
Services are required temporarily	External hire
Services are generic and there is sufficient market competition	Outsourcing
Utilise collective capacity to deliver services	Shared service centre
Services are complementary and/or innovative	Strategic collaboration



Sourcing vormen

Zelf doen tot strategische samenwerking

11 november 2022

Quint ©2022

CLIENT CONFIDENTIAL

See options per sourcing form previously identified by Eraneos and appended to this document.

Scenarios

Introduction: scenarios, criteria and vendors

Introduction: scenarios, criteria and vendors

Scenarios
In this sourcing strategy, we compare 3 scenarios:

1. Public cloud
2. Private cloud
3. On-premises

Scenario descriptions
A brief general description of each scenario is provided. The 3 scenarios are also assessed against a number of strategic criteria defined at a workshop. Finally, the main advantages of and risks associated with each scenario are outlined.

Vendors
For scenarios 1 and 2, a selection of vendors is appraised. For scenario 1, the major public cloud vendors are Amazon Web Services (AWS), …. For scenario 2, the selection includes Dutch, other European and non-European private cloud providers. For scenario 3, no vendors were appraised, since the limited service requirement means that no major differentiation is expected.

Scenario 1: public cloud offers access to numerous services

Scenario 1: Public cloud

General scenario description

This scenario involves SIDN opting to use a public cloud vendor and finding a (temporary) partner to supervise the transition (see section on roadmap). In this scenario, SIDN has access to the latest technologies and a wide range of managed services.

SIDN becomes a service integrator:

- Oversight of architectural principles and integration across domains
- Infra-as-code management assigned to DevOps teams
- Management of partner and cloud vendor contracts

Advantages of this scenario

- Less risk of vendor lock-in, providing that standard technology is chosen and a cloud-agnostic design is used
- Access to the latest technologies
- Wide selection of managed added-value services
- Global coverage achieved by distribution across numerous regions
- Partnerships with leading organisations

Risks associated with this scenario

- Operational problems due to lack of specific technical familiarity with the solution
- Higher costs due to lack of familiarity with complex pricing models
- Departure of existing personnel who do not support the change

Impact of the scenario on strategic objectives	Evaluation*
Further enhancement of the resilience, availability and security of SIDN's services, and the reduction of latency	+
Creation of space for the development of new services in the field of internet infrastructure security and data	+
Contribution to Dutch and European digital autonomy and counteraction of internet centralisation (NL/EU-first sourcing strategy)	-
Retention of SIDN's ability to attract the next generation of technical personnel, and to provide them with training in the field of internet infrastructure	+
Enhancement of SIDN's agility and flexibility, and thus the organisation's capacity for innovation	+
Assurance of SIDN's ongoing ability to use state-of-the-art ICT solutions	+
Improvement of cost-efficiency	+

*See details and notes on slide 21.

Scenario 2: private cloud for self-managed modernisation

Scenario 2: Private cloud

General scenario description

This scenario involves SIDN opting to use and contracting a private cloud vendor. The service provider guides SIDN through the transformation and implementation processes for the chosen private cloud environment. In this scenario, SIDN has less access to new technologies than in the public cloud scenario, and remains responsible for certain management tasks.

SIDN collaborates with a service provider:

- Managing contracts and service levels
- Performing certain management tasks and arranging handovers and alignment
- Working with the service provider to identify development opportunities for open-source applications (e.g. Terraform and PostgreSQL), Infra-as-code and so on.

Advantages of this scenario

- Direct access to the service provider's knowledge and skill
- Service provider exchanges ideas with SIDN and is involved in delivery of SIDN's services
- SIDN has a fixed point of contact and ability to specify the extent of the services
- Vendor is typically less remote
- Bespoke solutions possible

Risks associated with this scenario

- Service provider determines whether innovative solutions are adopted and at what speed
- Risk of vendor lock-in due to service provider's use of dedicated management tools
- Less scope for procurement of additional management services
- With a Dutch service provider: continuity risk due to smaller client base and investment capability
- Smaller pool of qualified personnel within service provider's organisation

Impact of the scenario on strategic objectives	Evaluation*
Further enhancement of the resilience, availability and security of SIDN's services, and the reduction of latency	-
Creation of scope for the development of new services in the field of internet infrastructure security and data	-
Contribution to Dutch and European digital autonomy and counteraction of internet centralisation (NL/EU-first sourcing strategy)	+
Retention of SIDN's ability to attract the next generation of technical personnel, and to provide them with training in the field of internet infrastructure	-
Enhancement of SIDN's agility and flexibility, and thus the organisation's capacity for innovation	+/-
Assurance of SIDN's ongoing ability to use state-of-the-art ICT solutions	+/-
Improvement of cost-efficiency	+/-

*See details and notes on slide 21.

Sourcing scenarios

Scenario 3: invest and manage yourself

Scenario 3: On-premises

General scenario description

This scenario involves SIDN retaining its existing sourcing model and continuing to use its existing data centres. SIDN is responsible for scaling and modernising infrastructure components to enable the use of innovative solutions.

SIDN makes upgrades and retains the role of technical manager:

- Investment in new hardware / data centre required to enable technological developments.
- Investment required in order to achieve and maintain appropriate levels of service management quality (incident, problem and change management, etc).

Advantages of this scenario

- Ability to continue using existing tooling and contracts
- No platform dependencies
- Full control with regard to digital autonomy and sovereignty

Risks associated with this scenario

- Inability to provide the necessary level of management quality
- Priority given to technical management, delaying innovation and DRS/Fury upgrade
- Key person risk, reducing prompt fault resolution capability
- Project delays due to periodic updates, refreshes and replacements

Impact of the scenario on strategic objectives	Evaluation*
Further enhancement of the resilience, availability and security of SIDN's services, and the reduction of latency	-
Creation of scope for the development of new services in the field of internet infrastructure security and data	-
Contribution to Dutch and European digital autonomy and counteraction of internet centralisation (NL/EU-first sourcing strategy)	+
Retention of SIDN's ability to attract the next generation of technical personnel, and to provide them with training in the field of internet infrastructure	-
Enhancement of SIDN's agility and flexibility, and thus the organisation's capacity for innovation	+/-
Assurance of SIDN's ongoing ability to use state-of-the-art ICT solutions	+/-
Improvement of cost-efficiency	+/-

*See details and notes on slide 21.

