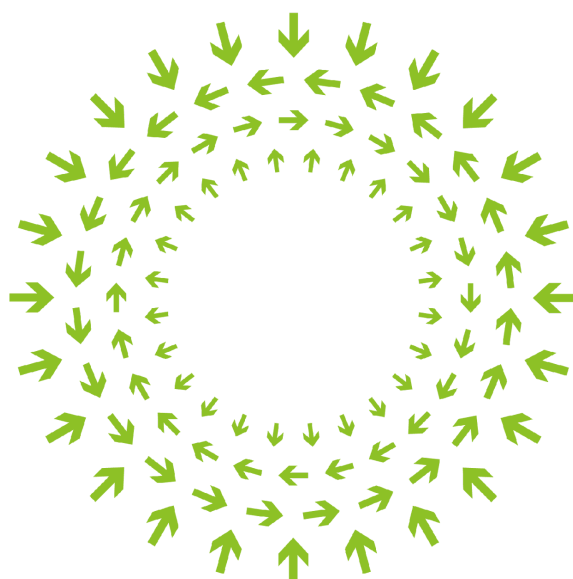




OPEN

Compute Project

f

Critical Facilities Operations Framework

Rev 2019 v1.5

Author: Coromatic Group AB

Table of Contents

TABLE OF CONTENTS	2
LICENSE	4
1 BACKGROUND	5
1.1 Framework alignment	5
1.2 Reviewal process for this document	5
1.3 The terms Customer and Supplier	5
1.4 Sourcing strategies	6
1.4.1 Model 1 – Single service outsourcing	6
1.4.2 Model 2 – Hybrid	6
1.4.3 Model 3 – Integrated site operations	7
2 OPERATIONS FRAMEWORK: GOVERNANCE MODEL	8
2.1 Management escalation and meetings	8
2.2 Integration of processes and governance through Transition	9
3 OPERATIONS FRAMEWORK: DELIVERY MODEL	11
3.1 Site Management function	11
3.1.1 Key roles for the Site Management function	11
3.2 On-site services	12
3.2.1 Key roles for on-site services	12
3.3 Delivery support	12
3.3.1 Service Desk 24/7/365	13
3.3.2 Governance	13
3.3.3 Advisory Services	13
3.3.4 Service Improvements	14
3.3.5 Supply chain and sourcing	15
3.3.6 Managed Operating Center – Remote Operations	15
4 SUMMARY OVERVIEW	16

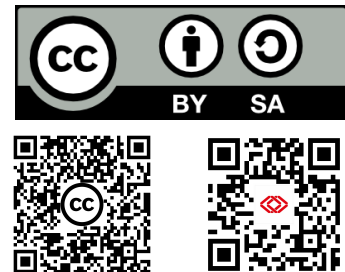
4.1	Site Management processes	16
4.1.1	Incident Management	16
4.1.2	Service Level Management	16
4.1.3	Lifecycle and Financial Management	16
4.1.4	Monitoring and Reporting	17
4.1.5	Work Orders and Project Management	18
4.1.6	Capacity Management and Optimization	18
4.1.7	Compliance Management	19
4.1.8	Document Management	19
4.1.9	Team and Suppliers Management	20
4.2	On-site services	21
4.2.1	Security and Access	21
4.2.2	Maintenance	22
4.2.3	Indoor/outdoor Facility Management	22
4.2.4	Site Inspections	22
4.2.5	Audits and Compliance reviews	23
4.2.6	Site Assistance	23
5	OCP CFOPS MINDMAP	24
6	OCP CFOPS TERMINOLOGY AND ACRONYMS LIST	24

License

This Work is licensed under the Creative Commons Attribution-ShareAlike 4.0 International License by:

Coromatic Group AB

The Work is based on an original concept by D Gjetrang and L Cardholm. Usage is governed by the terms and conditions set forth in the Creative Commons Attribution-ShareAlike 4.0 International License.



To view a copy of this license, visit <http://creativecommons.org/licenses/by-sa/4.0/> or send a letter to Creative Commons, PO Box 1866, Mountain View, CA 94042, USA.

Your use of this Work may be subject to other third-party rights. THIS WORK IS PROVIDED "AS IS." The contributors expressly disclaim any warranties (express, implied, or otherwise), including implied warranties of merchantability, non-infringement, fitness for a particular purpose, or title, related to the Work. The entire risk as to implementing or otherwise using the Work is assumed by the implementer and user. IN NO EVENT WILL ANY PARTY BE LIABLE TO ANY OTHER PARTY FOR LOST PROFITS OR ANY FORM OF INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER FROM ANY CAUSES OF ACTION OF ANY KIND WITH RESPECT TO THIS WORK OR ITS GOVERNING LICENSE, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), OR OTHERWISE, AND WHETHER OR NOT THE OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

1 Background

The datacenter industry is today responsible for driving innovation in one of the most mission critical functions many organizations rely on for their productivity; ensuring power and communication is constantly available to enable digitalization and efficiencies in production.

This organization relying on a fully functioning site may be in the ICT sector, but just as well in healthcare, retail or the financial services. Digitalization reaches well beyond data centers.

The sites have gone from bespoke technical rooms to standardized, open architecture facilities with designs based on the common accumulated wealth of experience.

To ensure resilience in operating such critical facilities, global best practices in business continuity, IT management and facility management should be leveraged.

