1. ABOUT BASEFARM

Basefarm is a Northern European managed services provider for mission critical it. We manage and run it-solutions on cloud platforms best suitable to our customer's needs. With 17 years' experience in managing on-line solutions, we help our customers achieve their digital ambitions. The foundation of the company is very much the same as 17 years back; a privately owned, transparent, honest company with a flat organization.

During the past decade, Basefarm scaled and continuously developed their organization to sell Enterprise Level, Managed Services and Solutions to businesses. This by making significant investments in operations systems and tools, data centers, network, security and complex solutions. But maybe most importantly: refining the process and quality framework and invested in employees. Today Basefarm has more than 500 experts in their offices that are situated in Norway, Sweden, Netherlands, Germany and Austria. Basefarm services hundreds of customers within different verticals like government, tourism, education, media and publishing, aviation and transport, industry, financial and business services. Some of our references in The Netherlands are Funda, Ziggo, D-rt Groep (D-reizen & VakantieXperts), Reeleezee, Bookit, and Kewill.

1.1 Our Values

Our values are prominently present within all layers of the company. And they form the basis of our entire way of thinking and acting.

Skillful: With our technical excellence and professionalism we take full responsibility for our customer's business needs and requirements.

Dedicated: We care for our customer's business and are committed to ensure the highest level of quality. We are energized by new challenges.

Close: We work in close collaboration with our customers. We have a deep understanding of our customer's requirements and together secure future development of the solutions.

Constructive: We are a solution oriented and constructive service provider. We focus on solutions rather than problems. With our systems and structured approach, we ensure stability and efficiency.

1.2 Vision & Mission

Vision

Expertise without comparison, technology without boundaries, growth without limits. Shaping tomorrows solutions today.

Mission

Our mission is to help our customers achieve their digital ambitions, through enabling and securing their online presence.

1.3 Customer Focus

Basefarm has special attention for Customer Satisfaction. Every year, a Customer Satisfaction Survey examines how Basefarm customers rate us on different parts such as service, support, invoicing, etc. This valuable information is processed into a SIP (Service Improvement Plan). If improvements can be done on short term, the required activities are immediately planned and implemented. When it comes to improvements in the medium or long term, the SIP will serve as input for the “Continual Service Improvement” process.

Concerning mid-term or long-term improvements, the SIP is used as input for the “Continual Service Improvement” process to improve Basefarm overall. Basefarm’s target regarding customer satisfaction is above 5 (on a scale of 1 to 6).

Basefarm achieves this by really happy customers (score of >5 from 1 to 6 in the overall customer satisfaction Survey and our satisfied employees (>80% High Satisfied score in the annual “Great Place to Work” Research) who work closely with their customers on their business successes. By providing the best possible (technical) foundation, our customers can successfully focus on innovation and growth. To summarize: We deliver “Technical Excellence” through expertise and knowledge.

Basefarm has achieved a shared first place in the “Emerce Top 100 2018” in the category “Managed Hosting”. Customers of Basefarm express their appreciation for the skill-level and the know-how, the trustworthiness, flexibility and the proper ratio between price and quality

1.4 Basefarm Customer Team

At Basefarm, a dedicated Customer Team will be instantiated, which primary consists of a Technical Account Manager (TAM), a Service Manager, an Account Manager and a Solution Architect. If needed the team can be expanded with additional specialists.

During the daily routine, the TAM is the primary contact for the technical solution and the implementation of changes (with the exception of standard changes). The 24x7 Service Desk, which is manned by highly qualified engineers, solves most of the events and incidents reported and performs the standard changes in addition. In the background, the Basefarm Service Desk is supported by an international team of specialists and the Customer Team. This enables the Customer Team to focus on proactive maintenance and optimization of the customer environment. While catering to the customer’s needs, Basefarm will continuously seek connection to the customer to ensure that our cooperation is as efficient as possible. This way our services stay connected to the dynamics of the business of our customers.

1.5 References

Klarna
Simplifying Buying

PayEx
Experts in payments

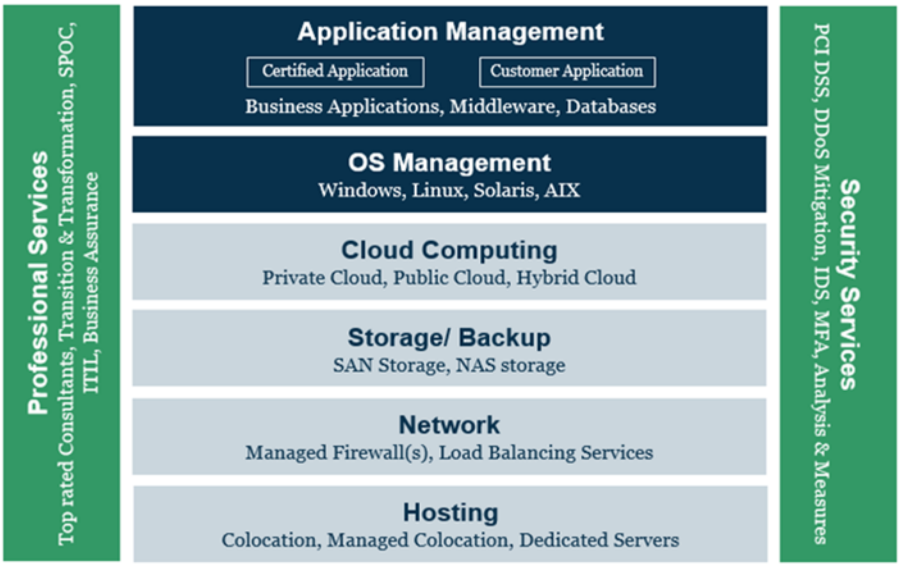
= exact

funda

D-reizen.nl

A. BASEFARM SERVICES

Standard services of Basefarm are presented in the figure below.