Notes on strategic criteria

Strategic criterion	Scenario 1: Public cloud	Scenario 2: Private cloud	Scenario 3: On-premises	Winner
Further enhancement of the resilience, availability and security of SIDN's services, and the reduction of latency	Access to market best practices, but always service-oriented and less infra-oriented. SLA is a contract.	Requires more direct management, less access to market best practices.	Requires more direct management, with almost no access to market best practices.	1
Creation of scope for the development of new services in the field of internet infrastructure security and data	Access to numerous out-of-the box services, releasing capacity for core business and innovation.	Less access to out-of-the box services than in the public cloud scenario.	Almost no access to out-of-the box services.	1
Contribution to Dutch and European digital autonomy and counteraction of internet centralisation (NL/EU-first sourcing strategy)	No public cloud vendors are NL/EU entities.	Possible vendors include NL, EU and non-EU entities.	With a Dutch co-location solution, full control retained.	3
Retention of SIDN's ability to attract the next generation of technical personnel, and to provide them with training in the field of internet infrastructure	Next generation wants modern technology and a matching engineering culture.	Fits more traditional forms of management.	Fits more traditional forms of management.	1
Enhancement of SIDN's agility and flexibility, and thus the organisation's capacity for innovation	Public cloud vendors are well resourced and can often offer out-of-the box solutions.	Depending on client base size, vendors are less well resourced and consequently offer fewer out-of-the-box features.	Considerable time will still have to be invested in traditional management.	1
Assurance of SIDN's ongoing ability to use state-of-the-art ICT solutions	Public cloud vendors are far better resourced for developments, integrations and incorporation of innovative players.	Modernisation of solutions depends on access to resources (people, capital).	Complete freedom to seek out state-of-the-art solutions.	1
Improvement of cost-efficiency	Solutions are scalable, and upscaling is consequently very easy.	Less scalability than in the public cloud scenario.	Less scalability than in the other scenarios.	1

Placeholder – TCO as is / cost drivers

To be completed

Outsourcing and cloud services always involve generic risks

Strategic risks
Services are no longer aligned with strategy or with operational and financial requirements

Compliance risks
Services no longer comply with applicable legislation or regulations.

Collaboration risks
Communication and collaboration is sub-optimal.

Portfolio risks
Services are not (any longer) provided on the basis of agreed service levels or specifications.

Commercial risks
Vendor behaviour or services result in increased or unpredictable costs.

Coordination risks
Complexity of contracts, services and vendors causes overheads, waste and/or inflexibility.

An effective control organisation is necessary for mitigation of those risks
(see roadmap).

Vendors

Candidate profiles
Vendor comparison – functional & technical
Gartner quadrants
General appraisal
User satisfaction with public cloud providers

Candidate profiles*

AWS

- Provides public cloud services in 31 regions and offers more than 200 services.
- AWS leads the way in terms of the introduction and early adoption of new technologies.

Azure

- Azure offers 200 cloud services from 60+ regions.
- Provides consistent hybrid cloud services and has an extensive compliance framework.

GCP

- The Google Cloud Platform is available in 37 regions with 100+ cloud services.
- Google is more popular with small and medium-sized organisations.

*Vendor comparison – functional & technical

SIDN vendor comparison																				
	Public cloud												Private cloud							
Criterion		AWS		Azure		GCP														
Functional																				
Worldwide coverage	🟢		🟢		🟢		🟡	Limited to EU	🟡	Limited to EU	🟢		🟢		🟠	Limited to NL	🟠	Limited to NL	🟢	
Scope of services	🟢		🟡	Fewer services than AWS	🟠	Fewer services than AWS or Azure	🟠	Fewer services than AWS, Azure or GCP	🟠	Fewer services than AWS, Azure, GCP or Scaleway	🟠	Fewer services than AWS, Azure or GCP	🟠	Fewer services than AWS, Azure or GCP	🟠	Fewer services than AWS, Azure or GCP	🟠	Fewer services than AWS, Azure or GCP	🟠	Fewer services than AWS, Azure or GCP
Sustainability	🟢		🟢		🟢		🟢		🟢		🟢		🟢		🟢		🟢		🟢	
Data encryption at rest and in transit	🟢		🟢		🟢		🟢		🟢		🟡	Does not currently offer KMS as a service; client cannot bring own keys; KMIP is managed by vendor	🟢		🟢		🟢		🟢	
Managed database (PostgreSQL, MySQL, SQL server)	🟢		🟢		🟢		🟢		🟡	No info available	🟢		🟡	No specific solution	🟢		🟡	No specific solution	🟢	
AM solution (Azure AD) for authentication	🟡	No direct integration	🟢		🟡	No direct integration	🟡	No info available	🟡	No info available	🟡	No info available	🟡	No direct integration	🟡	No direct integration	🟡	No info available	🟢	
Infrastructure as code	🟢		🟢		🟢		🟢		🟡	No info available	🟢		🟢		🟡	Bespoke solution	🟡	Bespoke solution	🟢	
Terrafrom infra-as-code support	🟢		🟢		🟢		🟢		🟢		🟢		🟢		🟠	Not listed as partner	🟠	Not listed as partner	🟠	Not listed as partner
Configurability and possibility to automate operations	🟢		🟢		🟢		🟢		🟢		🟢		🟢		🟢		🟢		🟢	
Containerised os serverless	🟢		🟢		🟢		🟢		🟢		🟢		🟡	No specific solution	🟡	Bespoke solution	🟡	No info available	🟡	No specific solution
Everything as code (including app configuration, etc)	🟢		🟢		🟢		🟢		🟡	No info available	🟢		🟡	No specific solution	🟡	Bespoke solution	🟡	No info available	🟡	No specific solution
Automated deployment	🟢		🟢		🟢		🟢		🟡	No specific solution	🟡	Supported by web hosting	🟡	No specific solution	🟡	No specific solution	🟡	No specific solution	🟡	No specific solution
Observability	🟢		🟢		🟢		🟢		🟡	No info available	🟡	Only log management	🟡	Observability options vary according to services and configurations	🟡	Observability options vary according to services and configurations	🟡	Observability options vary according to services and configurations	🟡	Observability options vary according to services and configurations
HSM (key management)	🟢		🟢		🟢		🟡	No info available	🟡	No info available	🟡	No info available	🟢		🟡	Bespoke solution	🟡	No info available	🟡	No info available
Load-balancer SaaS	🟢		🟢		🟢		🟢		🟢		🟢		🟢		🟡	Bespoke solution	🟡	No info available	🟢	
DDoS protection	🟢		🟢		🟢		🟢		🟢		🟢		🟢		🟢		🟢		🟢	
Disaster recovery	🟢		🟢		🟢		🟢		🟢		🟢		🟢		🟢		🟢		🟢	
Ransomware protection	🟢		🟢		🟢		🟢		🟢		🟢		🟢		🟢		🟢		🟢	
Security																				
EU Cloud CoC	🟠	Not listed as partner	🟢		🟢		🟠	Not listed as partner	🟢		🟠	Not listed as partner	🟠	Not listed as partner	🟠	Not listed as partner	🟠	Not listed as partner	🟠	Not listed as partner
EU GDPR	🟢		🟢		🟢		🟡	No info available	🟢		🟢		🟢		🟢		🟢		🟢	
EU model clauses	🟢		🟢		🟢		🟡	No info available	🟢		🟢		🟢		🟢	Not necessary (in NL)	🟢		🟢	
ISO 27001	🟢		🟢		🟢		🟡	No info available	🟢		🟢		🟢		🟢		🟢		🟢	
ISO 27017	🟢		🟢		🟢		🟡	No info available	🟢		🟢		🟢		🟠	Not on certificate	🟢		🟢	
ISO 27018	🟢		🟢		🟢		🟡	No info available	🟢		🟢		🟢		🟠	Not on certificate	🟠	Not on certificate	🟢	
ISO 27701	🟢		🟢		🟢		🟡	No info available	🟢		🟢		🟢		🟠	Not on certificate	🟠	Not on certificate	🟢	