1.1 Framework alignment

The Critical Facilities Operations Framework (CFOPS) is aligned with:

- OCP Ready™ Facility Recognition Program
- Process driven IT Service Management according to ITIL v4
- Operational practices in line with the criteria of EN 50600-x
- Uptime Institute's Tier Standard: Standard for Operational Sustainability
- Facilities Management practices in line with the principles of EN 15221-x
- Other industry experience and best practices, e.g. BICSI 009

1.2 Reviewal process for this document

The Critical Facilities Operations Framework is reviewed annually in accordance with the Guidelines for Document Management within the OCP DCF Project.

Stakeholder input is taken into consideration via experience-sharing within the community and is formalized through a public Change Proposal Form and Change Proposal Ledger. These are found at https://www.opencompute.org/wiki/Data_Center_Facility/CFOPS.

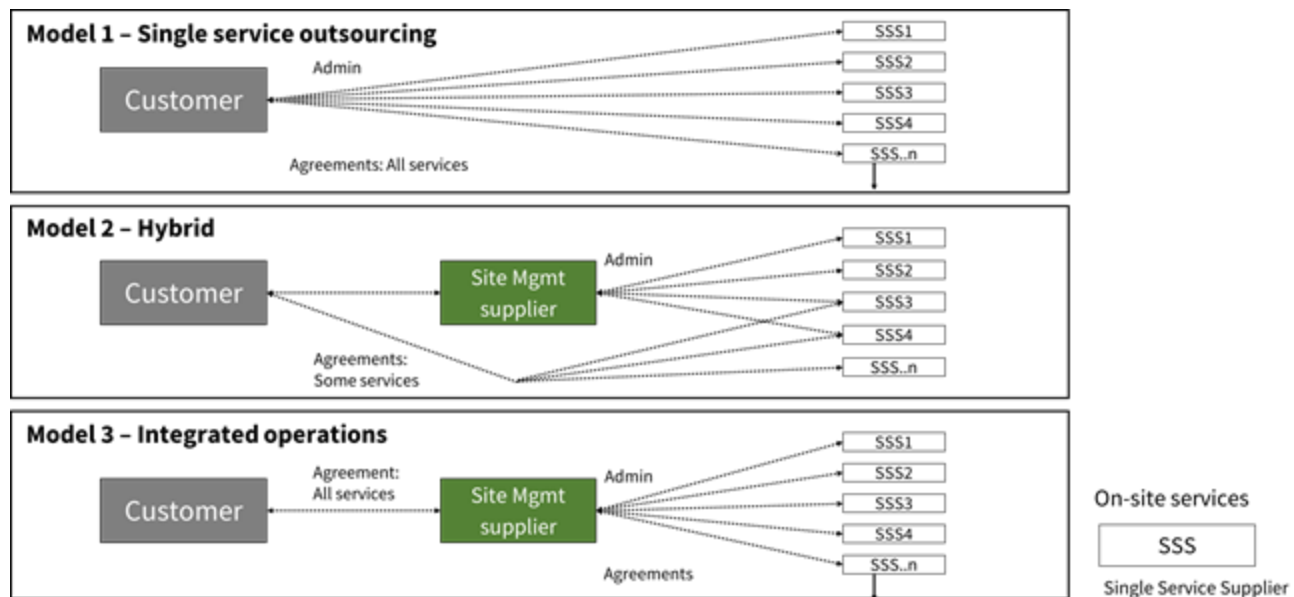
1.3 The terms Customer and Supplier

The terms “customer” and “supplier” are used to describe the relationship between demand and supply. This may be in-house resources delivering site services to other parts of the same organization or it could be outsourced to an external supplier.

In this context, external relationships could be exemplified by an OCP Ready operator and its tenant, while an internal relationship typically would mean that the customer representation comes from management and the supplier is from IT or RE/FM, or perhaps a combination of those functions. Regardless of which, the framework is built on the notion that the services provided are based on formal agreements between the parties, supported by defined service levels, border lists and governance structures for escalations etc.

1.4 Sourcing strategies

There are three different types of sourcing models in use for operations.



1.4.1 Model 1 – Single service outsourcing

The first model describes a customer with a multi-supplier sourcing approach. Single service suppliers provide the on-site services they are best suited for while the customer has a service management or operations function responsible for coordinating the suppliers.

This setup is to minimize risks of multiple service windows at the same time since the operations function coordinates the work, as well as having suppliers avoid performing services that could have a negative impact on other parts of the site configuration. The coordination is often handled via recurring performance and planning meetings.

The customer handles the procurement of services, annual ratings and price reviews of service suppliers, as well as financial and technical reviews of the actual services being planned and performed.

1.4.2 Model 2 – Hybrid

The second model is a hybrid of model 1, multi-supplier sourcing approach, and model 3, integrated operations. The customer has a main supplier providing site management services, which includes the responsibility for handling other suppliers within a pre-defined scope.

The site management supplier is responsible for minimizing the risk of multiple conflicting service windows as well as avoiding performing services that could have a negative impact on other parts of the site configuration by handling coordination of all on-site services that are in scope for the site management function.

The customer reaps the benefit of spending less time on coordination and follow-up in-house, while retaining control of certain services that are kept under direct sourcing, which the site management service supplier may not be best suited to handle.

The customer can still manage the procurement, annual ratings and price reviews of the site management and the on-site services.

