

Planning an efficient Security Operations Centre

Ashwin Venugopal - Founder, OpsConfer



Attribution:

The Microsoft Operations Framework (MOF) 4.0 is provided with permission from Microsoft Corporation & these guidelines are prepared by OpsConfer. This documentation is licensed to you under the Creative Commons Attribution License.

Overview

This is a heavily modified version based on Microsoft® Operations Framework (MOF) and this consists of integrated best practices, principles, and activities that provide comprehensive guidelines for achieving reliable SOC based on my experience.

This framework provides question-based guidance that allows you to determine what is needed for your organisation now, as well as activities that will keep the SOC running efficiently and effectively in the future.

This documentation encompasses all of the activities and processes involved in planning a Security Operations Centre. Here we will organise activities and processes into Functions, which will be again grouped together in plan phase.

Look for further documentations on Deliver, Operate and Manage Phase/sections of SOC Implementation Project. It will also continue similar documentation style.

We are an IT startup that is based at Bangalore, India and we focus on Cyber Security, Cloud & Security services.

We also work with MSSPs and work towards setting up a matured SOC.

At any point if you need any assistance, please feel free to reach to us on services@opsconfer.com. We we will be happy to assist you.

Thank you,

Ashwin Venugopal

Website: www.opsconfer.com

Facebook: <http://facebook.com/opsconfer/>

Twitter: <http://twitter.com/OpsConfer>

Linked-in: <http://linkedin.com/company/opsconfer/>



Attribution:

The Microsoft Operations Framework (MOF) 4.0 is provided with permission from Microsoft Corporation & these guidelines are prepared by OpsConfer. This documentation is licensed to you under the Creative Commons Attribution License. To view a copy of this license, visit [here](http://creativecommons.org/licenses/by/4.0/)

Overview

Goal

Our goal is to provide guidance to organisations to help them create, operate, and support SOC services while ensuring that the investment in SOC delivers expected business value at an acceptable level of risk.

Our purpose is to create an environment where business and SOC can work together toward operational maturity, using a proactive model that defines processes and standard procedures to gain efficiency and effectiveness. Using MOF this promotes a logical approach to decision-making and communication and to the planning, deployment, and support of SOC services.



What do we do unique?

- Our Overview guides are directed toward CIOs who need to see the big picture.
- Our Overview and workflow information in function-specific guides created are geared toward SOC managers who need to understand the SOC service strategies.
- Our Activities in function-specific guides are meant for the Security professionals who implement this framework within their work.

This documentation consists of a series of Phases, Functions, Processes & Activities. These describe the activities that need to occur for successful SOC service management—from the assessment that launches a new or improved service, through the process of optimising an existing service, all the way to the retirement of an outdated component.

Attribution:

The Microsoft Operations Framework (MOF) 4.0 is provided with permission from Microsoft Corporation & these guidelines are prepared by OpsConfer. This documentation is licensed to you under the Creative Commons Attribution License. To view a copy of this license, visit [here](https://creativecommons.org/licenses/by/4.0/)

Overview

Does Your Business Need a Security Operations Centre?

In the day and age of sophisticated digital hackers, your concern shouldn't be if you're going to get hacked, but what you're going to do when it happens. Investing in a security operations centre (SOC) can be your saving grace during an attempted cybersecurity attack. Cybersecurity is no longer just an IT problem—it's an organisational issue. Find out if a security operations centre is the ideal solution for securing your enterprise against cyber threats.

A security operations centre is an organisational hub of highly skilled team members and technology whose goal is to detect, prevent, and respond to cybersecurity threats. A security operations centre continually monitors a business' cybersecurity, preventing serious breaches in real time.

The SOC takes into account the physical safety, the functionality of the centre's layout, and the SOC's overall design. SOC's require several areas, including a supervisor's office and an operational room. The design of each zone must optimise comfort, efficiency, and visibility during operations.



To find out if building security operations centre is right for your company, ask yourself a few questions:

Do you have the tools and expertise to build a SOC in-house?

Building your SOC internally is possible with the right leadership and support. If you own a larger organisation, you likely already have the in-house tools and skills to build a security operations centre successfully.

Do you have the right people in place?

You need a team of trained and experienced people to research and identify potential cyber threats. If you don't have such a team, make sure you have room in the budget to hire one before building your SOC.

Does your business handle data you need to monitor 24/7?

If so, a security operations centre can be a game changer. SOC's enable you to carefully track your data around the clock, swooping in to neutralise a threat at a moment's notice.

Do you have money in the budget to build the facility?

Partnering with the right SOC provider can help you adhere to a budget with tailored solutions, but you still have to ensure that you have the money to integrate the equipment you need.

