Security and Operating Concept for the SupplyOn Platform (SBK5.1)

Version 5.1
June 2022

Your Supply Chain
Empowered. Connected. Visible. End-to-end.

Table of Contents

Index of Tables

Index of Figures

Index of Abbreviations

AG	German stock corporation
BMZ	Central fire alarm system
CIO	Chief Information Officer
CS	Computer-based Systems
CNST	China Standard Time (UTC +8)
D-U-N-S	Data Universal Numbering System (by Bisnode Dun & Bradstreet)
EAI	Enterprise Application Integration
EDI	Electronic Data Interchange
EDIFACT	Electronic Data Interchange For Administration, Commerce and Transport
GDPR	General Data Protection Regulation
UC	Utility Company
HTTPS	HyperText Transfer Protocol Secure
IPS	Intrusion Prevention System
IMS	Integrated Management System
IP	Internet Protocol
ITIL	IT Infrastructure Library
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
JST	Japan Standard Time (UTC +9)
KST	Korea Standard Time (UTC +9)
LAN	Local Area Network
CET	Central European Time (UTC +1)
CEST	Central European Summer Time (UTC +2)
OFTP	Odette File Transfer Protocol
PIN	Personal Identification Number
DC	Data Center
SAN	Storage Area Network
SMS	Short Message Service
TLS	Transport Layer Security
TOM	Technical and Organizational Measure(s)
UPS	Uninterruptible Power Supply
UTC	Universal Time, Coordinated
VdS	German Association of Property Insurers
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network
XML	Extensible Markup Language

1 Introduction

1.1 Objective and Contents of the Document

This document provides an overview of the security concept and operation of the SupplyOn online platform.

Based on the technical architecture, the security and operating concept provides information on operation of the data center and of each of the SupplyOn Services, as well as on comprehensive functionalities such as registration and customer support. The document is also designed to enable technically-interested readers to make a sound assessment of operation and security.

The security and operating concept covers all SupplyOn Services. Any specific departures from and additions to individual SupplyOn Services are governed by the relevant service description.

The information on the security and operating concept should not be regarded as independent or dependent warranties from SupplyOn.

In addition to the present document, the current version of “SupplyOn AG General Terms & Conditions for SupplyOn Services", referred to below as "GTCs", also applies and is an integral part of the contract. The definitions in the GTCs apply to this document accordingly.

The organizational measures, technical solutions, and process specifications described reflect the state-of-the-art and are subject to ongoing development by SupplyOn. The present document is therefore subject to changes resulting from ongoing development. The rules governing changes to the General Terms & Conditions apply equally to document modifications.

1.2 Security and Operating Principles of the SupplyOn Services

Users exchange business and personal data via the SupplyOn Services. When processing these data, SupplyOn has following objectives:

- **Confidentiality**
- **Integrity**
- **Availability**

SupplyOn has implemented extensive organizational measures, technical solutions and process specifications in order to prevent, as possible, security and operating incidents and minimize negative impact. However, there is no such thing as absolute security, either in the electronic or the conventional exchange of data. But a high security level can be achieved through essential measures, such as the use of current encryption technologies, certification according to ISO 27001, the integration of security experts and also the ongoing development of security concepts.

1.3 Data Protection and Business Secrets

On the platform, SupplyOn processes personal data in accordance with applicable data protection regulations (GDPR). These are primarily contact details for the contact persons of the customers. No sensitive personal data is stored or processed on the platform.

This security and operating concept describes the technical and organizational measures. Further key security-relevant processes deployed when handling personal data are also described. Where a customer uses the platform to process business secrets, SupplyOn shall not be obliged to take further measures to protect such business secrets beyond the measures set out in this document.

SupplyOn ensures that appropriate confidentiality and data protection provisions are agreed with all its technology partners.

2 Security Concept

2.1 Key Measures

The following key measures are taken in order to achieve the objectives of the security and operating concept.

Confidentiality: SupplyOn protects data transmission by means of strong encryption (at least 128-bit TLS) and protects access to the SupplyOn Services by means of user-specific accounts with user ID and password. The individual users are governed by a role concept that grants each and every user specific rights to use individual services and to access certain data. The role concept is defined for each of the services. SupplyOn deploys a multi-level firewall architecture to protect the systems and the data stored in the platform databases against unauthorized access from the outside.

Integrity: SupplyOn grants the various platform users specific rights to create and change data. Users are authorized to change specific data only. No unauthorized changes may be made.

Availability: SupplyOn Services are operated on a redundant server architecture and establishes redundant connections to various Internet backbones. Within the data center extensive technical concepts and measures are implemented in order to achieve the approved availability.

2.2 Organization Concept

SupplyOn has nominated a security officer with the following duties.

The security officer defines, develops, tests, implements and monitors the security concept, is responsible for its ongoing development, and coordinates external security audits.

The security officer also coordinates all security-relevant enquiries and suggestions submitted by customers and third parties. As the contact person, he/she also answers customer enquiries. He/she identifies any security-relevant incidents, gathers documentary evidence, investigates incidents, and proposes solutions. He/she evaluates new security technologies for potential use on the platform and also monitors the security standards agreed with the technology partners.

The security officer works in close collaboration with the data protection officer at SupplyOn and reports directly to the Management Board.

In case security-relevant problems have been identified and resolved, SupplyOn immediately informs the security officers of its customers, provided such officers have been nominated and this information has been requested. In such cases, the customers are informed of the actions taken and their causes in the form of an 8D Report (refer to section 5.10 for further information).