Financial and technical reviews of the services can be done by the customer, unless the parties agree that this is also to be handled by the site management supplier, e.g. using the principles of “open book”. The principle of “open book” indicates that the site management supplier openly accounts for the cost levels and transparently adds its fees and margin levels for handling the on-site service providers, e.g. financial and technical reviews and recurring planning meetings on behalf of the customer organization.

1.4.3 Model 3 – Integrated site operations

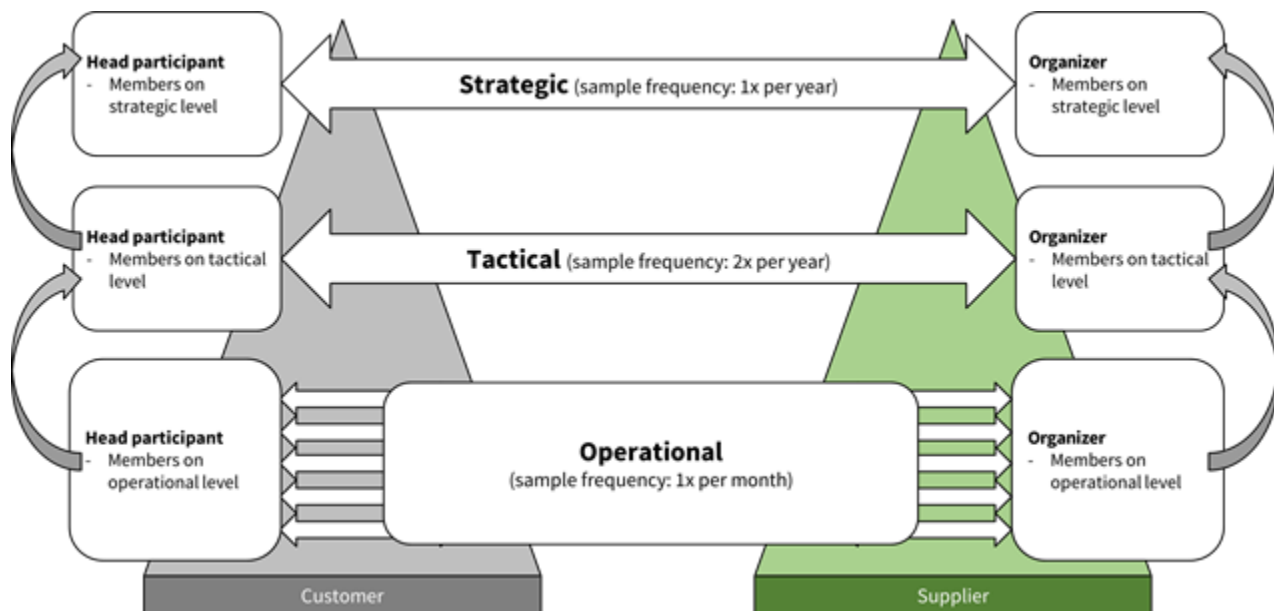
The third model, integrated site operations, means that the customer has a single service supplier handling all site related services and the governance of those at a given price structure.

This model may be in line with a pure demand-supply relationship at fixed or variable service fees, or it may be based on the integrated service supplier representing the customer in relationship to the on-site service suppliers with an “open book” approach or other fee structures.

2 Operations Framework: Governance model

The governance principles are based on the contracting parties leveraging three different layers of management and escalation: Operational, Tactical and Strategic.

The levels are populated with relevant stakeholders from both organizations. They meet at scheduled intervals to ensure customer satisfaction and seamless operations. The frequency of these meetings, and who should attend, is agreed for each contract.



2.1 Management escalation and meetings

The governance representatives for the parties are critical for the long-term efficiency of the sites in scope as they collaborate on improvements, handle change requests that affect the scope of the contract and resolve potential disputes.

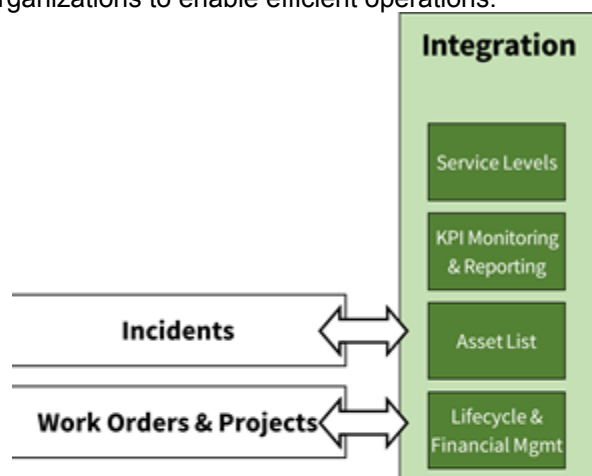
The governance protocols should therefore include that the parties inform each other immediately when representatives that are materially engaged in the governance of the services become unavailable or are replaced. With clear governance escalation mandates and protocols, the operational level teams are empowered to manage day-to-day matters whether it concerns risk, quality, environment, or compliance in other areas. This includes clearly defined service levels and penalties for non-performance which enables the parties to plan ahead and know what to expect in the contractual relationship.

Apart from these governance layers, it is not uncommon that the organizations agree to also have an annual event, where best practices, market outlooks and trends are shared between the working groups at all levels, as part of continuous improvements and collaboration.

2.2 Integration of processes and governance through Transition

The delivery requires integration of the parties' processes and governance structures to minimize risks and to secure continuous improvements. During the transition phase, the customer and the supplier align and integrate their processes, functions, systems and organizations to enable efficient operations.