Professional Services
Top rated Consultants, Transition & Transformation, SPOC, ITIL, Business Assurance
Application Management
Certified Application
Customer Application
Business Applications, Middleware, Databases
OS Management
Windows, Linux, Solaris, AIX
Cloud Computing
Private Cloud, Public Cloud, Hybrid Cloud
Storage/ Backup
SAN Storage, NAS storage
Network
Managed Firewall(s), Load Balancing Services
Hosting
Colocation, Managed Colocation, Dedicated Servers
Security Services
PCI DSS, DDoS Mitigation, IDS, MFA, Analysis & Measures

Appendix A describes the standard Basefarm Services. If any exceptions regarding these services are described in chapter **Error! Reference source not found.**, the latter prevails above appendix A.

A.1 Networking Services

A.1.1 Internet Bandwidth – 95 Percentile

With peak-based line lease the price is calculated based on consumed bandwidth. Excess traffic peaks are exempt from the calculation based on the 95% rule. This entails that the month's 36 hour with highest traffic levels are discarded. This is the sector's de-facto pricing model for high capacity line lease.

Key features and benefits:

- Industry-standard measuring method for line usage.
- Measuring interval every 5 minutes.
- Measuring period per calendar month.
- Traffic peaks up to 36 hours (5%) discarded.
- Usage above agreed commitment is invoiced in arrears.

Lease of shared Internet lines in accordance with agreed usage in Mbit/s. This includes both up and downstream traffic.

The Supplier measures the Operation Platform's allocated bandwidth every 5 minutes in the Measuring period. 5% of the measurements with the highest allocated bandwidth are exempt from the calculation, where the highest individual measurement of the remaining 95% comprise the basis for the calculation if the Customer's usage exceeds the agreed usage.

Customer's responsibility:

- If the Customer, without the Supplier's consent, has peaks in bandwidth usage that exceeds agreed usage beyond ten times or 1Gbit/s, the Supplier may impose bandwidth restrictions or denial of service.

A.1.2 Public IP usage

The Operation Platform is connected to (one or more) virtual networks (VLAN) in the Supplier's shared network infrastructure. The Customer's use of the network is dedicated and access is tailored to the Customer's requirements. Firewalls, load balancers, routers or other suitable equipment handle the Operation Platform's incoming and outgoing communication as well as communication between different VLANs.

The service can be delivered with either individual IP addresses or an entire subnet, as shown below:

- Network, public IP single address. Reservation of 1 IP address.
- Network, public IP subnet (Bitsize 29). Reservation of 8 IP addresses.
- Network, public IP subnet (Bitsize 28). Reservation of 16 IP addresses.
- Reservation of larger IP subnet needs special agreement with the Supplier.

Note: 5 of the IP addresses in one subnet cannot be used by the Customer because they are allocated to network-specific services.

A.1.3 Network Solutions - Dynamic Solutions

Network Solutions at Basefarm consist of load balancing and firewall services and are these solutions are subdivided in "Shared Solutions" (shared load balancer and shared firewall service), "Dynamic Solutions" (shared load balancer and dedicated firewall services) and "Enterprise Solutions" (dedicated load balancer and dedicated firewall services). The following table shows the different Network models for the "Dynamic Solutions".

NETWORK SOLUTION	PRODUCT DESCRIPTION	INCLUDED VLANS	OPTIONAL		PEAK FACTOR
			Client VPN	**P2P VPN**	
B-50	Shared 50 Mbps load balancer service and dedicated 150 Mbps firewall service	3	Yes	Yes	3
B-100	Shared 100 Mbps load balancer service and dedicated 300 Mbps firewall service	3	Yes	Yes	2
B-200	Shared 200 Mbps load balancer service and dedicated 600 Mbps firewall service	3	Yes	Yes	1,5

Table 1: Different Dynamic Network Solutions

Dynamic Network Solutions are delivered with dedicated firewalls and shared load balancers for the specified guaranteed throughput capacity. The throughput can peak above the guaranteed level according to the peak factor in the product matrix up to 5% of the time during one month.

Three security zones are included. Additional security zones and various VPN connections are optional services.

The peak factor is established to assure that the network solution has the necessary capacity available. Basefarm will contact the Customer and propose the option to migrate to a solution model with higher throughput if the throughput exceeds the peak factor. If the customer approves we will change the configuration and charge the corresponding Network Solution fee. The migration work is charged on hourly basis and will vary with the actual migration step. If the Customer disapproves, we can set the throughput limit according to the guaranteed throughput for the actual solution model. The throughput numbers are based on traffic flow consisting of a combination of small and big packets.

The customer must specify requirements for load balancing features and firewall rules.

A.1.4 Load Balancing profile

The Supplier’s load balancing services are provided by Shared Infrastructure and may be used both for load balancing of the Supplier’s web server services (Shared Infrastructure) and the Customer’s dedicated web servers and application servers (Dedicated Infrastructure).

With load balancing web requests are distributed/forwarded from a public or private IP address to a given server group, frequently consisting of two or more web servers in the Operation Platform with identical configurations. The load balancing service supports handling of an IP address to one or more port(s), i.e. one-to-one or one-to-many (this may also be referred to as reverse proxy or transparent IP). Ordinarily requests are evenly distributed based on the round-robin algorithm and with keep-alive-handling activated. Other distribution algorithms may be configured on agreement.

Standard switching

Standard load balancing takes place on the application layer. The load balancer inspects the current content of the request following different algorithms, stores the results, and selects the appropriate server from a server group that will get the next request.

Load balancers can set cookies in the response from the application. This preserves the communication between the user's browser and the internet service. Corresponding methods may also be used to control requests against specific applications and services. This is useful in cases where part of the platform provides individual services, i.e. a management interface.