3 Technical Architecture of the SupplyOn Platform

3.1 Platform Architecture

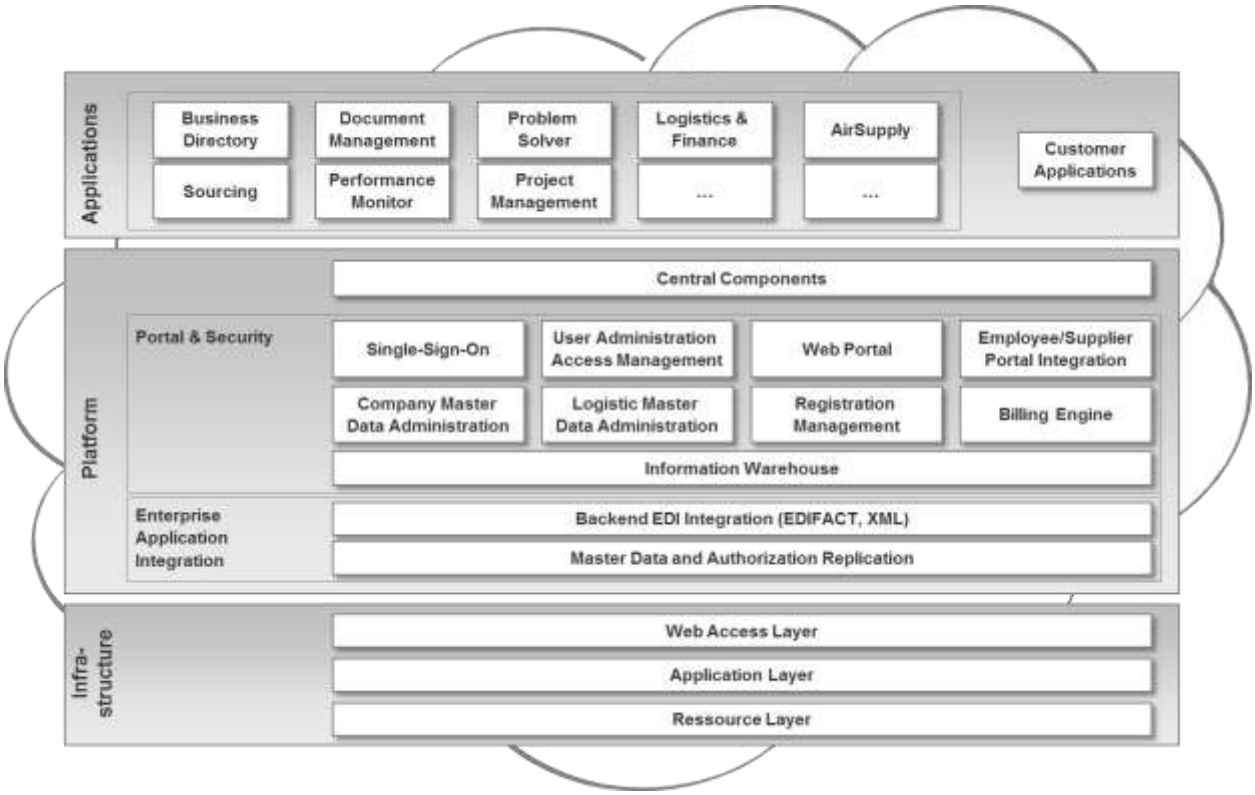

Figure 1: Platform Architecture

The individual SupplyOn Services (such as Sourcing) are operated on the basis of a central platform. This consists of the portal and security components, an information warehouse, and the Enterprise Application Integration (EAI) components.

3.1.1 Enterprise Application Integration Components

The Enterprise Application Integration components provide standardized integration interfaces for the backend systems of the customers (backend EDI integration (EDIFACT, XML)) and automatic replication of master data and user/roles/rights from the portal infrastructure to the individual SupplyOn applications (master data and authorization replication).

3.1.2 Portal and Security Components

The individual components of the portal infrastructure consist of the following functions:

- Web portal
  - Central point of entry to the SupplyOn platform and access to SupplyOn Services
  - Role-specific navigation menu
  - Portal integration with internal systems of customers
- Security
  - User authentication
  - Overarching role / authorization concept
  - User authentication and authorization in accordance with a uniform security policy

    - Single sign-on for all integrated SupplyOn Services, and portal integration with internal systems of customers
- User Management
    - Central administration of corporate users
    - Role-based assignment of user authorizations
    - Definition of password policies
- Master Data Management / Supply Chain Directory
    - Central management of the master data of all customers registered on the platform (organizational units) in the various hierarchy levels required for the SupplyOn Services
    - Additional management of all relevant logistics master data
    - Central management of the relationships between Buying Companies and Supplying Companies for all logistics processes (including routing information)
- Rollout and registration of Supplying Companies
    - Central management of all SupplyOn Services
    - Rollout and registration of Supplying Companies for specific SupplyOn Services, taking due account of data protection and security aspects
    - Current overview of the rollout status for Buying Companies
    - Overview of contracts and invoices for Supplying Companies
    - Control of master data replication

3.2 Technical Architecture

The key features of the technical architecture are described below.

3.2.1 System Landscapes

SupplyOn generally operates three completely separate system landscapes - a production system, a test system, and a development system.

3.2.2 Multi-Level System Architecture

SupplyOn uses modern systems in a multi-level system architecture. Web-, application-servers, middleware and databases are separated from each other. This enhances security, reduces complexity, and improves the scalability of the entire platform.

3.2.3 Scalability and Availability

The following measures are implemented to achieve the promised availability and to support flexible platform scaling.

- Use of redundant load balancers
- Scalable application server pools and database clusters
- Permanent availability of standby hardware
- Use of virtualization solutions to make best use of available hardware resources
- Use of a central, high-availability, mirrored SAN (Storage Area Network) for all customer-relevant data inventories

4 Data Center Operation (Hosting)

4.1 Security

4.1.1 Personnel

4.1.1.1 Data Protection

4.1.1.1.1 Data Protection Guidelines

The hosting partner has obliged all its employees to observe confidentiality. The IT security manager of the hosting partner draws up guidelines for the secure handling of data and is the customer contact for all issues relating to IT security.

The hosting partner has appointed an operational data protection officer. This officer is the contact for all issues regarding the processing of personal data.

4.1.1.1.2 Personnel

- Security checks of all hosting partner employees using appropriate procedures for the assignment of door keys and code cards
- Continuous checks of PC workstations and servers by means of virus scanners
- Non-disclosure clause in all labor contracts. These clauses cover all operational issues, particularly business and operational secrets, as well as the legal provisions regarding data protection.
- User setup only on written request
- Password changes at regular intervals
- Access to systems is granted only to persons with the necessary know-how
- Controlled de-registration procedure when employees leave a company

4.1.1.1.3 Physical Access Controls

- Physical access control to all security zones by means of code cards and electronic door locks

4.1.1.2 Access to Database Servers

- All access to database servers is via encrypted connections or dedicated administrator networks.
- Administrator network and data center network are strictly separated by means of a firewall cluster. Strong authentication at the firewall cluster and detailed logging are also implemented.