*Vendor comparison – strategic -2

SIDN vendor comparison

	Public cloud						Private cloud			
Criterion	AWS	Azure	GCP							
Strategic										
Further enhancement of the resilience, availability and security of SIDN's services, and the reduction of latency	🟢	🟢	🟢	🟡 Fewer features than AWS/Azure/GDP; limited global data centre availability	🟡 Fewer features than AWS/Azure/GDP; limited global data centre availability	🟢	🟡 Fewer features than public cloud	🟡 Requires more in-house management, offers less access to market best practices	🟡 Requires more in-house management, offers less access to market best practices	🟡 Fewer features than public cloud
Creation of scope for the development of new services in the field of internet infrastructure security and data	🟢	🟢	🟢	🟡 Limited scope	🟡 Limited scope, but partner solutions offer ample scope outside vendor's ecosystem	🟡 Fewer out-of-the-box solutions than AWS/Azure/GWP	🟡 Fewer out-of-the-box solutions than public cloud	🟡 Fewer out-of-the-box solutions than public cloud	🟡 Fewer out-of-the-box solutions than public cloud	🟡 Fewer out-of-the-box solutions than public cloud
Contribution to Dutch and European digital autonomy and counteraction of internet centralisation (NL/EU-first sourcing strategy)	🟡 Not NL/EU-first	🟡 Not NL/EU-first	🟡 Not NL/EU-first	🟢	🟢	🟢	🟡 Not NL/EU-first	🟢	🟢	🟢
Retention of SIDN's ability to attract the next generation of technical personnel, and to provide them with training in the field of internet infrastructure	🟢	🟢	🟢	🟡 More limited than AWS/Azure/GWP certified engineers	🟡 More limited than AWS/Azure/GWP certified engineers	🟡 More limited than AWS/Azure/GWP certified engineers	🟡 More suitable for traditional forms of management	🟡 More suitable for traditional forms of management	🟡 More suitable for traditional forms of management	🟡 More suitable for traditional forms of management
Enhancement of SIDN's agility and flexibility, and thus the organisation's capacity for innovation	🟢	🟢	🟢	🟡 Availability of innovative technology/services less certain than with AWS/Azure/GWP	🟡 Availability of innovative technology/services less certain than with AWS/Azure/GWP	🟡 Availability of innovative technology/services less certain than with AWS/Azure/GWP	🟡 Fewer out-of-the-box solutions than public cloud	🟡 Some services require in-house management; dependent on NL investment	🟡 Some services require in-house management; dependent on NL investment	🟡 Fewer out-of-the-box solutions than public cloud
Assurance of SIDN's ongoing ability to use state-of-the-art ICT solutions	🟢	🟢	🟢	🟡 Less state-of-the-art than AWS/Azure/GWP	🟡 Less state-of-the-art than AWS/Azure/GWP	🟡 Less state-of-the-art than AWS/Azure/GWP	🟡 Less state-of-the-art than public cloud	🟡 Modernisation dependent on NL investment	🟡 Modernisation dependent on NL investment	🟡 Less state-of-the-art than public cloud
Improvement of cost-efficiency	🟢	🟢	🟢	🟡 Some scope, but limited by lack of supporting services	🟡 Some scope, but limited by lack of supporting services	🟡 Some scope, but limited by lack of supporting services	🟡 Less scalable than public cloud	🟡 Limited scalability	🟡 Limited scalability	🟡 Less scalable than public cloud

This information has been deleted for copyright reasons.

This information has been deleted for copyright reasons.

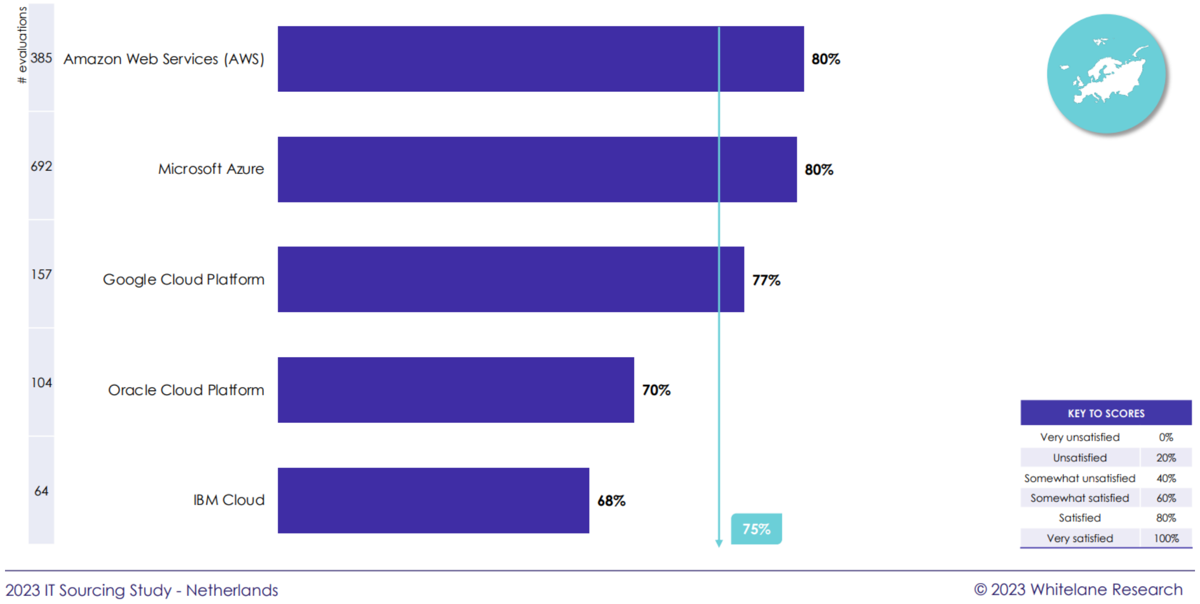
General appraisal of AWS | Azure | GCP

	Amazon (AWS)	Microsoft (Azure)	Google Cloud
Strengths	+ Offers the most services, from networks to robots + Most mature + Considered best for reliability and security + More computing power than Azure or GCP	+ Straightforward integration and migration of existing Microsoft services + Many more options available, including the best AI, machine learning and analytical services + Most services are cheaper than AWS or GCP + Good support for hybrid cloud strategies	+ Works well with other Google services and products + Excellent support for containerised workloads
Weaknesses	- All major software vendors who make their applications available on AWS Dev/Enterprise support must be paid. - The huge selection of available services and options can be bewildering for newcomers. - Relatively few hybrid cloud alternatives are available.	- Less service choice than with AWS - Designed specifically for business customers	- Fewer services available than with AWS or Azure - Limited support for business use scenarios

Satisfaction scores for public cloud providers

The figure below shows that Amazon and Microsoft secured similar customer satisfaction scores in the 2022 Whitelane* study. It should be noted, however, that Azure has almost twice as many contracts (>1 million euros) in the Netherlands than AWS.