Included in the service is SSL termination and load distribution of SSL-decrypted / plain text requests to the web server. By offloading the web server and application server for data processing and request handling, significant gains can be created in terms of design and further scaling of the operating platform.

Standard load balancing, or application load balancing, advantages / forwards content session or session dependent web requests to two or more servers; the communication between sender and recipient assumes task related or rule-based functionality in load balancing.

Examples of standard load balancing services are:

- URL inspection
- Persistence/sticky based on http cookie set by load balancer, ip source address or SSL session ID
- Automatic failover service (by mistake in retail service or loss of Web server (s))
- SSL- handling / termination

In comparison with round-robin, “least sessions” as allocation algorithm, is efficient in handling resource intensive requests against the web server.

A.1.5 VPN

With VPN communication between the customer, the customer's partners and the operation platform, seamless and private communication is ensured between the parties. We provide both point to point and client VPN connections.

VPN Users

Using a VPN client the customer's users can connect to the operation platform independently of location and network connection. The client is either integrated in the customer's operating system or requires the installation of software.

Virtual Private Network (VPN) for connection as required to Operation Platform for Customer/third party. Service is based on authentication of users registered in the Supplier's Operation Administration System.

The Customer's/third party's communication with the Operation Platform across VPN follows "split horizon" routing rules, i.e. that the VPN connection is only used for communication against the Operation Platform.

Prerequisites

- VPN users with the Customer use IPSec, and this is conditional on the configuration of client software installed in the operating system. (Some operating systems include this). The Suppliers regulations concerning protocols, authentication, encryption, etc., are guiding for installation of the Service.

A.2 Storage and Backup

Backup is required for the restore of data in the event of disk failure or disasters. On request Basefarm can also recreate lost data caused by user error.

A.2.1 Agent-based backup per server

We configure and perform backups on all database systems/servers in the operation platform at the request of the customer. All backups, i.e. customer data, system data and configuration, are stored offsite at a different location geographically separated from the operation platform.

The service includes client setup and configuration of dedicated servers, both physical and virtual, and backup client license. Terms for backup of operating systems and databases are specifically described for individual Services.

Supplier's responsibility:

- Carry out backup of Dedicated Infrastructure as agreed with Customer.
- Ensure that backup is carried out and implement corrective measures in case of discrepancies.

Customer's responsibility:

- Agree with Supplier on backup of Dedicated Infrastructure in the case of changes to the Operation Platform.
- The Customer may, following agreement with the Supplier, adjust the backup frequency, time for running backup and/or backup length if the Customer has specific requirements that deviate from the Supplier's backup routines.
- For backup of file systems the following adjustments may be agreed:
    - Files are stored for shorter or longer periods.
    - Deleted and changed files may be handled differently.
    - Frequency of backup of changed files.
    - Number of generations of a file that is stored.

Included Operation Processes:

- Perform backup of Dedicated Infrastructure.
- Monitor backup result and implement corrective measures.

A.2.2 Backup usage

Backup of the servers will be performed using Basefarm's shared backup services, with data and tape storage in a third datacenter. The backup data stored in the backup system will be invoiced monthly based on volume (price per GB data stored). Any volume above the agreed commitment is invoiced in arrears.

A.3 Basefarm Managed Cloud

The virtual servers (VMs) in the solution for Customer are created on Basefarm Managed Cloud. This cloud offering is a shared virtualization platform that is "stretched" across Basefarm's two datacenters in Oslo, supported by fully redundant networking and storage services. The platform is highly scalable on all levels, which then also applies to the Infrastructure of the Customer utilizing the platform.