4.1.1.3 Remote Access

Remote access is handled very restrictively and secured via state-of-the-art mechanisms. Employees must also sign a comprehensive formal obligation.

4.1.1.4 Personnel Training

At regular intervals the hosting partner trains employees on the latest security technology developments and innovations. Employees are granted access to systems only after they have received adequate training. Employees must complete a training assessment form for each training session. This feedback is the basis for improving the training schedule. After a number of weeks, the hosting partner checks whether employees are able to put the knowledge acquired during training into practice.

4.1.2 External Communication Links

External communication links via public networks (Internet) are always encrypted.

4.1.3 Server Configuration

All servers are configured to ensure that only services required by the application or by administration are enabled and approved, and only accounts needed for administration are used.

Only personalized administrative accounts valid only for SupplyOn systems are used for access and for running application processes.

The hosting partner uses point-to-point interactive protocols with strong authentication and encryption for the administrator access and for operation.

The hosting partner eliminates security-relevant operating system weaknesses without delay by installing relevant manufacturer patches. Less critical weaknesses are eliminated by installing patches during normal operation.

An external service provider regularly runs a security check on all servers accessible via the Internet to identify potential weaknesses that can be exploited from the outside (see section 4.1.12).

4.1.4 Network Architecture

With regard to the network architecture of the SupplyOn Services, a distinction is made between application servers and database servers. Connections are uniquely defined by precise component parameterization and corresponding access restrictions.

4.1.5 Load Balancers

Load balancers distribute access operations across the downstream servers, and are core elements of a high-availability architecture. Existing resources can be used optimal because the load balancers permanently monitor server status and distribute data traffic to servers with free capacity. In addition, TLS connections are terminated at the load balancer and therefore reduce the load on the servers.

4.1.6 Internet Connection

The Internet connection of the SupplyOn systems is appropriately dimensioned and designed for high availability.

4.1.7 Monitoring and Alerting

A system management tool is deployed for automated system monitoring. All operating system and database statuses as well as application processes and log files are continuously monitored and messages are sent to a central console (Single Point of Control). Outside attended service hours, alerts are sent to on-call service units using short text messages. The hosting partner is therefore quickly informed of potential faults and is able to take immediate action.

All computers and network components are monitored automatically by administrators around the clock, also on weekends and public holidays.

All problems are recorded in a trouble ticket system and are processed according to priority level.

4.1.8 Log Entries

All operating activities on the servers are automatically logged. The hosting partner retains the operating system log entries for at least 30 days.

4.1.9 Firewalls

Firewall systems are used as central security components. Firewalls restrict communication connections and access operations to the individual systems. Firewalls allow only connections that are absolutely necessary. All connections not explicitly permitted by the firewall filter rules are blocked. HTTPS is used exclusively as the communication protocol between SupplyOn Services and the web browser of customers.

The system landscape is protected by a multi-level firewall architecture designed exclusively for the SupplyOn systems.

Two redundant, and therefore highly available, firewall systems are deployed and each performs different functions. The first external firewall, the frontend firewall at the Internet end, protects systems with public access. All systems publicly accessible from the Internet are integrated in a network segment at this firewall. The security requirements for such systems are lower because no data is maintained on them.

The second firewall system, the backend firewall, protects the data on the database servers. The production database servers are connected to the backend firewall via a dedicated network segment.

The application servers are also integrated into the backend firewall. These are thus protected against access from the Internet by the external firewall. The internal firewall restricts connections between the application servers and the database servers.

The databases are separated from the web servers by a second firewall. If the web server is attacked, the data remains encapsulated and is still protected on the server.

The firewall protects the production network against the internal network of the hosting partner. Administrators access the servers of the platform via this firewall. Administrator access to the firewalls is protected by means of two-factor authentication using tokens.

The described firewall infrastructure permits setup of various network segments for server operation. The segments offer different security levels for the systems. All publicly accessible systems are operated in a separate network segment. The database servers with the highest security requirements are protected by two firewall systems.

Server-based routing firewalls are used. A specially hardened operating system is deployed for the firewalls. The hardware is redundant and operates in hot standby mode. In the event of malfunction, the hot standby system automatically assumes full functionality via the VRRP protocol.

All firewalls are managed centrally. The firewall policies are maintained on the management station and are distributed and installed on the firewall gateways from there. All firewalls send their log files to the management station where the logs are managed. The firewalls operate as package filters and perform dynamic filtering.

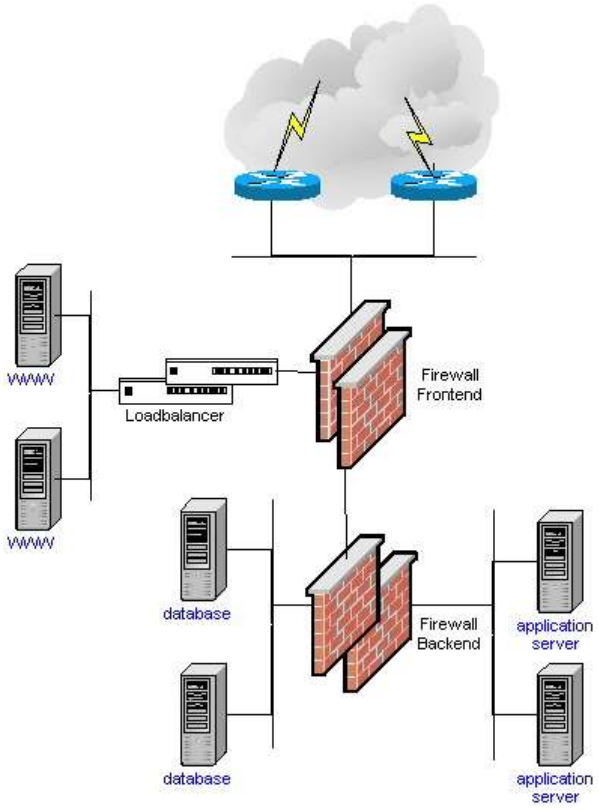

Figure 2: Firewall Systems

All firewall policies are based on the principle that all accesses are initially forbidden and individual accesses are permitted step by step in line with requirements.

4.1.10 Virus Protection

All incoming e-mails on the mail servers in the administration network are checked for viruses by default. The virus scanners used are updated regularly. Administrators are included on the update and information lists of the manufacturers of standard antivirus applications, and are therefore given timely notification of new viruses and appropriate remedial actions.