The starting point should be the current site strategy set by the customer. The site strategy aims to align the actual capabilities with future demands of users and owners; it is not unusual with a life span of up to 30 years or more for a critical facility. During its initial planning, it may have other capability targets and expectations than in later stages. Technical requirements, demands for lowered environmental



impact and even the desired level of resilience can change during the sites lifetime.

To ensure minimized risks and transparency, the transition should be run as a clearly defined project that is led and quality assured by highly skilled and experienced transition specialists. In some instances, team members from the previous customer organization join a new supplier, while in other situations the organizations are kept as-is.

Besides technical resources, the site strategy needs to include a sourcing strategy for external suppliers. Relying on suppliers may in return require skills in project management and supplier management and will affect which processes to integrate with external parties.

Through a risk-based transition methodology the parties collaborate and ensure there is an agreed Statement of Work (SOW) which clarifies what services are included in the baseline and what services are available via separate service requests.

Key items formally confirmed and clarified before or during transition:

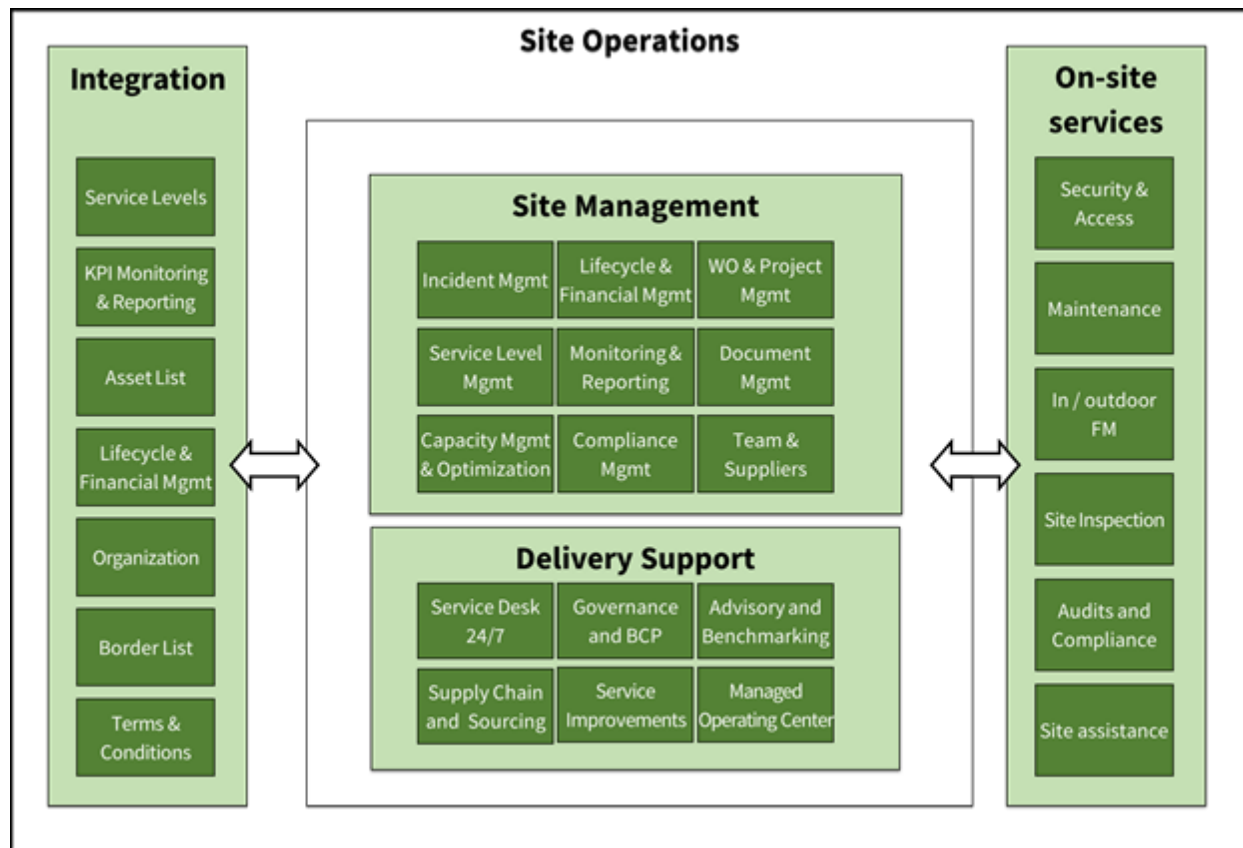
- Service levels and penalties in case of failure
- Asset Lists which clarifies the detailed scope for on-site services
- Border Lists where accountabilities and responsibilities are confirmed
- Organizational model for demand and supply with stakeholders and their dependencies
- Terms and conditions that regulate the provided services

Processes and systems clarified or integrated during the transition period:

- Incident management and Business Continuity Planning (BCP)
- Work Orders & Project Management
- Authentication and authorization management for on-site access
- Budgeting, lifecycle management and financial management
- Key Performance Indicators (KPIs) for Monitoring and reporting
- Annual plan for Site Operations and recurring governance meetings
- Collection of existing site policies and reference library elements for Document management and list missing information with due dates and accountable parties for completion

The most commonly integrated systems range from technical monitoring to physical access controls and security systems. Technical site monitoring is typically based on the underlying site infrastructure that communicate through standardized protocols, e.g. SNMP or ModBus.