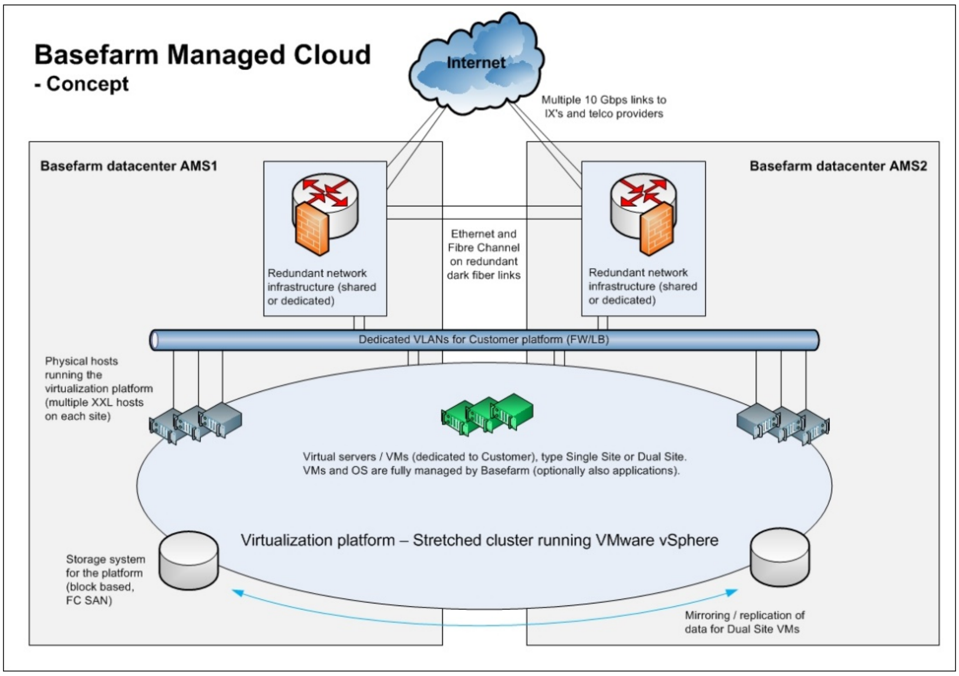

Basefarm Managed Cloud
- Concept
Internet
Multiple 10 Gbps links to IX's and telco providers
Basefarm datacenter AMS1
Basefarm datacenter AMS2
Redundant network infrastructure (shared or dedicated)
Ethernet and Fibre Channel on redundant dark fiber links
Redundant network infrastructure (shared or dedicated)
Dedicated VLANs for Customer platform (FW/LB)
Physical hosts running the virtualization platform (multiple XXL hosts on each site)
Virtual servers / VMs (dedicated to Customer), type Single Site or Dual Site.
VMs and OS are fully managed by Basefarm (optionally also applications).
Virtualization platform – Stretched cluster running VMware vSphere
Storage system for the platform (block based, FC SAN)
Mirroring / replication of data for Dual Site VMs

Figure 1: The Basefarm Managed Cloud

With Managed Cloud fast access to virtual hardware resources is offered as a service – as required, and for low initial costs. We call this Infrastructure-as-a-Service, because the service's pricing model is pay-as-you-go. Capacity expansions are dynamic and are calculated based on monthly allocated CPU, RAM and storage in accordance with the price list. For the customer this entails that the previous month's consumption is invoiced in arrears. Future capacity requirements are performed by activating (or deactivating) resources, and that related operation costs are variable (OpEx).

Managed Cloud can be used and integrated with other hardware in the Operation Platform.

The Customer leases the virtual servers from a shared virtualization platform for handling of business-critical tasks. In use, the VMs can be considered to the Customer to be dedicated, and the Supplier's responsibility for operation of dedicated hardware is given equal status to the operation of virtual machines as they are provided by this Service.

The VMs are dynamically distributed over several physical machines in one or two datacenters, and use the Supplier's high availability network cloud for data communication and access to storage resources. The Service can subsequently be used and integrated with other hardware in the Operation Platform.

Basefarm distinguishes between the following VMs:

- Single-site VM - within one data center
- Dual-site VM - within two data centers

VMs are provided with the following standard specification:

- 0 virtual CPU (vCPU), 0 GB RAM, 0 GB disk

For each individual VM the following extensions can be implemented on request:

- Extra vCPU
- Extra RAM
- Extra Disk

Prerequisites:

- Operation of the OS must be submitted by the Supplier

The following is included in the price:

- Lease of VM per month

The following is NOT included in the VM price:

- OS licenses
- OS operation
- Backup

A.4 Basefarm Operating System

With Basefarm OS (BOS), the Supplier is responsible for operation of the operating system (OS) and for ensuring optimum consistency and quality in this. The Supplier is responsible for ensuring that the OS, as a platform for Software and End-user services, works as intended. The Supplier’s responsibility and included Operation Processes apply to operating systems installed on both physical and virtual hardware.

Supplier’s responsibility:

- Perform installation and configuration of OS.
- Perform security and revision updates.
- Monitor and meter OS processes and components.
- Activate access to Shared Services for secure login and outgoing mail.
- Inform the Customer of plans, changes, incidents and other matters that may affect the operational quality of the Applications.

Customer's responsibility:

- Operation and maintenance of End-user services and Software.
- Inform the Supplier of plans, changes, incidents and other matters that may impact the operational quality of the OS.

Included Infrastructure:

- Access to Shared Service for secure login (SSH/RDP) to the Operation Platform.

Included Operation Processes:

- Perform updates.
- Troubleshooting and fault correction related to the OS.
- Monitoring and metering in accordance with The Supplier's standard for the OS.

Prerequisites

- In the case of failure the OS is restored using the Supplier's operation tools.
- The Supplier reserves the right to logon to the server with administrator privileges.
- If the Customer needs to perform tasks as administrator (e.g. restart processes, deploy new software, etc.), the Supplier must facilitate this following agreement with Customer.

A.4.1 Operation of Linux Operating Systems

For the Managed Linux Service the Supplier carries out operation of Red Hat Enterprise Linux.

OPERATION PROCESS	DESCRIPTION
Monitoring	The Supplier monitors Linux as follows: • Ping-requests • Fill level of disks • TCP connection (SSH) • Central processes running (i.e. sshd, crond) • Time deviations
Measuring	The Supplier measures Linux as follows: • CPU and memory (usage and swapping) • Disk (usage)
Updating	Installation of updates is performed according to the Suppliers automatic update routines. Updates will be scheduled and agreed upon with the Customer. Included Operation Processes: • Installation of updates • If error situations in Customer Software occurs (Customer Application) and this is due to the update, troubleshooting and error correction carried out by the Supplier in connection with Customer Software is not included.
Upgrading	The Supplier does not upgrade OS versions, e.g. from RHEL 6 to 7, but performs a complete reinstallation. If new versions are required, the customer must order this from the Supplier in accordance with Change Process.

Table 2: Operation Processes for Basefarm Linux Operating System

A.5 Basefarm Application Management

The service Basefarm Application Management (BAM) regulates responsibility for operation of the software that is included in the solution. Basefarm categorizes applications in "Certified Applications" and "Customer Applications". Both kinds of applications are managed by Basefarm.

The Certified Applications are applications where Basefarm has extensive experience, with knowledge spread widely in the organization and automation support in the operations- and management tools. Most Basefarm customers also have some customer specific applications, where Basefarm is able to manage the applications based on descriptions and instructions from the customers. A simple way of describing the difference between the two categories is that for the "Certified Applications", Basefarm knows best, while for the Customer Applications, Basefarm assumes that the customer knows best. The customer will then also act as the main responsible for some activities – hence the RACI matrix as shown below.