4.1.11 Intrusion Detection/Prevention

Special tools for automatic intrusion detection and prevention are used at SupplyOn. Regular updates of the signature databases minimize the risk of successful attacks. The hosting partner deploys intrusion detection/prevention systems (IDS/IPS) at the central transitions to the Internet. The systems operate on a network basis and analyze the associated data. In addition, a further IDS/IPS system tailored specifically to requirements of SupplyOn is used. IPS system messages are sent to a central management system where they are processed immediately. Detailed reports are generated regularly. The hosting partner and SupplyOn discuss and decide on appropriate rule changes on the basis of the reports.

4.1.12 Vulnerability Scans

Vulnerability scans are run at regular intervals on all servers accessible from the Internet. Additional scans are run whenever new security vulnerabilities are identified on the Internet. The vulnerability scan software is updated regularly to check potentially affected systems for new security vulnerabilities.

Security vulnerabilities detected during a scan are forwarded to system managers without delay. The system managers are given precise information on the vulnerabilities as well as detailed instructions on how to eliminate them.

4.1.13 Application Tests

In addition to system and network scans, external specialists are commissioned regularly to run application tests.

The SupplyOn security officer coordinates these tests and ensures that the results are incorporated into the relevant SupplyOn processes and the required actions are taken.

4.1.14 Emergency Concept

The hosting partner has set up an emergency system with instructions for the “Manager on Duty”; the instructions specify who is responsible in the event of an emergency and who is to be contacted. These must be alarmed and informed in certain situations. Events such as fire, water ingress, power failure, and climate control failure are also covered by detailed instructions and rules of behavior.

The hosting partner conducts regular emergency exercises which are documented accordingly. Regular personnel training courses and simulated computer downtimes help improve system restart times.

If operation can no longer be maintained in one of the hosting partner's two data centers, a restart of the complete SupplyOn platform (equivalent to emergency operation) is performed within 48 hours with maximum data loss of one hour.

4.1.15 Audits

The data center and the operation of individual SupplyOn Services are audited regularly by external, independent auditors. In addition, all information security relevant processes within SupplyOn are audited. This is done once a year, internally by the security officer and externally by appropriate auditors.

4.2 Operation

4.2.1 General

The SupplyOn platform is hosted by a hosting partner at two distributed data centers.

The data centers of the hosting partner feature the latest security standards such as:

- UPS, emergency diesel generators as UPS backup
- Fire protection, fire alarm systems, moisture detectors
- Several fire control zones
- Physical access control with cards and additional PINs (security level graded according to Class C of the VdS) and restricted to authorized personnel
- Internal and external camera surveillance with infrared spotlights
- Guard and lockup service
- Burglar alarm with door contacts, alarm spiders on the windows
- All staff obligated to observe confidentiality
- Staff security checks
- Redundant broadband Internet connections via several providers
- Redundant medium voltage supply via separate feed points
- Redundant climate control

Regular internal audits are conducted in the departments of the hosting partner. All management systems are operated in an IMS (Integrated Management System).

The hosting partner and its data centers are certified in accordance to relevant standards (including ISO 27001).

In addition to the process descriptions, operating manuals are also available for each individual system. These are listed as “Reference” documents in the quality management documents.

4.2.2 Water Protection

Moisture detectors are installed in all high-security areas in addition to optical smoke alarms and temperature sensors. The detectors feature continuous, moisture-sensitive wires. If moisture is present, the resistance in the wires changes and an alarm is triggered via the fire-proof and water-resistant fire alarm cable.

4.2.3 Fire Protection

- The entire high security area is equipped with T90-specification fire protection doors

- The individual fire compartments are separated in accordance with F90. This also applies for all cable penetrations.
- Separate data center rooms
- Two separate security zones for the WAN infrastructure in different sections of the building
- Separate utilities rooms (climate control, power, water, heating) in different sections of the building

4.2.3.1 Fire Alarm and Extinguishing Systems

- Central fire alarm system (BMZ) with connection to fire service; fire alarm sub-systems are fitted in all high-security rooms
- Optical smoke alarms in the suspended ceiling, double floor and in the rooms below the ceiling; to minimize false alarms, all smoke alarms are configured in a dual detector circuit; additional test chambers are fitted in the supply and waste air chambers
- Heat detectors to immediately detect temperature rises in high-security areas
- Manual call points in all monitored rooms
- Fault reports, warnings and alarms are transmitted from the building control system to a central information monitor in the reception area

4.2.3.2 Alarm System

In accordance with the applicable guidelines, the alarm system is configured as follows:

- All rooms are fitted with speakers that play-back automatic announcements in case of fire. The announcements relate first and foremost to how employees should evacuate the building.
- Optical display (alarm and malfunction) at the central fire alarm system and the central information monitor in the reception area, flashing displays indicating gas leaks via the room entrance, flashlights and loud sirens in the rooms
- Access to the fire service on line cards (fire service head cards) in the central fire alarm system
- Optical signal through revolving lights at the fire service access

4.2.4 Building Protection

The rooms for servers and disk storage, the backup room, and the rooms for the WAN infrastructure and the utilities rooms are separate. Access is controlled by means of inductive card readers for personnel cards, additional security devices (PIN code entry), and electronic door locks. Door safety ratings conform to Class C of the VdS.

The PIN code for data center access is changed at the start of each quarter. It is also changed immediately if an authorized employee loses his/her inductive card or leaves the company.

The company reception desk is always manned. A security information system is also installed at the desk. Alarms are received at an information monitor with labeled call buttons. The video monitors are permanently visible from the reception area. All installations reflect the state-of-the-art.

The following measures exist to protect the building envelope:

- Glass breakage detectors on first and second floors
- Video surveillance (five cameras with infrared spotlights and movement sensors)
- The guard service controls all keys – electrical access is controlled by authorized personnel
- Guard patrols at various times
- A single central entrance
- Secured cellar shafts
- Internal security control center
- Physical access control to the data center for visitors and employees of external companies (dual-control principle)
- Physical access rules and monitoring of the high-security areas by recording movement patterns

4.2.5 Power Supply

All systems and facilities operated in the high-security area are supplied via an online UPS. This means there is a physical separation between the power supply from the utilities companies and the UPS network (consisting of several separate UPS systems for the different data centers). Voltage fluctuations, power failures etc. therefore have no impact on operation in the high security area.