3 Operations Framework: Delivery model



3.1 Site Management function

Site management is an off-site function that is accountable for managing overall activities pertaining to the site. This includes financial planning, service level management, performance monitoring and incident management for the site, and more.

3.1.1 Key roles for the Site Management function

Several roles exist and these may have different titles, but three main roles should be identified and assigned to ensure a resilient site management function.

- **Primary Site Manager** is appointed as the main contact for the customer and the primary source for understanding the contract scope and management of the sites.
- **Contract Manager** is supporting in improving the financials and service quality of the contracted deliveries. This includes validating change request consequences and collaborating with the customer on Tactical level.
- **Delivery support** is provided by other expertise required to fulfill the service level obligations, whether it is the 24/7 manned **Service Desk** or management advice provided by an external supplier of **Advisory Services** or other specialized services.

The roles should not be full-time roles for single individuals, but instead be appointed on a rolling schedule to avoid key person dependencies and ensure a broader view and experience on how to manage the specific site, or sites, in scope.

Service requests and planned works are scheduled by the site management team, while incidents or emergency access may be triggered directly through the incident process or via technical alarms.

3.2 On-site services

On-site services include all work that takes place physically on a site. This is regardless if it is manned with site engineers and site technicians or if it is un-manned and managed remotely with call-out times. The services include scheduled and requested work, as well as unplanned activities triggered by technical alarms or security incidents.

Intrusive or dangerous work on critical assets is performed under a permit to work system. Governance of these services, and approval of them, are determined in agreement with the customer.

3.2.1 Key roles for on-site services

Several on-site roles exist and these may have different titles, but two main roles should be identified documented to ensure a resilient function. As the work is performed in live environments it is important that these are trained and certified accordingly.

- **Site Engineer** is a role that is focused on specific named sites and understanding the general technical design of these sites. The role entails responsibility for planning and overseeing on-site works. It is the local project manager and the “go to person” for approvals and document review, e.g. permit to work or as built drawings.
- **Site technician** is a role that is focused on specific named sites. This is the local “go to person” for understanding technical aspects of the site, handling of customer equipment or having third parties escorted in the premises. The role may also include technical risk reviews of site systems or maintenance tasks.
- **Service technician** performs planned or corrective maintenance on site systems in accordance with agreed method statements.

Other expertise is available, whether it is compliance audits provided by suppliers of **Advisory Services**, or specialists handling the security and access control, technical cleaning of sensitive equipment and net floor areas, or other on-site services.

3.3 Delivery support

Instead of managing each site as an isolated team effort, there are shared support functions to drive cost efficiency and quality gains. It also provides continuous improvements, e.g. shared service desk, knowledge management, service improvements, business continuity planning and benchmarking.

3.3.1 Service Desk 24/7/365

The sites should be serviced by a full-time service desk. It manages the monitoring of alarms as well as service requests. Work should be performed in English and in local languages.

Typical features include:

- Accessible via web, e-mail and phone
- Provides site management and customer access to service records

It is a vital part of the incident process as it ensures technical specialists are dispatched to site and service records are collected and stored to fulfill service level obligations.

3.3.2 Governance

To help the parties collaborate and evolve the services over time, as well as managing incidents and resolve potential conflicts, the governance structure is established and documented.

It should tie in with existing delegations of authority and business continuity plans for both the customer and the site management supplier. Preferably, representatives from the customer and the supplier can resolve issues together before they escalate to Strategic level.

3.3.3 Advisory Services

Advisory Services support the customer and site management function by providing management advice in several areas:

- **Site strategy and site portfolio management** cover, e.g. strategies for energy and environmental improvements, financial analyses and business cases for investments. Planning of transformation programs that range from transition, change of ownership or decommission of sites and advising management on site portfolio optimization over a 3-10-year period.
- **Risk management** includes, e.g. Business Impact Analysis of site failures, formal compliance audits and reviews, business continuity and risk mitigation for processes and technology to improve site robustness and organizational resilience.
- **Performance improvements and cost reductions** – execution of transformation programs that range from transition, change of ownership or decommission of sites. Energy optimizations for improved climate footprint and cost reductions. Trainings, benchmarking programs and implementation of management KPIs to drive measurable performance improvements are also provided.

3.3.4 Service Improvements

Continuous improvements are based on a systematic quality management work to drive cost efficiency and reliability improvements in the services.

With the support from across the supplier organization, identified problems and possible improvements are shared as lessons learned and recommendations between the different site services teams.

- **Problem Management** – when incidents are managed and mitigated, they are also followed up and reported on, including root-cause analysis, to reduce any future site impact.
- **Knowledge Management** – the supplier should provide regular trainings and certifications of its team members. It should continuously gather, analyze and share information to keep abreast of operational and technological development.
- **Benchmarking** – Benchmarking of site performance against reference data from other sites operated by the supplier, or within the customer's own portfolio of sites, can be performed by Advisory experts.

The improvement approach used for process improvements is based on the PDSA (Plan-Do-Study-Act). A common perception of PDSA is that it is easy to use and can be applied in practice by anyone. At one level this is true, and the simplicity of the PDSA method and its applicability to many different situations can be viewed as one of its main strengths.

However, this simplicity also requires the users to understand how to adapt the use of PDSA to address different problems. An important aspect of this is to conduct investigations to ensure that the problem is correctly understood and framed before applying the PDSA method.