A: Accountable - The party accountable for the operating performance and/or accountable for making the necessary arrangements to ensure such implementation.

R: Responsible - The party doing the work to perform operating performance in accordance with the agreed scope.

C: Consulted - The party whose opinions are obtained through dialogue.

I: Informed - The party who is kept informed of the progress/status prior to, during or after the execution and delivery by the other party.

Letter quoted in parentheses ( ) indicates an option for participation which can be agreed, and following that the criteria for such participation shall be described.

	CERTIFIED APPLICATION		CUSTOMER APPLICATION	
Operation task	**Basefarm**	**Customer**	**Basefarm**	**Customer**
Installation	AR	(C)I	RCI	A(R)
Monitoring	AR	I	AR	CI
Backup	AR	I	AR	CI
Restore	AR	I	AR	CI
Troubleshooting	AR	CI	AR*	(R)CI
Debugging	AR	CI	RCI	A(R)
Updating	AR	CI	RCI	A(R)
Upgrading	AR	(I)	RCI	A(R)
Optimizing/Tuning	AR	CI	RCI	A(R)
Third Party Agreements	AR	(I)	CI	AR
Third Party Follow Up	AR	-	AR	(R)CI
Develop installation documentation	AR	-	(R)I	AR
Develop operational documentation	AR	(I)	AR	CI

Table 3: RACI matrix Basefarm certified and customer applications

*) Basefarm performs the troubleshooting tasks specified by and agreed upon with the customer. If the error is not corrected when these tasks are carried out, the matter is escalated to the technical contact at the customer or Third Party for further troubleshooting/debugging.

Based on customer demand, market maturity, support in operations tools, level of knowledge etc., Basefarm continuously evaluate which applications can be candidates for the certification process. This means that some of the applications used in the solution of Exact could be Certified Applications in the future.

Description of operating performance, each party's responsibilities and operations including scale, is presented in the following sections.

Prerequisites

- Operating system(s) that the Software is installed on, must be installed and operated by the Supplier.

A.5.1 Operation of Software (Certified Application)

For the Certified Application Service the Supplier has full responsibility for the Software (Certified Application) working as intended, albeit limited by those agreements that exist between the Customer and the application provider, so-called third party maintenance agreements. Such Software must ordinarily comply with the Supplier's quality criteria for:

- Required operational quality and stability.
- Handling of backup, restore, monitoring and quality measurements.
- Handling of installation, configuration and deposit in Operation Administration System.
- Documentation of general procedures in accordance with agreed Service level.

Supplier's responsibility:

- Installation and configuration of Software.
- Optimization (tuning) of Software.
- Monitoring and measuring relevant processes and components in Software.
- Perform testing, troubleshooting and error correction in Software.
- Carry out updates of revisions/patches from software provider.
- Carry out upgrades to new versions of Software.
- Implement and carry out log handling, such as automatic rotation, compression and deletion.

Included Operation Processes:

- Perform testing, troubleshooting and error correction in Software.
- Update in accordance with agreement for specific Software.

Prerequisites

- Installation of Software (Certified Application) must be performed by Supplier.

A.5.2 Oracle Basic Management

Our goal is to provide a standardized installation that fulfils our own- and the customer's requirements for security, scalability and performance. We have achieved this by creating a flexible framework that integrates installation, configuration and day-to-day operation with our operation administration system and CMDB.

All services Basefarm provides in connection with the operation of Oracle uses a basic operation service as a point of departure. This consists of the following:

- Installation
- Monitoring
- Reporting

- Backup
- Operational operation
- Updates

Installation

Our Oracle Database installation is based on a standardized and automated installation procedure. All input to the installation is taken from our internal CMDB that allows us to quickly and automatically recreate an environment on a new machine. This includes both installation and configuration. The software is installed with latest security patch approved by Oracle (PSU).

Monitoring

In addition to monitoring hardware, operating system and network, we have developed Oracle-specific monitoring that is integrated with our error handling systems. Basefarm Service Desk receives and handles notifications based on the monitoring of:

- Availability
- Logs
- Fill level
- Resource usage
- Backup
- HA / Cluster
- Reporting

We measure and create graphs of the performance data that the customer can access via the Customer portal. By default, we create graphs of the following (other metrics can be added, based on requirements):

- Sessions
- Logon
- SGA/PGA consumption
- Data Growth
- Waits
- Cache hit ratio
- Backup

The following is standardized for the Oracle database on production systems:

Full weekly backup

Daily incremental backup

Backup retention is set for 30 days – we can restore backup from at least 30 days back in time.

In order to perform a complete reconstruction in the case of hardware failure, our backup routines include all necessary information in order to quickly recreate the installation. Backup is regularly verified by loading it onto our test server which has been set up for this purpose.

Operational operation

In addition to monitoring disk space, we have automatic rotation of log files and clearing of trace files.

Updates

We keep the database up to date with security patches and other recommended patches from Oracle. This is not included in the service but is carried out as a consultancy service in collaboration with the customer.

Agreement text

OPERATION PROCESS	DESCRIPTION
Backup	Backup of Oracle Database is performed automatically in accordance with the following routine: • Full weekly backup • Daily incremental backup • Daily export to file
Restore	• In order to perform a complete reconstruction, the Supplier's CMDB and backup routines include all necessary information in order to recreate the installation. • In the case of hardware failure and unless otherwise agreed between the Parties, the Customer's database(s) are ordinarily restored by the Supplier from the latest available backup data
Monitoring	The Supplier monitors Oracle Database as follows: • Availability • Logs • Fill level • Resource usage • Backup • HA / Cluster
Measuring	The supplier monitors a number of parameters in Oracle Database for performance, stability and availability. The measurements, which also are available for the Customer on Customer portal, are used to predict capacity development and perform error diagnostics.
Updating	With respect to the version definition from Oracle and how the database versions are deployed, ordinarily all changes to a release are conditional to an Upgrade, see below. This is mainly due to complexity in and/or the scope of the release change and how this may or may not affect the End User Services and/or other Software in the Operation Platform. The Supplier's work in connection with release changes in Oracle Database are not included in monthly compensation.
Upgrading	The Supplier upgrades Oracle Database following agreement with the Customer.
Log handling	Carried out in accordance with the Supplier's standard.