The Google Cloud Platform's satisfaction score of 77 per cent was also high, but Google has only half as many contracts (>1 million euros) as AWS.



KEY TO SCORES	
Very unsatisfied	0%
Unsatisfied	20%
Somewhat unsatisfied	40%
Somewhat satisfied	60%
Satisfied	80%
Very satisfied	100%

2023 IT Sourcing Study - Netherlands

© 2023 Whitelane Research

* The 2023 Dutch IT Sourcing Study, performed by Whitelane Research in collaboration with Eraneos, looked at more than 450 distinct IT sourcing arrangements and 740 cloud sourcing arrangements, and involved more than 220 participants from the top IT spending organisations in the Netherlands.

Eraneos's advice

Towards an SIDN cloud model
DRS landing zone
DNS landing zone

Eraneos advises carefully considered migration to the public cloud

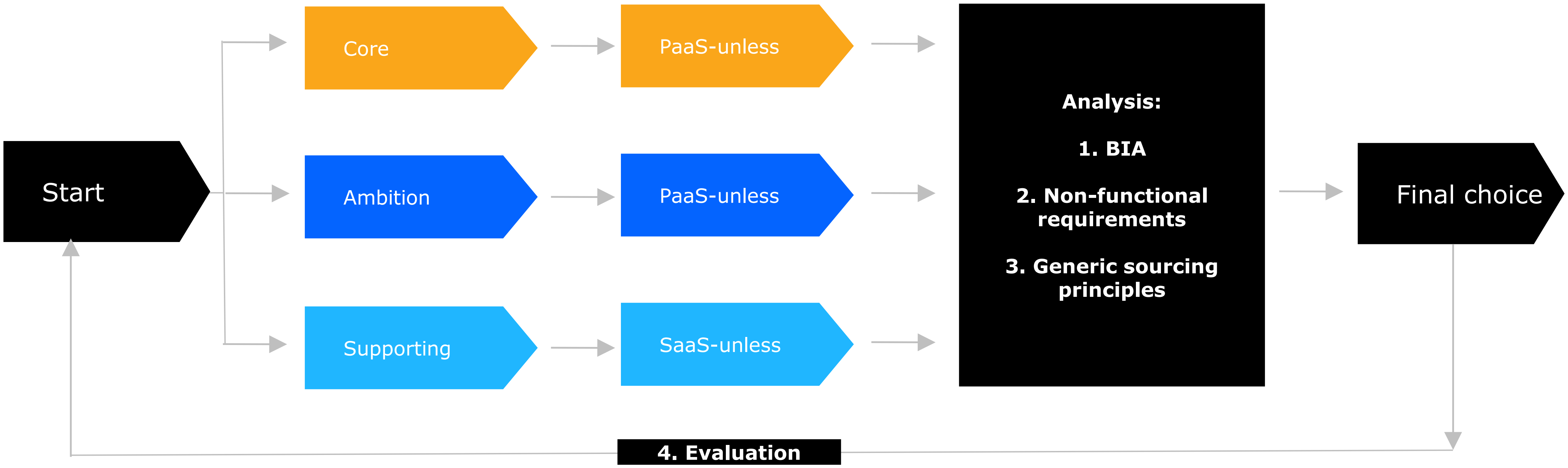
Public cloud is preferable
The strategic assessment identified the public cloud scenario as preferable. The large number of services available from public cloud vendors will relieve SIDN's technical management burden, thus enabling it to focus on innovation. The one trade-off for SIDN is compromising on its desire to play exemplary role in relation to the NL/EU-first strategy. SIDN might therefore consider the possibility of contributing to the further development of EU cloud initiatives, such as Gaia-X.

AWS is the best candidate, but not without risk
Within the public cloud domain, AWS is the best candidate. Although the differences are not enormous, AWS is the market leader and, as such, has the widest palette of services and the highest level of innovation. However, the use of AWS would not be without risk. SIDN currently lacks technical personnel familiar with the platform. External support will therefore be necessary for landing zone design and acquisition of the knowledge required to implement migration.

Careful consideration required
SIDN is seeking a platform that provides the best possible support for its objectives and ambitions. However, it is inadvisable to adopt a cloud-first and SaaS-first strategy without a clearly direction of travel. On the following slide, a cloud model is proposed for SIDN, involving 2 distinct sourcing models: one for core and ambition, the other for supporting applications. We propose that, in each case, a business impact analysis should be performed, the non-functional requirements should be considered, and available services should be assessed against the generic sourcing principles to establish whether they are, for example, unique or generic market offerings.

Roadmap to implementation
This sourcing strategy provides SIDN with a starting point for further development of a roadmap for all SIDN's ICT services and for implementation preparations. Such a roadmap is presented in the following section. For implementation of the roadmap, it is important not only to develop an architectural design, but also to build up internal knowledge and competences, so that SIDN has both appropriate technological expertise in house to maintain control of landscape operation, and the control competences required to, for example, manage the complex financial models in the cloud. Finally, it is advisable to develop the sourcing strategy further, to cover the management and implementation of other services, such as office IT, printing and telephony. That will provide structure and direction for the period ahead.

SIDN cloud model



While the proposed SIDN cloud model features a sourcing model for each domain, each choice must be challenged to arrive at a smart choice.