In the event of a power failure, the UPS switches in immediately (online UPS). A diesel generator is cascade-connected; this starts automatically after approx. 10 seconds, thus ensuring that the IT network and all devices in the network remain operational. For security reasons, CS units are always operated on the secondary side of the UPS and the diesel generators act as backup systems for the UPS batteries. The diesel fuel in the emergency power generators is sufficient for three days of independent operation.

4.2.6 Climate Control

The cooling installations are designed with the necessary redundancy. Maintenance contracts with the appropriate response times have been concluded for fault rectification. The components of the air-conditioning system are enclosed within fences and are continuously monitored by surveillance cameras. If possible, the water chillers of the air-conditioning systems are located on the flat roofs of the building.

4.2.7 Organization

4.2.7.1 Data Center Systems

All installed systems, servers, and network components are managed in a data center management system. Named persons have access to the management system in accordance with a defined authorization concept. The lifecycles of the facilities and components can also be tracked in the data center management system.

4.2.7.2 Partners

Maintenance contracts have been signed with the technology partners of the hosting partner. Appropriate reaction and response times have been agreed for each escalation level. Wherever possible, support calls are processed by telephone. If necessary, the partner's engineers provide on-site assistance under the supervision of a hosting partner employee.

Partners may enter the data center only by prior arrangement and after approval by the CIO and head of the relevant business unit. Partners must prove their identity by means of an official ID document. The hosting partner personnel must draw the attention of partners to the basic provisions of data privacy and to the security regulations. Partners must complete and sign a security declaration each time they enter the data center.

Partners may have access only via secure communication channels and are granted access authorization only for a requisite period of time agreed with the Support Center.

Access rights are configured specifically for each customer system. All external accesses are logged and are described in detail in the operations guides. Furthermore, the external partners of the hosting partner are obligated to observe confidentiality.

Remote access by partners is handled very restrictively. The process for authorizing remote access for partners is the same as for employees (see section 4.1.1.3). Access is authorized only as needed for a limited period and is also monitored.

4.2.8 Data Backup and Recovery

Databases and file systems are backed up so that lost or modified data can be recovered quickly.

4.2.8.1 Backup Infrastructure

The backup infrastructure is geographically separate (backup and archiving rooms are located in separate fire control zones) from the production systems of the platform. Automatic systems are used to perform backups. Backups are retained for a 2-week period.

Backup management is performed centrally. Log backups are cloned to enable point-in-time recovery at any time if a data medium is faulty.

The current backup status is kept at a geographically separate location.

Image copies of server system areas are created in addition to file system and database backups. These support rapid disaster recovery if a system configuration is destroyed. Dedicated emergency plans exist for necessary restore operations.

4.2.8.2 Database Backup

A full backup of the database serves as a safepoint. Archive copies are made three times a week. The archive log is backed up three times a day. If the database is destroyed, the associated data is fully recovered by restoring a full backup together with the subsequent archive log. The archive log size check and backup are carried out automatically and are monitored.

4.2.8.3 File System Backup

Central SAN storage units are used for all critical services. These permit excellent scalability if additional storage requirements arise. Disaster concepts with synchronous data mirroring are also easily implemented with SAN technology. Depending on availability requirements, local storage systems are also used for less critical applications.

A full backup of the file system is carried out once a week. In a full backup, all files are written to a backup data medium at a certain point in time. Status changes to the files since the last data backup are ignored. The backup interval of one week ensures that incremental backup effort is kept to an acceptable level.

An incremental backup is carried out daily to permit current backups. In an incremental backup, only data that has changed since the last backup is recorded. The combination of full and incremental backup ensures that current data can be restored.

4.2.9 Online Availability and Performance Measurement

SupplyOn and the hosting partner monitor the availability and performance of the individual SupplyOn Services by means of online measurements during which selected core processes of the individual SupplyOn Services run automatically.

All core processes run every 15 minutes. Consequently, availability problems at service level and performance problems can be identified quickly and appropriate remedial action can be taken.

5 SupplyOn Platform

5.1 System Landscapes

SupplyOn generally operates three separate system landscapes - a production system, a test system, and a development system.

5.1.1 Production System

The production system comprises the production and training environments. These are used as follows:

SupplyOn checks new customers and their administrators in the registration process. SupplyOn authorizes customers to use the selected SupplyOn Services only after they have been checked successfully. SupplyOn manages only companies and their customer administrators.

Dummy customers and dummy users are managed in the training environment. All transactions performed in the training environment are dummy transactions. The dummy customers and their customer administrators are managed exclusively by SupplyOn. Training sessions are conducted and demos are given in this environment.

5.1.2 Test System

SupplyOn tests both fault rectification measures and new releases on the test system. Intensive tests ensure that faults and errors do not compromise the production environment. After successful testing, released changes are transferred from the test system to the production environment.

Furthermore, the test system offers the customer the possibility to carry out connectivity projects and own customer tests independently of the production environment. Specific security measures for the production environment (e.g. IPS systems) do not apply to the test system.

The test system is only accessible to a restricted group of users consisting of SupplyOn, partners and customers. This is ensured by separate authentication at network level by means of IP access control or firewall password.

It may be that the functionality on the test system still has undetected errors that could lead to unauthorized access by other users, as this system is also used for security tests prior to go-live.

For this reason, Customers are advised to use only test data without any need for protection (in particular no real personal data) on the test system. SupplyOn shall not assume any liability for breaches of confidentiality of data requiring protection in the test system.

5.1.3 Development System

Ongoing development of the central platform infrastructure and of the individual SupplyOn Services as well as quality assurance of development activities take place on the development system.

5.2 Software Logistics Process

Software development and development quality assurance are carried out on the development system. The software is then installed on the test system by the software partner. The hosting partner ensures, through appropriate documentation and processes, that the software partner documents all changes and modifications in the test environment. SupplyOn then performs software testing in this environment. Testing includes functional tests, performance tests, load tests, security tests, and operating tests. SupplyOn does not release software until it has been tested successfully.

The hosting partner then installs the software on the production system. Software installation is usually supported by a software partner. Again, SupplyOn performs testing before the environment is released for production operation. All changes to the production system are made in such a way that they can be fully reversed if problems occur.