Table 4: Operation Processes for Oracle Basic Management

B. BASEFARM IMPLEMENTATION SERVICES

Implementation is a core process in the Supplier's Quality System. The implementation process details a project methodology, procedures, templates, role descriptions, etc., tailored for projects that deal with the implementation of systems and services for new customers, or major changes for existing customers. Activities to be performed by the Supplier are described, as well as interfaces to activities/phases belonging to the Customer.

The Implementation Process does not cover in detail activities normally performed by the Customer; e.g. installation and test of applications, which are not to be managed by the Supplier according to the Agreement, migration activities, etc. In cases where the Supplier takes responsibility for such activities, these are performed according to general models for project management, and the activities must be planned in detail in collaboration with relevant personnel from the Customer during the project's planning phase.

The following figure gives an overview of the Supplier's project methodology, with a description of phases and milestones that are dependent on the Customer.

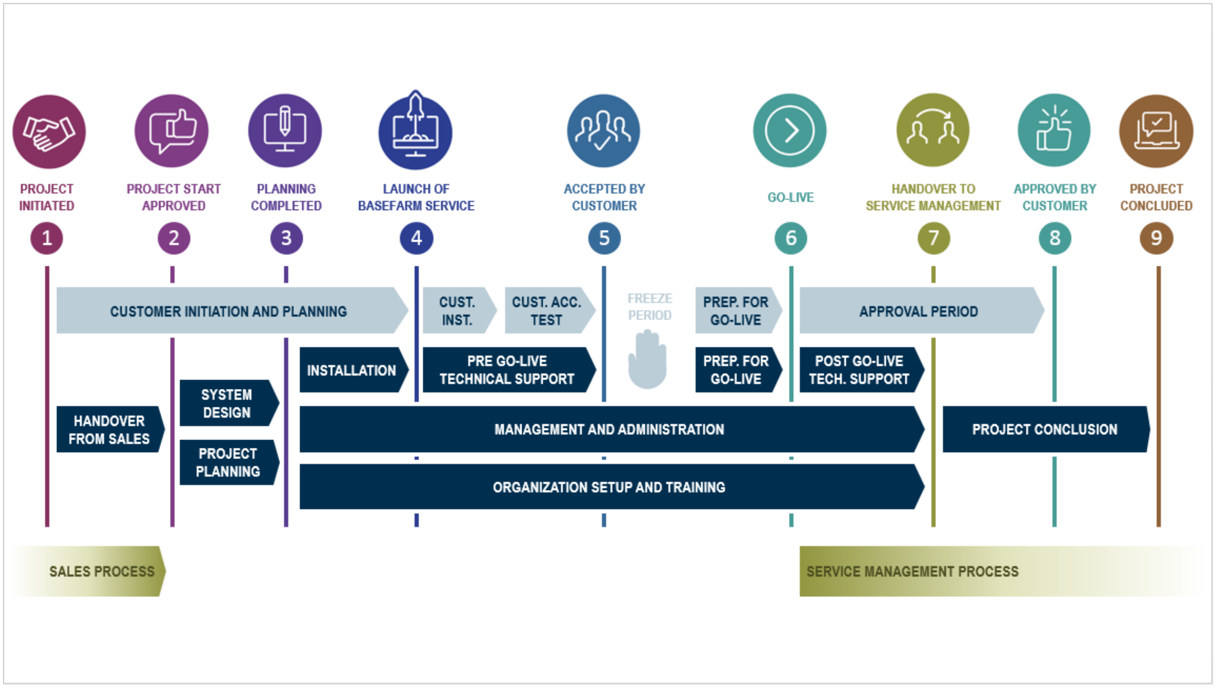


Figure 2: Basefarm's Project Methodology

The project is divided into the phases "Planning" (MS1-MS3), "Execution" (MS4 MS5), "Acceptance Test", "Start-up" (MS5-MS6) and "Approval "(MS6-MS8). Each phase is further divided according to the Supplier's implementation process. Each phase is described in more detail below.

Planning

The Planning phase has two parts. The first part includes preparing for project start in the Supplier's internal systems, and project resources are appointed. Following this, plans and design documentation sufficient for Supplier installation until MS4 are detailed. Any workshops and meetings (as considered necessary for the project in question) are held with the Customer to align plans and arrive at a common understanding of the detailed system design. When this planning is done, MS3 is achieved.

In addition to the planning of the Supplier's part of the Execution phase, planning of the Customer's part of the implementation will normally start already in the Planning phase. The Planning phase will include activities for the parties to work together on a detailed plan for activities necessary for transition from the existing Operations platform, focusing on ensuring a smooth transition and to avoid unnecessary disruption to the operational services. These planning activities will not be complete by MS3, but will be ongoing in parallel with other activities until just before MS6.

Principal test planning will also be performed during the planning phase.

Execution

The Execution phase is divided into two main parts:

Installation and test of the Operations Platform, including all elements covered by the Supplier's responsibility (after which MS4 is achieved)

Installation and test of customer specific applications on the Operations platform not included prior to MS4 (after which MS5 is achieved)

All elements in the Operations Platform that the Supplier will be responsible for will be implemented in the first part of the Execution phase, including installation and test of hardware, network and OS configuration, and basic installation of agreed software without Customer-specific configuration. The Supplier's standard monitoring and backup setup, and test of all basic services (BOT) will also be performed in this phase.