The challenge process involves the following stages:

1. BIA: requirements regarding availability, integrity and confidentiality
2. Non-functional requirements: requirements regarding performance, etc
3. Generic sourcing principles: principles concerning market availability and standardisation
4. Evaluation: periodic evaluation of stages 1 to 3

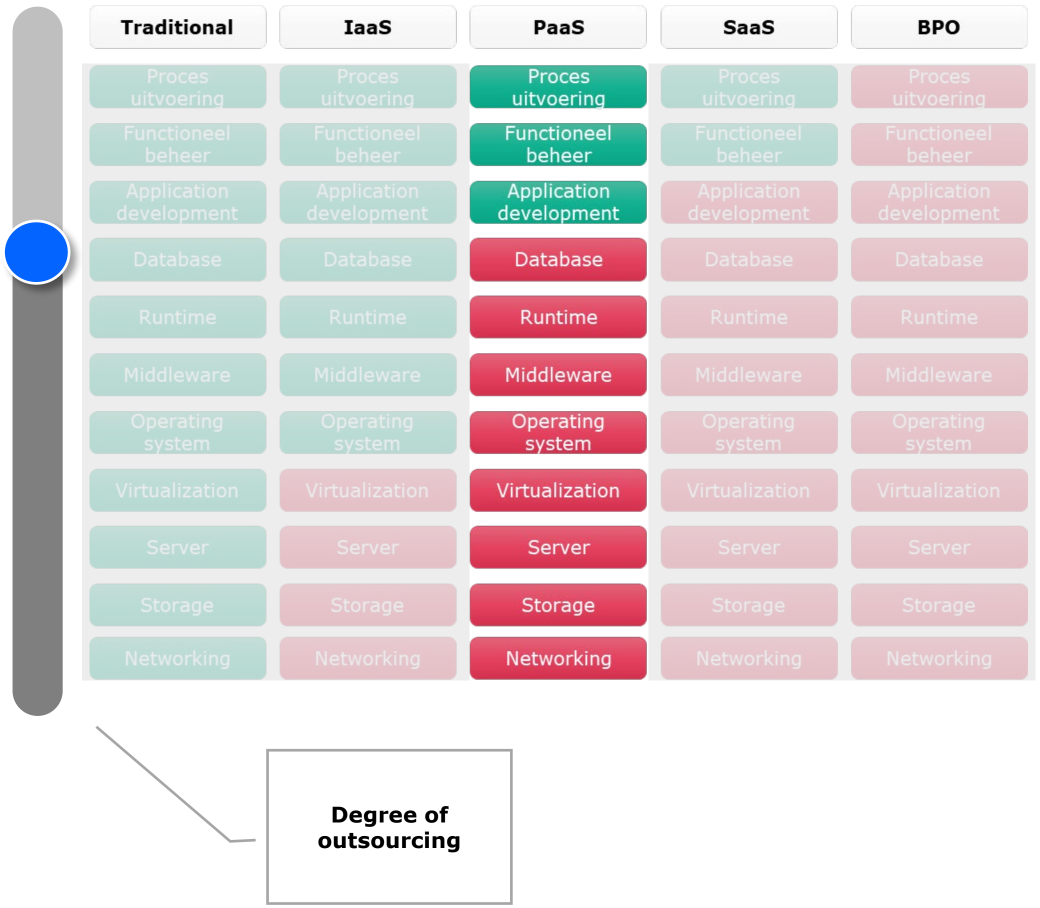
Examples involving the DRS and DNS are presented on the following slides.

DRS landing zone

Key elements of example

1. DRS is a core service.
2. The standard sourcing model is PaaS-unless.
3. BIA assumes an uptime of approximately 99.5 per cent.
4. Non-functional requirements do not imply special requirements.
5. Generic sourcing principles indicate:
   a) Application is identity-determinant and unique → Operate in house
   b) Landing zone is generic and there is sufficient market activity → Outsource
6. Hence, the DRS can land on PaaS in the public cloud.

This selection model is a simplified representation of reality appropriate for the strategic nature of this document. See also the recommendations regarding architecture and BIAs in the section on the roadmap.



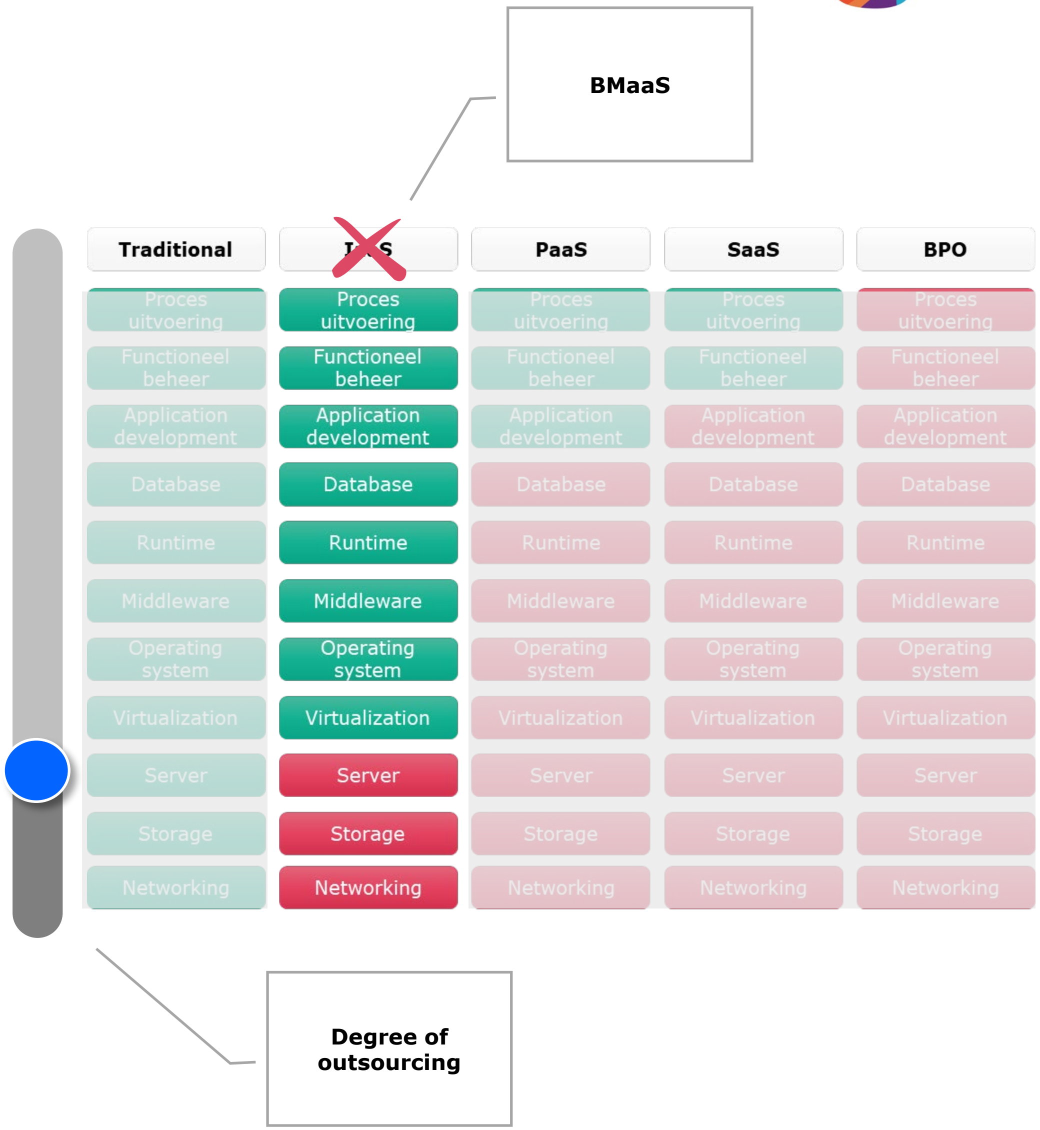
Traditional	IaaS	PaaS	SaaS	BPO
Proces uitvoering	Proces uitvoering	Proces uitvoering	Proces uitvoering	Proces uitvoering
Functioneel beheer	Functioneel beheer	Functioneel beheer	Functioneel beheer	Functioneel beheer
Application development	Application development	Application development	Application development	Application development
Database	Database	Database	Database	Database
Runtime	Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware	Middleware
Operating system	Operating system	Operating system	Operating system	Operating system
Virtualization	Virtualization	Virtualization	Virtualization	Virtualization
Server	Server	Server	Server	Server
Storage	Storage	Storage	Storage	Storage
Networking	Networking	Networking	Networking	Networking