Investigations can include process mapping, failure mode effects analysis, cause and effect analysis, stakeholder engagement and interviews, data analysis and review of existing evidence. This requires an extensive repertoire of skills and knowledge to be used in conjunction with the basic PDSA model.



PDSA-OCP CFOPS
Framework v2019v1.

3.3.5 Supply chain and sourcing

Handling mission critical functions and critical facilities require not only high standards within your own organization. This commitment should also cover suppliers and products used to perform services.

- **Supply Chain** drives selection of strategic suppliers of services or products by setting common baselines to meet, e.g. with regards to cost, quality, environment, security and CSR.
- **Warehouse & Logistics** can be handled for the customer. This often covers access to critical spare parts on site but can also include access to centralized warehouses or logistics hubs.

3.3.6 Managed Operating Center – Remote Operations

Sites may be operated remotely to a much larger degree than only a few years ago. This enables remote expert support for several processes, e.g. capacity management and optimization, risk management as well as energy use improvements.

A Managed Operation Center (MOC) enables the site management function to assess, analyze and improve performance of the technically monitored site systems components, e.g. UPS, chillers, power meters, auxiliary systems, as well as CCTV or in-rack equipment, from individual power strips to servers. Furthermore, this opens up for predictive maintenance rather than relying on planned preventive maintenance, and many other benefits.

4 Summary overview

4.1 Site Management processes

The following sections summarize the processes in-scope for the site management function.

4.1.1 Incident Management

The aim of Incident Management is the removal of failures and recovery to normal operation state. Accidents should be handled as an incident category.

The incident process ensures relevant governance escalation to meet Business Continuity Plan and initiation of Problem Management.

The incident management process is aligned and integrated with the customer to minimize the impact on business operations.

4.1.2 Service Level Management

Service level management aims to ensure that the delivered service quality matches the agreed Service Level Agreement (SLA) in line with the border list.

The site management function will analyze, and report service level compliance based on monitoring, including breaches or situations that can lead to an SLA breach.

4.1.3 Lifecycle and Financial Management

Site systems lifecycle management

At time of purchase of a site system, lifecycle management rely on the vendors' specifications for End Of Life (EOL). Nevertheless, these specifications are based on laboratory measurements and there can be a significant deviation from the specification and operation in a real site. Therefore, lifecycle management monitors the actual costs and operational properties of the supply system items during their lifetime. The aim is to control warranty rights and requirements and create a change-out forecast for the items.

Financial management

The aim is to budget and forecast site costs. This is done by analyzing and accounting all services and site systems costs. Costs that are not directly related to an item or service should be distributed by cost distribution models.

Tender and selection

The aim is to ensure purchasing of services and site systems considering requirements on resilience, robustness and Total Cost of Ownership (TCO) to meet service level expectations. The approach should include energy costs as well as investment and services.

Requirements of operations concerning reliability, maintainability and integration into monitoring should also be considered. Decommissioning of infrastructure elements should be based on actual TCO and according to recycling and disposal obligations.

4.1.4 Monitoring and Reporting

Monitoring is implemented for detection of current status and failures. Gaps and inaccurate data can lead to wrong decisions and affect the effectiveness of all other site management processes.

Monitoring can be done via remote data collection, or on-site, either via automated data collection or manual assessments.

Reporting is made via different channels, e.g. operational level governance meetings, automated KPI reports and reviews.

From a monitoring perspective, Service Levels are not different from any other Key Performance Indicators. Instead, what separates Service Levels from other Key Performance Indicators (KPIs) is that if Service Levels are breached, it leads to pre-defined penalties with escalations.

KPIs, on the other hand, are parameters used to evaluate performance without pre-defined penalties. However, they may very well trigger escalations or other actions to adjust the site performance.

This means that any KPIs can form the base for a Service level, if agreed between the parties, e.g. Performance of Planned Preventive Maintenance in a timely manner (Quality KPI) or Measurable cost reductions in operating the site (Financial KPI)

Type of KPI	Recommended Key Performance Indicators
Availability	- Building Construction (Capacity use / Available space, Floor Area Type, Documentation type) - Power Distribution (Uptime, Capacity Use, MTBF, MTTR, Reduced resilience periods) - Environmental Control (Uptime, Capacity Use, MTBF, MTTR, Reduced resilience periods) - Telecom Cabling Infrastructure (Uptime, Capacity Use, MTBF, MTTR, Reduced resilience periods) - Security Systems (Uptime, Capacity Use, MTBF, MTTR, Reduced resilience periods)
Resource and Energy	- PUE (Power Usage Effectiveness) - ERE (Energy Re-use Efficiency) - REF (Renewable Energy Factor) - CUE (Carbon Usage Effectiveness) - WUE (Water Usage Effectiveness)
Financial	- Cost Report - Site Investments (Recommended, Approved, Planned, Declined, WIP, Completed) - Invoices (Received, Approved, Rejected, Being processed, Paid, Delayed)
Risk	- Risk Register (Risk Heatmap) - Incidents (Reported, Open/Closed, Root-cause) - Site access (Approved accesses, Authorized persons; Changes/Total) - Audits & Compliance Reviews (Planned/Requested, Completed, Deferred)
Quality	- On-site works (Response, Reaction, Planned/Requested/Call-outs, Completed, Deferred) - Time to report Incident (Planned/Requested/Expected, Completed, Deferred) - Deviations & Complaints (Reported, Open/Closed) - Audits & Compliance findings (Reported, Open/Closed) - Customer satisfaction (Net Promoter Score) - Annual Plans (Type, For Approval/Approved/Declined) - Certifications (Planned, Completed, Deferred)

The monitoring and reporting process is aligned and integrated with the customer to ensure management reporting requirements and site needs for normal operation.