MS4 is achieved when the Operations Platform have been installed with all elements for which the Supplier is responsible, test has been executed and approved, and the Customer has verified that necessary access has been given.

In the second part of the Execution phase all Customer applications will be installed and configured, according to Customer requirements. This phase includes all work performed by the Customer (or by third parties on behalf of the Customer) on the Operations Platform, prior to the Customer Acceptance Test and Go-Live.

The Parties will also agree on configuration of any application specific monitoring and backup, beyond what is included in the Supplier's basic Operational services. Any additional monitoring and backup will be configured prior to the Customer Acceptance Test.

Customer Acceptance Test

After the Customer's applications have been installed and all Customer-specific configuration of the Operations Platform have been performed, the Customer Acceptance Test phase begins. The Customer is responsible for the Acceptance Test and associated activities. The Supplier can assist in this phase if needed. The Parties will agree the scope and nature of such assistance.

During the Customer's Acceptance Test phase, the Parties jointly complete the planning of Start-Up activities.

MS5 is achieved once the Parties agree that the Operations Platform is ready to go live.

Start-up

The Supplier's implementation process includes a freeze period before MS6. This is to be able to verify that the Operations Platform is stable before it goes live.

The Start-up phase includes necessary activities to put the Operations Platform into production (start-up of normal operations). Any operational services that up to this point have been configured but not initiated, such as monitoring, will be activated.

MS6 is achieved once the Operations Platform and related operational services are fully activated in accordance with the Agreement.

Approval

The Approval phase is a time-limited period directly following Start-up in which the Parties verify that the Operations Platform and related services work as intended.

The Supplier assumes full operational responsibility during this phase. Since it is not possible to test the Operations Platform under ordinary production conditions prior to Start-up, SLA refunds are not applicable for the duration of the Approval phase, which ends with the achievement of MS8. Unless otherwise agreed, the duration of the Approval phase is two calendar weeks.

During the Approval phase, the Supplier's project organization will hand over the Operations Platform to the operations organization. The project organization will assist the operations organization throughout the Approval period, to ensure the necessary transfer of expertise and completion of necessary customer-specific routines before MS8 is achieved.

Project closure

The implementation project is closed after MS8, pursuant to internal final reporting and wind-up meetings. A Customer satisfaction survey related to the project's performance is also conducted before the project is formally completed.

Limitations:

- Unless otherwise agreed, the Supplier does not assume responsibility for the test of end-user services or Customer application functionality.
- The Supplier does not assume responsibility for functional errors or deficiencies resulting from the Customer's application.
- Any additions to originally agreed project scope, which are identified and/or started but not, completed during the implementation project, shall not be considered as a factor in the Customer's Approval of the project.

Prerequisites:

- The following assumptions applies for the execution of the implementation project:
- That the Customer participates in a kick-off meeting, and actively contributes to the creation of a realistic progress plan for the project.
- That the Customer will be involved in initial planning with regards to necessary input for the detailed design of the Operations Platform and specification of technical requirements. Additional requirements that change the design agreed in the Contract, or which are presented after the detailed design is completed, must be handled as changes and may be invoiced in addition to any previously agreed price.
- That the customer appoint technical and administrative personnel to interface with the Supplier, and that these reply to questions from the Supplier without undue delay throughout the project.
- That the Customer provide estimates of expected usage of the Operations Platform (usage patterns and volume) to the Supplier, in due time to be used as input to design specification and considerations related to scaling of services.
- That the Customer, in the event of delays to project progress as a result of the Customer's activities, cover the Supplier's work and any other costs related to the delays.
- That the Customer perform, or ensure that Customer's third parties perform, the Customer's activities in the period between MS4 and MS6.
- That the Customer, without undue delay, inform the Supplier of any errors or deviations discovered, so that these can be corrected with the least possible impact to the agreed project progress.

C. SECURITY SERVICES

Basefarm has more than 500 experts helping more than 400 customers (companies and organizations) in Europe delivering digital innovation to more than 40 million end-users worldwide. Over the past 18 years Basefarm has proved its capability in operating critical solutions in an efficient way. Our expertise and experience in operating services with high focus on security requirements makes us a leading IT company in the market.

Most of our customers demand the highest possible security level. Basefarm's security personnel have extensive experience with the many aspects of internet-related security. Because we specialize in the operation of business-critical digital services, security is included in everything we do, and that includes design, hardware, organization, and processes. Our Security Incident Response Team (SIRT) is a vital part of our proactive security work.

Basefarm cooperates closely with partners and maintains in-depth knowledge of their products and services. For instance, Basefarm is a Microsoft Gold Partner Hosting, HP Cloud Agile Select Partner, VMware Enterprise Solution Provider, VMware Service Provider Premier, VMware vCloud Powered Partner, NetApp Partner, EMC Alliance Partner, IBM Business Partner, Akamai NetAlliance Partner, and Oracle Gold Partner.

Security has always been a significant tool for any solution in Basefarm, for security products as IDS and SIEM solutions. We have partnership with Mnemonic, one of the leading security companies in Nordic market. Please check for more detailed info: https://www.mnemonic.no/managed-detection-and-response/

Basefarm is a trusted provider of managed security services to many influential customers in the Nordic market and other European countries, such as Norwegian Airline, Klarna, SJ (Statens Järnvägar), Flytoget, Payex, Mollie and many more. These leading companies are passing millions of various transactions on daily basis, and our professional security team in Basefarm has always been alerted to the threat.

C.1 Client SIEM – points for discussion

Before providing more details on the Basefarm IDS and SIEM/SOC services, we feel it is important to address the requirement to ship log source data to the customer SIEM.