5.3 Operating Processes

The operating processes and operating organization at SupplyOn are – as far as practicable – based on ITIL. This applies particularly to the Service Desk, Incident Management, Problem Management, Change Management, Release Management and Configuration Management processes.

5.4 Release Management

Ongoing development of the SupplyOn Services is planned in close collaboration with customers. Customers are able to submit suggestions for improvement to SupplyOn. SupplyOn assesses such suggestions and provides feedback on the further course of action. Customers are given timely notification of the scheduling, development, and going live of new releases.

5.5 Availability

Availability relates to usability of the SupplyOn Services at the transition point of SupplyOn to the Internet or other communication networks for which SupplyOn is not responsible. This also applies for the connection of additional SaaS solutions of partners (e.g. EDI connection of carriers). The following types of downtime are ignored when determining availability:

- Downtimes due to all forms of force majeure
- Downtimes due to computer crime
- Non-fulfillment or violation of the customer's duty to cooperate
- Downtimes or malfunctions of the Internet or communication networks

SupplyOn provides the individual services on the production system with a defined monthly availability percentage, this percentage figure is relating to a defined time window.
Unless stated otherwise in the individual service descriptions, the following values apply:

Availability	99 %
Time window	Mon-Sun 00:00-24:00 hrs CET/CEST

Table 1: Availability of Production System

The time needed to restart the production system after a malfunction is usually not more than four hours.

SupplyOn provides a monthly availability report for the SupplyOn Services.

5.6 Maintenance Windows

Downtimes as a result of regular scheduled maintenance windows and additional maintenance windows are ignored when determining availability. SupplyOn gives quarterly advance notification of all regular, scheduled maintenance windows at least one month before the end of the previous quarter. If, particularly in the case of maintenance windows combined with go-live dates for releases, changes are subsequently required in the course of detailed planning, such changes are notified in advance no later than one week prior to the start of the maintenance window.

Regular, scheduled maintenance windows for SupplyOn Services
The time period for maintenance windows extends from

- Saturday 20:00 hrs to Sunday 18:00 hrs CET/CEST, or from
- Sunday 07:00 hrs to Sunday 23:00 hrs CET/CEST.

Additional maintenance windows
Only in exceptional circumstances may SupplyOn require maintenance windows in addition to regular scheduled maintenance windows without the associated downtimes being included in the determination of availability. Advance notification must be given by SupplyOn at least one week prior to the start of the maintenance window. If the customer agrees to additional maintenance windows, the associated downtimes are ignored when determining availability. The customer nominates a contact who is authorized to approve additional maintenance windows for each service. Customer approval is deemed to have been granted if the contact fails to respond within three working days following advance notification by SupplyOn.

Emergency maintenance window
If achievement of the security and operating targets of the SupplyOn Services (see section 1.2) is seriously at risk due to a critical security or operating weakness, SupplyOn will take immediate action by performing any necessary measures to minimize potential damage for customers during an emergency maintenance window.

A critical, high-risk security weakness is present if exploitation of the weakness could lead to serious damage and if SupplyOn is of the opinion that there is a realistic probability of exploitation. The same applies if there are indications that the weakness has already been exploited. SupplyOn will supply information on necessary emergency maintenance windows and on any actions the customer must take immediately to minimize damage.

5.7 Registration Process

To connect a Supplying Company to SupplyOn, the Buying Company selects - during application rollout - the corresponding SupplyOn Services via which communication is to take place with the Supplying Company, and specifies the corresponding D-U-N-S number, the company, the company' address, and a contact person. Alternatively, it is possible to upload several data records.

Using the data provided, SupplyOn verifies the identity of the named Supplying Company and checks whether the company is already registered with SupplyOn.

If the Supplying Company is not yet registered with SupplyOn, once-only "PID registration" is carried out. The Supplying Company registers itself with its master data (based on the Odette PID standard), downloads the contract document at the end of the registration process, and sends the signed document to SupplyOn. After SupplyOn has successfully checked the contract, the company is authorized to use the "connects" confirmed during registration. A "connect" is a connection established between a Supplying and a Buying Company via a SupplyOn Service.

If the Supplying Company is already registered with SupplyOn at the time of rollout, the corresponding connect can be confirmed directly online and can be used without delay, providing no additional configuration work is required.

5.8 User Management, Authentication and Authorization

5.8.1 User Management

In accordance with the concept of delegated user management at SupplyOn, the customer administrator deploys central user management to manage users of the relevant organizational unit. The administrator is nominated when the customer is registered. Administrator tasks include the following:

- Creation, maintenance and deletion of users and their master data
- Assignment of roles to users
- Locking and unlocking users
- Maintenance of customer master data (address, contact person)
- Creation of further administrators at the customer end

If requested by the customer, it is possible to share administrator authorization ("separation of duty") in order to support customer-internal checking of user administration processes. This allows an administrator to be assigned the authorization of only creating, changing, and deleting users and their master data. The other administrator can be assigned the authorization of only assigning roles to users. The approval of both administrators is needed to create new users in this constellation and authorize them access to data. A single administrator cannot therefore create new users with access authorization to data.

5.8.2 User Administration Teams

Within an organizational unit (legally independent unit), administrators are able to subdivide the unit for purposes of user management in administration teams. Users and administrators can then be assigned to these teams. An administrator assigned to a group may manage only the users in the group and may not create and manage any other groups. Administrators can therefore be created with responsibility only for a limited group of users within the organizational unit.

5.8.3 Group-Wide Access Concept

The group-wise access concept enables users to be granted access to business processes and data in several organizational units of the same group on the basis of a central user ID. Approval by the responsible administrator in the relevant organizational unit is required to grant such authorization. Users then have a central user ID that authorizes them to access business processes and data in multiple organizational units.

5.8.4 Authentication

Users are authenticated by user name and password. Authentication by means of 2-factor (2FA) authentication is also possible if requested by the customer. User name and password are transmitted in encrypted form. If certificate-based authentication is set up for the customer, the standard TLS protocol is used.

5.8.5 Authorization

Users have only the specific authorizations assigned to them. Following activation by SupplyOn, administrators are able to assign authorizations to users. Single users are not able to extend their own authorizations.

Administrators can lock users and unlock them after positive identification. SupplyOn documents the creation, modification, and locking of users so that it is possible to track which changes were made by whom and when.