DNS landing zone

Key elements of example

1. DNS is a core service.
2. The standard sourcing model is PaaS-unless.
3. BIA assumes an uptime of approximately 99.9 per cent.
4. Non-functional requirements do imply special performance or latency requirements.
5. Generic sourcing principles indicate:
   a) Application is identity-determinant and unique → Operate in house
   b) Landing zone is generic and there is sufficient market activity → Outsource
6. Hence, the DNS can land on bare metal as a service.

This selection model is a simplified representation of reality appropriate for the strategic nature of this document. See also the recommendations regarding architecture and BIAs in the section on the roadmap.



BMaaS

Traditional	~~IaaS~~	PaaS	SaaS	BPO
Proces uitvoering	Proces uitvoering	Proces uitvoering	Proces uitvoering	Proces uitvoering
Functioneel beheer	Functioneel beheer	Functioneel beheer	Functioneel beheer	Functioneel beheer
Application development	Application development	Application development	Application development	Application development
Database	Database	Database	Database	Database
Runtime	Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware	Middleware
Operating system	Operating system	Operating system	Operating system	Operating system
Virtualization	Virtualization	Virtualization	Virtualization	Virtualization
Server	Server	Server	Server	Server
Storage	Storage	Storage	Storage	Storage
Networking	Networking	Networking	Networking	Networking

Degree of outsourcing

Roadmap

Cloud-ready model for SIDN

Next steps

Produce detailed roadmaps
This proposed sourcing strategy provides SIDN with a starting point for further development of a roadmap for all SIDN's ICT services and for implementation preparations. In order to mitigate the risks associated with lack of technological expertise and familiarity with the complex cost models, it is advisable to find an AWS partner* to assist with onboarding, landing zone design and training of SIDN personnel. Along that pathway, SIDN can decide what forms of support it requires from the partner and/or AWS in the future. In that context, utilising the partnership with CIRA may be advantageous. It is also important to be on the lookout for partners' use of bespoke tools, in order to avoid vendor or technology lock-ins.

Draw up a transition plan
A transition plan is required for the management of roadmaps in a coherent portfolio. Consideration should be given to the sequence in which migrations are performed, and to dependencies linked to existing contracts and investments. The structure of the new ICT organisation should take account of the need for competence development within both Dev and Ops. It is important to adopt a clear approach in order to mitigate the risk of personnel loss, and to take account of organisational contraction (e.g. due to more efficient management of applications such as the DRS and supporting applications).

Establish control mechanisms
As well as appropriate technical expertise, it is important to establish proper governance for the services (see also the appendix). Such mechanisms should address matters such as architecture assurance, procurement and supplier management, landscape-wide integration and BIA updating. We advise reformatting the BIAs and making them more consistent with market norms. It is important that the work is done by a broad team, rather than only by the responsible manager, otherwise there is a risk that some requirements are neglected.

Formulate a sourcing strategy for other services
It is advisable to develop the sourcing strategy further, to cover the management and implementation of other ICT services, such as office IT, printing and telephony. That will provide structure and direction for the period ahead.

* Options for identifying AWS partners include: AWS Partner Solutions Finder (amazonaws.com). An action plan (RFI/RFP-light) for fast and effective partnership formation can be carried out, subject to consultation

Appendices

1. Sourcing, cloud and outsourcing
2. Generic sourcing principles
3. Value chain control

1. Sourcing, cloud and outsourcing

Traditional	IaaS	PaaS	SaaS	BPO
🟩 Process execution	🟩 Process execution	🟩 Process execution	🟩 Process execution	🟥 Process execution
🟩 Functional management	🟩 Functional management	🟩 Functional management	🟩 Functional management	🟥 Functional management
🟩 Application development	🟩 Application development	🟩 Application development	🟥 Application development	🟥 Application development
🟩 Database	🟩 Database	🟥 Database	🟥 Database	🟥 Database
🟩 Runtime	🟩 Runtime	🟥 Runtime	🟥 Runtime	🟥 Runtime
🟩 Middleware	🟩 Middleware	🟥 Middleware	🟥 Middleware	🟥 Middleware
🟩 Operating system	🟩 Operating system	🟥 Operating system	🟥 Operating system	🟥 Operating system
🟩 Virtualisation	🟥 Virtualisation	🟥 Virtualisation	🟥 Virtualisation	🟥 Virtualisation
🟩 Server	🟥 Server	🟥 Server	🟥 Server	🟥 Server
🟩 Storage	🟥 Storage	🟥 Storage	🟥 Storage	🟥 Storage
🟩 Networking	🟥 Networking	🟥 Networking	🟥 Networking	🟥 Networking

🟩 Done in house

🟥 Done by the vendor

We use the term '**sourcing**' to mean making a considered decision regarding the deployment of capacity for the performance of ICT activities and services. That implies choosing from insourcing, external hire, outsourcing, shared services and strategic collaboration. In practice, it is unusual for a single choice to be appropriate for the entire ICT landscape. Typically a separate decision is made for each service or cluster of services.