4.1.5 Work Orders and Project Management

Service Requests

SR work orders are changes to normal operating configurations within the scope of service levels and border list, and therefore *do not require contractual changes*.

These should be planned to enable proper coordination and use pre-authorized method statements or project plans.

A cost assessment and a risk assessment is required to evaluate any associated impacts or risks and mitigate against them. A fallback plan is necessary for services that cannot be completed successfully, and downtimes should be minimized by coordinating to approved service windows.

The SR should be approved at appropriate governance level, based on agreed delegation of authorities between the parties.

The results should be reviewed by the creator to analyze the desired effect. Final approval includes that required documentation has been produced and recorded appropriately.

Change Requests

CR work orders are changes that affect the scope of service levels or border list, and therefore *do require contractual changes*.

A business case and a risk assessment are required. The expected contractual effects should be described, e.g. revised scope of services, increased/reduced site systems or border list updates.

The CR is approved at appropriate governance level, based on agreed delegation of authorities between the parties. When the contract has been adjusted, a Service Request may be created and approved accordingly.

The Work Order and project management process is aligned and integrated with the customer to ensure efficiency and fit-for-purpose governance escalations.

4.1.6 Capacity Management and Optimization

Capacity management and optimization aims to secure optimal usage and reliability of the site's provisioned capacity and performance. Therefore, it should analyze, manage and plan:

- Availability
- Resource and Energy use
- Financials
- Risks
- Quality

There is a strong relation between the level of redundancy, the provisioned and the used capacity of site systems. Overloading the provisioned capacity leads to a loss of redundancy. This increases risks of failure, but not necessarily to an actual failure.

Site systems fall into five categories:

- Building Construction
- Power Distribution
- Environmental Control
- Telecom Cabling Infrastructure
- Security Systems

Additional site systems or services to bring the site to increased capacity, to mitigate risks or quality issues should be put in place in time to meet the forecasted requirements.

To reduce resource and energy consumption, especially under part load conditions, only enough site systems should be installed to provide sufficient capacity for a pre-agreed future period, e.g. 18 months.

4.1.7 Compliance Management

The aim of compliance management is to ensure that other requirements than the formal service levels are not breached.

Compliance Management is used for creating, updating and issuing policies and procedures for managing compliance regarding

- Regulatory matters, e.g. statutory reporting or environmental permits
- Operations Framework or standards to be met
- Customer site-specific requirements, e.g. Disaster Recovery training

The compliance management process is aligned with the border list to ensure transparency on accountabilities and may include other topics.

4.1.8 Document Management

The aim of the document management process is ensuring access to critical documentation to support site management processes and on-site services.

Materials found in the site policies and reference library fall into one of three categories;

- master records used in several processes, e.g. Asset List or Border List
- templates for preparing day-to-day materials in other processes, e.g. Permit to Work
- policy requirements on other processes, e.g. Cost Distribution Model or DR Plan

Gaps in the site policies or reference library affect the effectiveness of all other site management processes and inaccurate or obsolete documents can lead to wrong decisions in the other site management processes.

Site policies

Site Management is responsible for creating, issuing and updating policies and procedures for management of the site:

- Site strategy including sourcing strategy for external suppliers
- Disaster Recovery Plan, including Emergency Operating Procedures (EOP)
- Standard Operating Procedures (SOP) for site management
- Cost Distribution Model for the site
- On-site work rules
- Organization, incl. third party dependencies

Reference library

The materials in reference library are identified recorded and provided to site management from the providers of related services or systems.

- Agreements and border lists
- As built drawings and studies, e.g. soil, electrical, environmental
- Asset lists incl. end of life (EOL) for site systems
- Warranties, acceptance tests and certificates of regulatory compliance
- Site Configurations Procedures, incl. manuals and vendor instructions
- Method statements for on-site services
- Service records for on-site services
- Meetings and decisions records

The site management function analyzes and structures the different materials into the relevant reference library categories.

The document management process is aligned with the border list, while some of the materials are also integrated and aligned with the customer to ensure efficiency and fit-for-purpose governance escalations, e.g. disaster recovery plan.

4.1.9 Team and Suppliers Management

Team and suppliers management aims to secure that on-site and off-site personnel, and third parties are qualified and available to meet set resilience expectations.

Plan / Schedule

All relevant personnel should be planned for with schedules and named individuals to minimize risks for gaps in deliveries of services

Staff register

Personnel being appointed to deliver services related to the site need to meet certain criteria depending on what type of services they provide. This should be registered and kept up-to date to ensure appropriate site operations.

- Qualifications
- Security clearance
- Site specific training

The team and suppliers management process is aligned and integrated with the customer to minimize the impact on business operations, e.g. security clearance.

4.2 On-site services

4.2.1 Security and Access

The security and access process, procedures and building construction should be appropriate to the assets that they are protecting. This would include critical assets in the primary area as well as site systems in other parts of the net floor area.