5.8.6 Password Policy

The following password policy applies for the login procedure:

- Passwords must be at least 12 characters long
- Passwords must contain a special character, upper and lower case characters, and a digit
- Passwords expire after 90 days
- Old passwords may no longer be used when new passwords are assigned
- Passwords must not contain the name of the user
- Accounts are locked after three failed login attempts; there is no automatic unlock
- Initial passwords (new registration, password reassignment) must be changed at first login (system-controlled)

5.8.7 Password Reset Function

A user password can in any case be reset by the appropriate customer administrator or by a portal administrator. Passwords are reset by the customer administrator internally in the organizational unit of the relevant users. The portal administrator is involved by means of a call center ticket. Once a written (or e-mail) request including the relevant user ID has been received and the details have been checked, a new initial password is set and the user is informed accordingly by telephone. The user is given a new initial password for purposes of authentication. The user must replace the initial password with a new password at first login.

The platform also allows users to reset their own passwords without needing to contact the internal or portal administrator. Users are responsible for performing the password reset process.

The following customer-specific variants can be implemented for password reset in each organizational unit:

Variant 1 – Password reset is possible (default setting):
The password reset function is available to users in the organizational unit. To initiate password reset, users must specify their user ID and e-mail address stored in the system. The system then sends an e-mail to the users' stored e-mail address. The e-mail contains a unique access token with limited validity in the form of a link. When users follow the link, a page is displayed in which they can assign a new password for their user ID. Display is on an https-protected page. If the user ID is locked (e.g. due to unsuccessful login attempts), users cannot initiate the password reset process.

Variant 2 – Password reset is only possible after answering a security question:
The password reset process is similar to variant 1. However, before an e-mail is sent with the access token, users are confronted with a security question and an associated answer that must both be stored in the system. If users cannot answer the question correctly, the system terminates the process.

Only the customer administrator or a portal administrator can reset the password if no security question and answer is stored for a user in the system.

5.8.8 Access to Registration-Free Services

Buying Companies can decide individually whether Supplying Companies are able to make restricted use of individual processes of certain services without registration. These services are referred to as registration-free services. To do this, Buying company users enter on the SupplyOn platform the e-mail addresses of employees of a Supplying company that is not registered with SupplyOn.

These e-mail addresses are used by SupplyOn to notify the employees of the Supplying Company by e-mail of new transactions in a SupplyOn Service. Employees of the Supplying Company are granted access to a transaction by means of access information in the e-mail (e.g. a link) and can then process or respond to the transaction.

By means of random components in the access information, SupplyOn ensures that access information cannot easily be guessed by unauthorized third parties. In addition, access to business objects and transactions using registration-free services via web browser is https-protected. Depending on the particular registration-free service and the individual setting of the Buying Company, access can be protected by further means, such as:

- an additional prompt for a password prior to access to the transaction, or
- limited validity period of access information in the e-mail.

5.8.9 Session Management

Sessions are managed using temporary cookies. Session timeout is application-specific and is triggered by a mechanism controlled centrally via the portal. This mechanism logs users out after a defined period of inactivity or when they use the logout function.

5.8.10 SupplyOn Administrators

SupplyOn administrators perform a personalized, 2-factor (2FA) authentication-based logon to the SupplyOn platform.

5.9 Customer Support

5.9.1 Call Opening (Ticket)

SupplyOn Customer Support is organized as a central Service Desk and can be reached via a central telephone number and by e-mail.

Customers can communicate with SupplyOn Customer Support via the above channels. Customers should report backend integration problems by e-mail.

If customers open a call by e-mail, they should always add a prefix* in the subject line to identify the appropriate SupplyOn Service; they must also provide a brief description of the problem.

* Sourcing, Document Management, WebEDI, VMI, Problem Solver, Performance Monitor, Project Management, etc.

5.9.2 Authorized Call Personnel for Backend Integration

To ensure smooth support, the Buying Company must nominate personnel with call authorization for backend integration problem reports in the corresponding support agreements. Customers may amend these agreements at any time and send them to SupplyOn.

5.9.3 Enquiry Types

The following enquiries and reports must be submitted to SupplyOn via Customer Support:

- Software/application/functionality problems
- Availability problems
- Performance problems

SupplyOn can maintain agreed service levels only if customers use the defined communication channels.

5.9.4 Support Levels

Customer Support is based on the following multi-level concept:

- As **First Level Support,** the central Customer Support Hotline answers customer questions on technology and content that it is able to resolve. The Customer Support Hotline forwards problems that could not be solved to Second Level Support for clarification. The majority of customer problems can be resolved quickly thanks to the intensive training of First Level Support employees and current entries in a knowledge database.

- **Second Level Support** deals with specific questions on technology and content. If necessary, technical questions relating to operation of the relevant service or backend integration are forwarded to Third Level Support for clarification. Second Level Support employees are specialists in the relevant SupplyOn Services and/or backend integration.

- **Third Level Support** is provided by the technology partners of SupplyOn.

First Level Support is the direct and central point of contact for users. It calls in Second or Third Level Support where necessary and routes feedback to users. In exceptional cases, Second or Third Level Support may contact users directly for clarification purposes.

5.9.5 Call Tracking System

All enquiries are processed in the web-based SupplyOn Call Tracking System. All processing actions of SupplyOn and its technology partners are recorded in this system, and all system changes needed to resolve enquiries are logged together with the associated change approvals. This procedure complies with the ITIL processes for Incident Management, Problem Management, and Change Management. As a result, the entire process from enquiry receipt to enquiry resolution can be tracked and monitored transparently.

5.9.6 Priorities

Enquiries are classified by priority in consultation with the caller as follows:

- HIGH: System downtimes and problems that make the use of the platform impossible or significantly impair use of the platform for its intended purpose (e.g. platform cannot be used for multiple business transactions between Buying and Supplying Companies).

- MEDIUM: Problems that significantly impair use of the platform or do not adequately enable execution of a business process (e.g. platform cannot be used for individual business transactions between Buying and Supplying Companies).

- LOW: Problems that do not significantly impair use of the platform (e.g. minor functional faults that do not impair business processes).