In the context of this sourcing strategy, we adhere to the NIST definition of '**cloud**':

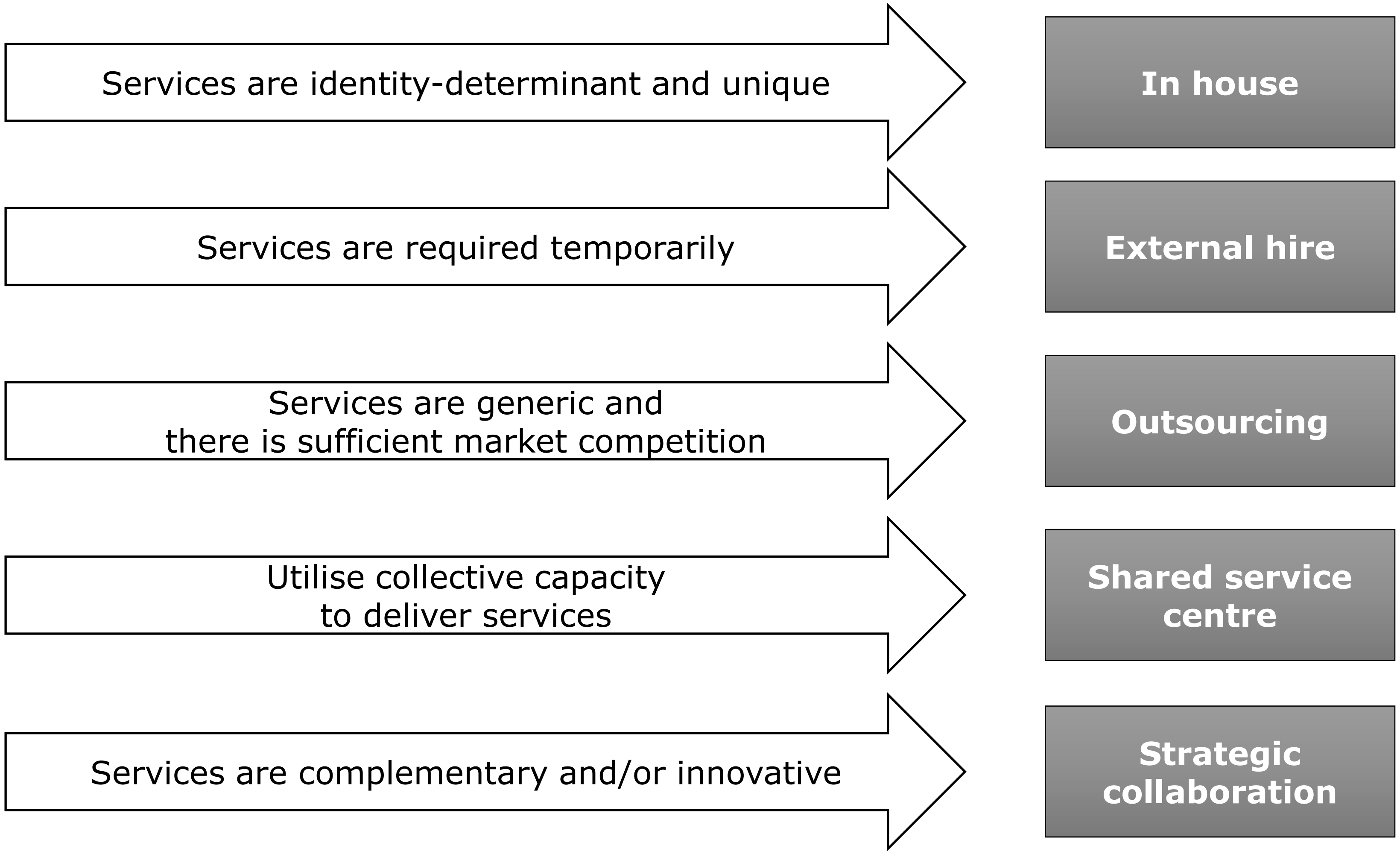
‘An on-demand, massively scalable service, hosted on shared infrastructure, accessible via the internet. Typical services provide data storage, data processing, and pre-built functionality, such as logging.’

Cloud services can be distinguished on the basis of the degree of **outsourcing**:

1. Complete cloud services, involving the provision of an entire application environment, usually referred to in practice as 'software as a service' (SaaS).
2. Cloud platforms that make components available, on which the customer can independently land an application, usually referred to in practice as 'platform as a service' (PaaS) or 'infrastructure as a service' (IaaS).

Where a complete service is outsourced, the process execution and functional management of an application are also undertaken by an outside party; in practice, this is usually referred to as business process outsourcing (BPO).

2. Generic sourcing principles



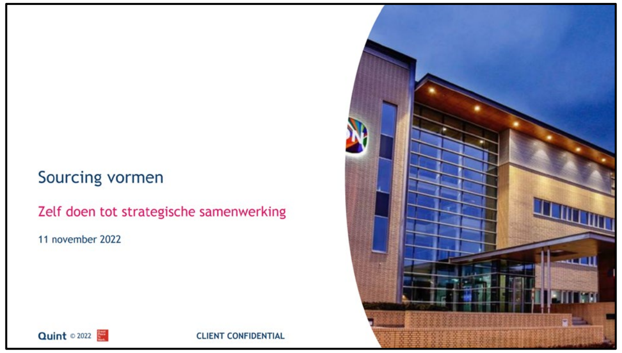
Services are identity-determinant and unique → In house

Services are required temporarily → External hire

Services are generic and there is sufficient market competition → Outsourcing

Utilise collective capacity to deliver services → Shared service centre

Services are complementary and/or innovative → Strategic collaboration



Sourcing vormen

Zelf doen tot strategische samenwerking

11 november 2022

Quint © 2022

CLIENT CONFIDENTIAL

See options per sourcing form previously identified by Eraneos and appended to this document.

2. Insourcing is the best option if...

- **Client has expertise in house**
- **Decision relates to a business function that is/should be one of the client's USPs**
- **Quality of internal business function performance is high**
- **Decision relates to something where client needs to make the difference**
- **Decision relates to a business function where client wants to excel**
- **Subject to the condition that client has sufficient scale to perform services in house; below a critical threshold, knowledge management and continuity are at risk**

If a policy on the selection of a sourcing form for this business function exists.

If there is no (individual) market player that can perform the business function entirely independently.

If (internal performance of) the business function is essential for the organisation or unit to secure the desired position within the concern.

If performing the business function in house brings about a shift towards customers in the value chain and thus increases visibility.

If a business function requires (numerous) modifications, and a great deal of specialist knowledge is needed to realise them.

If the quality of internal business function provision satisfies the applicable requirements.

If performance of the business function requires organisation-specific knowledge primarily available only within the organisation.

If the organisation lacks the competences required for supervision of an outside provider.

If the business function must be integrated (aligned with other business functions) in relation to customers.

If the business function contributes to the tailoring of customer-oriented services.

If there is no (individual) market player that can perform the business function entirely independently.

2. External hire is the best option if…

- **Client requires temporary and/or specific knowledge/expertise resources**

If the business function is purely operational and not identity-determinant.

If the business function's turnaround time needs to be reduced.

If the organisation lacks the technical knowledge/competence to perform the business function.

If the business function is readily available in standardised form on the (commercial) market.

If the business function requires extended 'opening hours' outside normal office hours, which cannot be covered by internal personnel.

If the knowledge required to perform the business function is 'old fashioned' and use of an outside service provider enables internal staff to be deployed on modern technologies.