Basefarm recommends their customers to get the most benefit from buying the Security Services from the same provider that also manages their services. Basefarm, when delivering both service areas, will have deep knowledge about the customer, their hosted infrastructure, services and their associated risks. That implies a significant advantage to do an excellent job in security.

Also, if we do find any security issues we are able to respond to these by applying fixes in the hosting infrastructure directly by ourselves. A 3rd party company providing only security services, will depend on someone else to for instance patch software to fix any security bugs.

This is a non-desirable situation since it has impact on both time, resources and processes/procedures.

Customers sometimes are worried about putting all their eggs in one basket, and want a clear separation of duties between managed operation services and managed security.

We are clear about the fact that the Basefarm SecOps team is organizationally separated, and "independent" from the rest of the operational organization within Basefarm, including the customer teams.

C.2 IDS

For monitoring of the network and detection of security breaches Basefarm will place equipment with IDS functionality on a SPAN port or TAP in the customers datacenter. The SPAN port or TAP will mirror traffic from targeted VLANs and forward to the IDS device, allowing the device to monitor the network traffic.

The IDS device is initially expected to be configured on ports configured in tap mode. Ports configured in tap mode allows for passively monitoring of the traffic flows across the network by way of a switch SPAN or mirror port. Also possible is using a network tap or a packet broker copying traffic to the appliance.

Basefarm will operate and perform security monitoring/reporting 24/7/365 of the IDS device. This security incident detection and network monitoring service has the following functions, described in more detail in the sections below

DEVICE MANAGEMENT **- HEALTH & AVAILABILITY MONITORING** **- DEVICE INCIDENT MANAGEMENT** **- CHANGE MANAGEMENT**	✓
Provider developed signatures	✓
Log Management	✓
Security Analysis by Analysis Engine	✓
Security Incident Reporting	✓
Validation and Enrichment by Security Analyst	✓

The Advanced Analytics service offer advanced detection and response capabilities to meet today's advanced and evasive Threat Actors. The Advanced Analytics Engine applies a mixture of traditional threat detection techniques (e.g. Correlation, Pattern matching, Reputation feeds) in combination with Advanced Analytics (e.g. Machine Learning, Statistical modeling, Kill-Chain Modelling) and Threat Intelligence, which jointly minimizes the risk of breaches going unnoticed.

In addition to monitor the IDS function, the security incident detection and network monitoring service can be extended with the Advanced Analytics service and correlate the IDS alarms with other functions from the analyze unit. This requires additional services.

C.2.1 Provider developed IDS signatures

Special assigned teams are actively tracking the Threat Landscape (e.g. Monitoring for activity of new/existing adversaries, research and evaluation of unknown threats) to constantly enhance the detection capabilities provided by the proprietary Analysis Engine used to detect security incident breaches, or that of monitored security devices. The SOC teams create signatures for supported IDS vendors and rules as the result of daily operational delivery and monitoring the threat landscape.

C.3 SIEM/Log management

C.3.1 Log Collection

Logs are collected from all customer devices in scope for the contract. Standard pricing as offered does include three log sources. Additional log sources can be added against additional fees.

C.3.2 Log Indexing

The collected logs are indexed to provide the ability for the Analysis Engine and Security Analysts to find and investigate potential security incidents in a timely fashion. Fields are extracted from the logs according to the Provider's standards for the various source types.

C.3.3 Log Retention

The logs are stored in original format. Logs can be made available for download to help the customer meet compliance objectives and forensic investigations. Retention period will be defined by the customer and the Provider prior to the service enrolment. Details regarding the retention period need to be discussed in detail.

C.3.4 Penetration tests/vulnerability scanning

Included in the Providers penetration tests and vulnerability scanning is a test report that is presented and delivered to the Customer, which minimum contains:

1. Executive Summary
2. Description of the scope and any agreed refine the test had
3. Description of the methods used
4. Overview of the findings made
5. Any errors identified are being considered by CVSS standard
6. Recommended actions

In addition to the report an excel spreadsheet will be delivered with the report's content in a concentrated and listed form. The spreadsheet expands each vulnerability with IP / DNS / URL, criticality, category, detailed information about the vulnerability, suggestions for improvement and any references. It is intended as a tool for customer when vulnerabilities should be closed.

All safety findings are continuously documented and stored in a secure manner with a view to simplification and reuse of results in subsequent tests, comparisons (delta) and statistics for the number and type of findings over time. The final report will contain enough detail for the customer (technicians) to understand the findings made and be able to correct them. The report is well structured and presents findings in clear and straightforward in a summary.

C.4 Physical and logical Security

The Provider employs the highest level of security and controls surrounding its premise systems and technologies. To accomplish this the Provider have implemented a series of physical and logical access control measures designed to ensure only authorized personnel have access to these critical business services, technologies and locations. Premises owned or managed by the Provider will be protected from unauthorized access. Technologies will be in place to ensure we are able to identify, authenticate and monitor access as appropriate for each site.

Logically alert data is automatically tagged with Customer name/ID and stored in separate tables to ensure data separation. This does not however impede the security analysts from providing alert cross correlation between clients to investigate if more than one customer is a target for a specific threat.

Procedurally, all customer incident report goes through a two steps verification before they get sent. The first step is automated and checks that no other customer name is included in the incident report. The second step is an eyes on glass review by the security analyst.

C.5 Certification

Basefarm is currently undergoing SOC2 Type II certification which has controls for data separation and privacy. Certification is scheduled for this year (2018) and reporting will be available from 2019. Basefarm is also finishing the ISAE3402 type II accreditation and will be able to provide ISAE Type II reporting covering 2018.

Basefarm's customer portal and undelaying ticketing system is penetration tested on a regular basis and audited as a part of Basefarm's ISO27001 certification.