Perimeter protection

A critical facility should be appropriately protected against threats that may break the perimeter. By protecting against external and environmental threats, i.e. man-made or natural disasters, it is focused on ensuring that only designated access points can be used to gain entry to the critical facility. Typical services may include patrolling by guards or CCTV monitoring of different parts of the building and its external premises.

Furthermore, the building construction itself may allow for several protective layers or zones which can increase the level of the perimeter protection and further protect against breaches outside the ordinary access control points.

Access control

All personnel, visitors and deliveries to the site should be registered and processed according to operational procedures where at least the following should be made:

- Verification of identity, i.e. authentication
- Verification of authorization
- Logging of access

Remote monitoring of alarm systems and CCTV is normally used to control access to premises or rooms when a correct authentication has been performed.

Appropriate controls are put in place to ensure that access control audit logs cannot be altered, tampered, or deleted, thus destroying evidential integrity. This integrity is generally required to support a potential criminal prosecution because of a security incident.

The access control system audit logs should be inspected on a recurring basis.

The security and access process is aligned and integrated with the customer to minimize the impact on business operations.

4.2.2 Maintenance

The aim of maintenance is to keep the site robust and at the status of normal operation by replacing components under controlled conditions, i.e. scheduled, budgeted and approved.

Therefore, the maintenance plan for site systems should be carried out according to best practice and compliant to the instructions of the vendor.

All work is governed by on-site work rules and should be performed under a permit to work system by authorized persons.

4.2.3 Indoor/outdoor Facility Management

Facility Management services comprise Space & Infrastructure and People & Organization services.

The aim of indoor and outdoor facility management (FM) is to enable the site to be managed at normal status by handling specific services under controlled conditions, i.e. scheduled, budgeted and approved. Gaps in Facility Management can shorten the life expectancy of the site, cause incidents and failures or prevent access to the site, e.g. lacking snow removal. Incorrect procedures could lead to health and safety risks or compliance violations, e.g. ineffective pest control.

Services are defined as being performed outdoors or inside building constructions.

When FM services are performed within building constructions, these are split between services performed within the Net Floor Area (NFA) and those performed outside the Net Floor Area.

4.2.4 Site Inspections

Site inspection duties are performed on a scheduled basis to ensure personnel Health and Safety (H&S) or to minimize site systems technical risks.

Health & Safety / On-site work rules should consider:

- Temporary hazards, escape routes, protection gear, first aid kit, handling of dangerous goods etc.
- Performance according to Site Policies and Permit to work
- Site security requirements, e.g. wearing a badge
- Site appearance, e.g. cleanliness, documentation, dress code, etc.

Technical Risk Reviews (TRR) include inspection of site systems:

- Risks for system breakdowns
- Misconfigurations or lack of optimizations, e.g. regarding energy use
- Incorrect or obsolete technical documentation
- Use of improper spare parts or MESTs, etc.

Regulatory reporting typically includes reports of handling waste:

- Chemicals used and spills
- Hazardous materials and waste handling

In case there are breaches in any form, these are reported to the site management function. The status of site inspections should be a regular topic for the Operational Governance Meetings.

4.2.5 Audits and Compliance reviews

The aim of audits and compliance reviews is to assure that other requirements than the formal service levels are not breached. An annual compliance audit of the sites in scope and their respective process KPIs should be considered a minimum.

Qualified experts should independently plan, perform and report on findings, e.g. deviations, risks or potential improvements regarding

- Regulatory matters, e.g. statutory reporting or environmental permits
- Operations Framework or standards the site should meet

The audits and compliance reviews process should be aligned with the customer to minimize the impact on business operations and to agree relevant regulations or standards, e.g. this CFOPS Framework, EN 50600, ISO 27001, ISO 9001, ISO 14001, LEEDS, EU Code of Conduct, EED – Energy Efficiency Directive, UI Operational Sustainability, ISAE 3402, BICSI 009 etc.

4.2.6 Site Assistance

The aim of Site assistance services is to enable the customer to perform its primary activities in the site at normal status. This is done by handling specific services under controlled conditions, i.e. scheduled, budgeted and approved.

Services are performed inside building constructions. They may be performed within or outside the Net Floor Area (NFA) and may comprise Space & Infrastructure and People & Organization services.

Manned site

Site engineers or site technicians can man a site as per agreement, normally during office hours or 24/7, but also at scheduled critical times, e.g. end-of-month week.

Smart / Remote hands

These services involve designated personnel physically touching customer's equipment and critical assets in accordance with written or verbal instructions. Sample services performed:

- Power shutdown
- Visual inspection of customer's equipment
- Cables and patching
- Installation of hardware (move-add-change)

Third party escorting

The service is used to ensure personnel only have access to equipment and critical assets when subject to one or more of the following:

- site operational procedures
- operational requirements
- 'two-person rule' access

Goods handling

To minimize the amount of third parties accessing the premises this can be handled by dedicated personnel. Sample services:

- Receiving goods (incl. signing receipts)
- Packing/unpacking (incl. inventory and defect controls)
- Recycling and disposal
- Hand-out of goods (requiring signing by recipient)

The site assistance services may contain other site-specific services agreed with the customer, to enable customer's optimal use of the site.

5 OCP CFOPS MindMap

OCP-CFOPS-MindM
ap.2019v1.5.pptx

6 OCP CFOPS TERMINOLOGY AND ACRONYMS LIST

OCP-CFOPS-Termin
ology_2019v1.5.doc