If the technology used by the client is outdated and requires modernisation based on the method/technology available from the vendor.

If the capacity for the business function is required in the short term and only for a short time.

If the capacity required for the business function is highly variable.

If the business function needs to be performed better or in a more appropriate way, and an external service provider can demonstrably do so.

If a higher degree of capital/organisational resource utilisation is necessary.

If the business function's fixed cost percentage needs to be reduced (by means of flexible pricing mechanisms).

If the volume is very small (smaller than the critical volume required for the maintenance of internal knowledge and competences).

If a business function requires (numerous) modifications, and a great deal of specialist knowledge is needed to realise them.

If the organisation lacks the competences required for supervision of an outside provider.

2. Outsourcing is the best option if…

- **It will reduce costs; financial considerations are relevant mainly if the business function accounts for a high proportion of overall costs**
- **Decision relates to a service that is NOT already or intended to be one of the client's USPs**
- **Internally provided services would not be of the required quality**
- **It will result in a greater level of cost variabilisation than internal provision (85 per cent indirect costs)**
- **It will result in more transparent cost allocation than the existing situation**

If the business function is purely operational and not identity-determinant.

If the organisation lacks the technical knowledge/competence to perform the business function.

If the business function is readily available in standardised form on the (commercial) market.

If a policy on the selection of a sourcing form for this business function exists.

If the business function requires extended 'opening hours' outside normal office hours, which cannot be covered by internal personnel.

If the knowledge required to perform the business function is 'old fashioned' and use of an outside service provider releases internal staff for other activities.

If the technology used by the client is outdated and requires modernisation based on the technology available from the vendor.

If the capacity required for the business function is highly variable.

If better insight into the costs associated with the business function is required.

If the business function needs to be performed better or in a more appropriate way, and an external service provider can demonstrably do so.

If a higher degree of capital/organisational resource utilisation is necessary.

If the volume is very small (smaller than the critical volume required for the maintenance of internal knowledge and competences).

2. SSC is the best option if…

- **Client's holding company has the expertise and capacity, and can therefore achieve the necessary quality**
- **Volume of client's input is too small to warrant other models**

If other units within the organisation perform the business function.

If a policy on the selection of a sourcing form for this business function exists.

If there is no (individual) market player that can perform the business function entirely independently.

If the business function requires extended 'opening hours' outside normal office hours, which cannot be covered by internal personnel.

Ample relevant knowledge is present within other units of the organisation.

If the knowledge required to perform the business function is 'old fashioned' and use of an outside service provider enables internal staff to be deployed on modern technologies.

If the technology used by the client is outdated and requires modernisation based on the technology available from the client's holding company.

If the capacity required for the business function is highly variable.

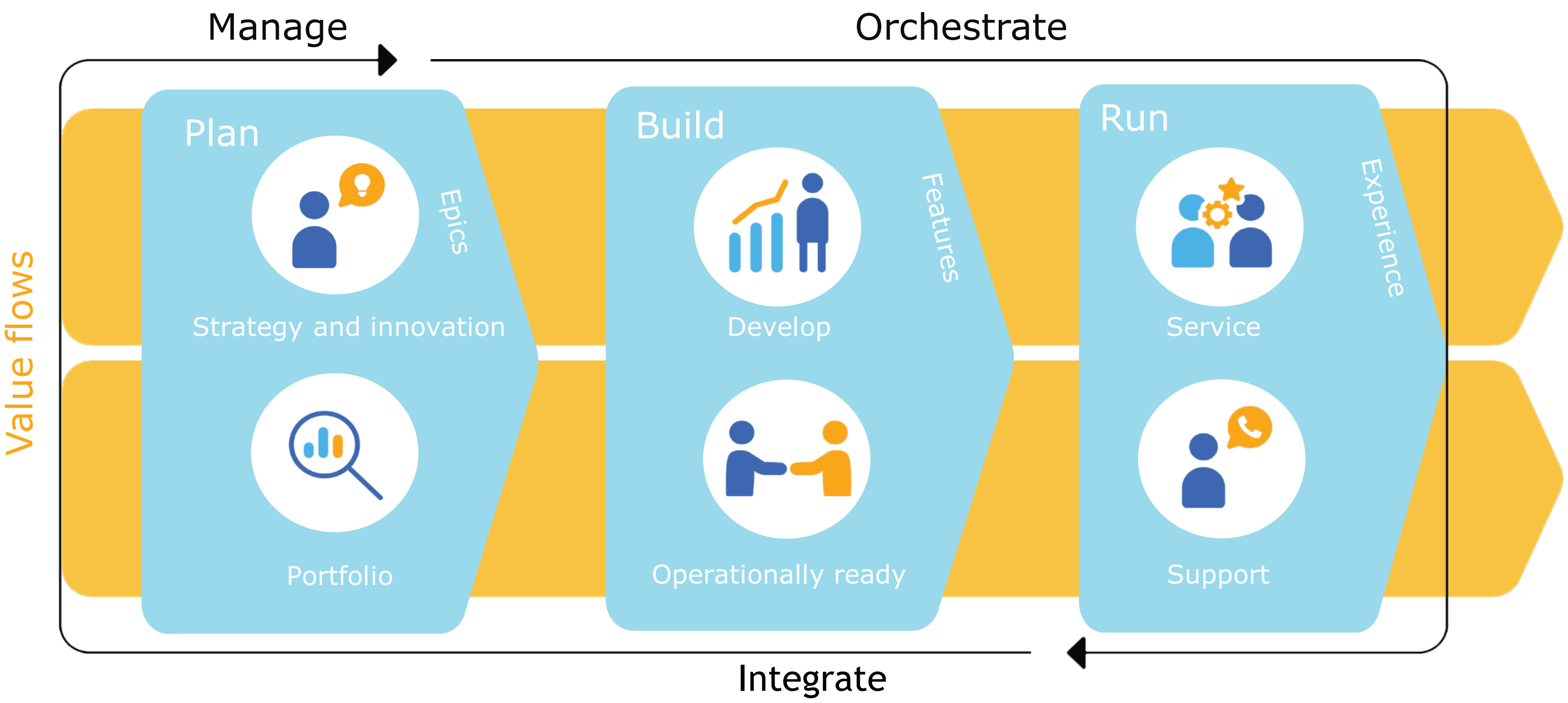
If the various technologies used to perform the business function require organisation-wide harmonisation or standardisation.

If better insight into the costs associated with the business function is required.

If the business function needs to be performed better or in a more appropriate way, and an external service provider can demonstrably do so.

If a higher degree of capital/organisational resource utilisation is necessary.

3. Governance



Governance consists of:

***Direction**:*
Governance, principles, policy & strategic planning

Orchestration:
Modifying and modernising services using an agile and/or project-based approach

Integration:
Operational delivery and automation of the services

The objective is to provide the services in a controlled, predictable and valuable manner.