5.9.7 Service Level

The following service levels apply for Customer Support:

Services	**Service Level**
Languages	German, English, French, Spanish, Portuguese, Chinese, Japanese, Korean
Availability (German, English)	Mon-Sun: 00:00-24:00 hrs CET/CEST
Availability (French, Spanish, Portuguese)	Mon-Fri: 06:00-20:00 hrs CET/CEST
Availability (Chinese, Japanese, Korean)	China: Mon-Fri: 08:00-17:00 hrs (CNST) Korea: Mon-Fri: 08:00-17:00 hrs (KST) Japan: Mon-Fri: 08:00-17:00 hrs (JST)
Call acceptance	80 % of incoming calls are answered within 20 seconds
Response times* acc. to priority level	HIGH: 2 hrs MEDIUM: 4 hrs LOW: 8 hrs
Service hours	For priority level HIGH: Mon-Sun: 00:00-24:00 hrs CET/CEST, except public holidays** For priority level MEDIUM/LOW: Mon-Fri: 08:00-18:00 hrs CET/CEST, except public holidays**

Table 2: Service Levels for Customer Support

* Within the specified response time, users receive qualified feedback with a proposed solution or an action plan which includes the next steps for solving the problem. The time needed by the customer or their business partners (suppliers, service providers, etc.) to supply information and times outside the corresponding service hours are not included in the response times.

** New Year (01.01.) and Christmas (25 and 26.12.)

5.9.8 Escalation Model

A three-level escalation model is used:

	Escalation level 1	**Escalation level 2**	**Escalation level 3**
Responsible	Customer Support Manager	IT Director	Chief Operations Officer

Table 3: Escalation Model

Escalation to escalation level 1 occurs if no action or inadequate action is taken within the defined response times. Escalation to the next escalation level occurs if the previous escalation level agent cannot be reached and/or if, due to the economic impact of the fault, urgent clarification or a redefinition of priorities is necessary.

SupplyOn provides details on escalation rules in a separate escalation concept and agrees these with the customer. The escalation roles of both parties are defined and the precise escalation topics and processes are specified.

Internally, SupplyOn also applies appropriate escalation concepts vis-à-vis the hosting partner and/or software partners.

5.9.9 Customer Information

In addition to processing and answering enquiries, Customer Support supplies customers with information on the following topics/events:

Topic / Event	Via e-mail	Via login pages	When	Information provided
Regular scheduled maintenance windows*	Buying Company: project manager, backend manager, key user***, company administrators***	All	See section on “Availability”	Date, scheduled duration, affected services
Additional scheduled maintenance windows*	See above	See above	1 week prior to start	Date, scheduled duration, affected services, reason
Short-term, unscheduled maintenance windows*	See above	See above	Immediately after notification	Date, scheduled duration, affected services, reason
Current service faults** expected to last longer than 15 mins.	See above	See above	Immediately after notification	Type of fault, expected duration (if known), affected services
Rectification of a current service fault	See above	See above	Immediately after rectification	End of fault, cause of fault (if already known)
Problems with backend integration, relative to individual messages	Buying Company: backend manager***	-	24 hrs. after occurrence, relative to 7x24 hrs (logistics), relative to service times (non-logistics)	Faulty EDI messages or XML files

Table 4: Customer Support Customer Information

* For details see section on “Availability”
** Non-availability of services or HIGH priority software problems
*** Project managers, key users and backend managers must be nominated in writing to SupplyOn.

5.9.10 System Requirements

Contract partners must satisfy certain technical requirements (e.g. use of approved browsers and browser versions) in order to use the SupplyOn Services via a browser interface. The current system requirements are listed in detail at the following Internet address: www.SupplyOn.com/requirements.

5.9.11 Monitoring Backend Integration

SupplyOn monitors the backend integration log and error files on the SupplyOn systems. If problems occur, SupplyOn first attempts to rectify the problems at the SupplyOn end. If the problems are not at the SupplyOn end and the customer has not already been notified by means of automatic error messages and/or error reports, SupplyOn informs the backend managers responsible for the individual backend interfaces of the customers about the faulty EDI messages or XML files or about incorrect configuration and, as far as possible, supplies the details needed to rectify the fault at the customer end (see section on Customer Information).

In this case, SupplyOn reserves to the right to invoice any costs incurred due to faults at the customer end.

5.9.12 Support Scope for Backend Integration

In the context of backend integration support, SupplyOn is responsible only for problems arising on the SupplyOn systems. SupplyOn's responsibility ends at the SupplyOn interface. This is either the point of transition to the Internet or the ISDN/OFTP interface (or vice-versa).

This expressly excludes internal systems of the customer and the communication paths between the customer and SupplyOn.

If a problem occurs with SupplyOn backend integration when a customer-own application is used, the user must first contact customer-internal IT support. If the customer's support team identify the cause as a fault in backend integration that is within SupplyOn's area of responsibility (as defined above), the customer support team member contacts SupplyOn Customer Support (First Level). Only the customer support team member with call authorization (see section 5.9.2) may report problems of this type. Only for problems relating to portal integration (Single-Sign-On via the SupplyOn Platform in internal systems), users have to contact directly the SupplyOn Customer Support, which will help find a solution with help from the customer-own support.

The employee with call authorization prequalifies the problem and also provides SupplyOn with all information needed to identify the nature of the problem and to confirm that the problem does not fall within the customer's area of responsibility (e.g. extracts from error or log files).

The processing of enquiries by SupplyOn is included in the scope of supply. Exceptions are defined in the relevant service descriptions. If such exceptions occur, SupplyOn explicitly notifies the customer during processing that the enquiry will be subject to a charge. The customer can then decide whether or not to use SupplyOn fee-based support to resolve the problem.

With some problems, it is not initially clear whether the cause lies with the customer or with SupplyOn. In this case, SupplyOn provides trouble shooting assistance to the customer as part of backend integration support. If it is established that the problem is within the customer's area of responsibility, SupplyOn reserves the right to invoice the costs incurred to the customer.

5.10 8D Report

SupplyOn generates an 8D report with the following information for all HIGH-priority system problems:

D1 Problem-solving team

D2 Problem description – monitoring and functional

D3 Immediate actions

D4 Cause analysis

D5 Potential remedial actions

D6 Implementation of remedial actions

D2 Preventive measures – monitoring and functional

D8 Concluding meeting

Usually the report is sent to the relevant customer within 14 days of problem occurrence.

6 Connection of External Platforms

In order to deliver certain services SupplyOn is connecting partner platforms. The security and operating concepts of partner platforms are not covered by the present document but are described in separate documents.