Many modern businesses across several industries could benefit from a security operations centre, particularly since business continues to become more data-centric. If you answered yes to these four

Attribution:

The Microsoft Operations Framework (MOF) 4.0 is provided with permission from Microsoft Corporation & these guidelines are prepared by OpsConfer. This documentation is licensed to you under the Creative Commons Attribution License. To view a copy of this license, visit [here](https://creativecommons.org/licenses/by/4.0/)

Plan Phase

Overview of the Plan Phase



- Understanding the business strategy and requirements and how the Security Operations Centre support the business.
- Understanding what reliability means to this Security Operations Centre and how it will be measured and improved by reviewing and taking action where needed.
- Understanding what policy requirements exist and how they impact the Security Operations Centre.
- Providing the financial structure to support the Security Operations Centre and drive the right decisions.
- Creating an Security Operations Centre strategy to provide value to the business strategy and making the portfolio decisions that support that Security Operations Centre strategy.

Goals of the Plan Phase

- Valuable and compelling.
- Predictable and reliable.
- Compliant.
- Cost-effective.
- Adaptable to the changing needs of the business.

Attribution:

The Microsoft Operations Framework (MOF) 4.0 is provided with permission from Microsoft Corporation & these guidelines are prepared by OpsConfer. This documentation is licensed to you under the Creative Commons Attribution License. To view a copy of this license, visit [here](#)

Plan Phase

Why do you need a Security Operations Centre?

In the day and age of sophisticated digital hackers, your concern shouldn't be if you're going to get hacked, but what you're going to do when it happens. Investing in a security operations centre (SOC) can be your saving grace during an attempted cybersecurity attack. Cybersecurity is no longer just an IT problem—it's an organisational issue. Find out if a security operations centre is the ideal solution for securing your enterprise against cyber threats.

A security operations centre is an organisational hub of highly skilled team members and technology whose goal is to detect, prevent, and respond to cybersecurity threats. A security operations centre continually monitors a business' cybersecurity, preventing serious breaches in real time.

The SOC takes into account the physical safety, the functionality of the centre's layout, and the SOC's overall design. SOC's require several areas, including a supervisor's office and an operational room. The design of each zone must optimise comfort, efficiency, and visibility during operations.

The Plan Phase is where business and SOC Team work as partners to determine how SOC will be focused to deliver valuable services that enable the organisation to succeed.

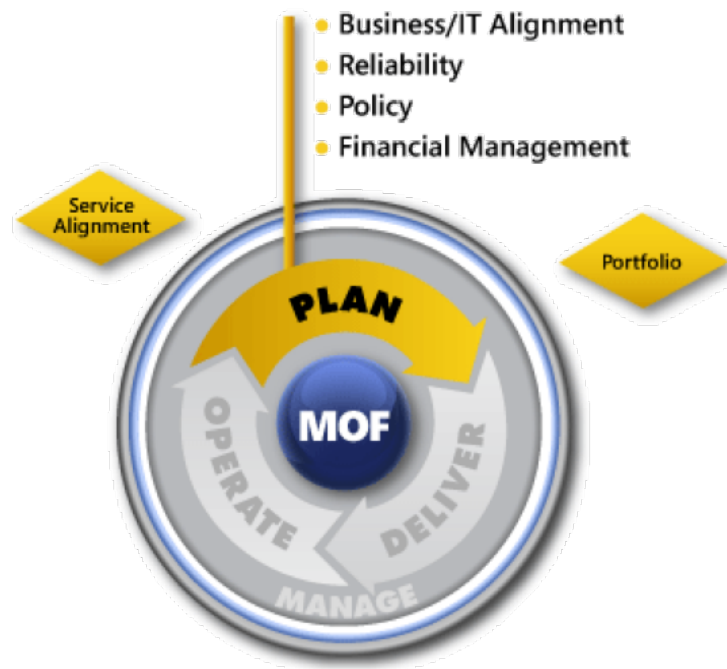
SOC Strategy.

The SOC strategy is the plan that aligns the organisation's objectives, policies, and procedures into a cohesive approach to deliver the desired set of services that support the business strategy. Quality, costs, and reliability need to be balanced in order to achieve the organisation's desired outcomes.

During the Plan Phase, Cyber Security professionals work with the business to align business objectives and functions with SOC's capabilities and constraints. The SOC strategy is the result of this alignment and serves as a roadmap for SOC. The strategy continually evolves and improves as organisations improve their optimising skills and ability to adapt to business changes.

Attribution:

The Microsoft Operations Framework (MOF) 4.0 is provided with permission from Microsoft Corporation & these guidelines are prepared by OpsConfer. This documentation is licensed to you under the Creative Commons Attribution License. To view a copy of this license, visit [here](https://creativecommons.org/licenses/by/4.0/)



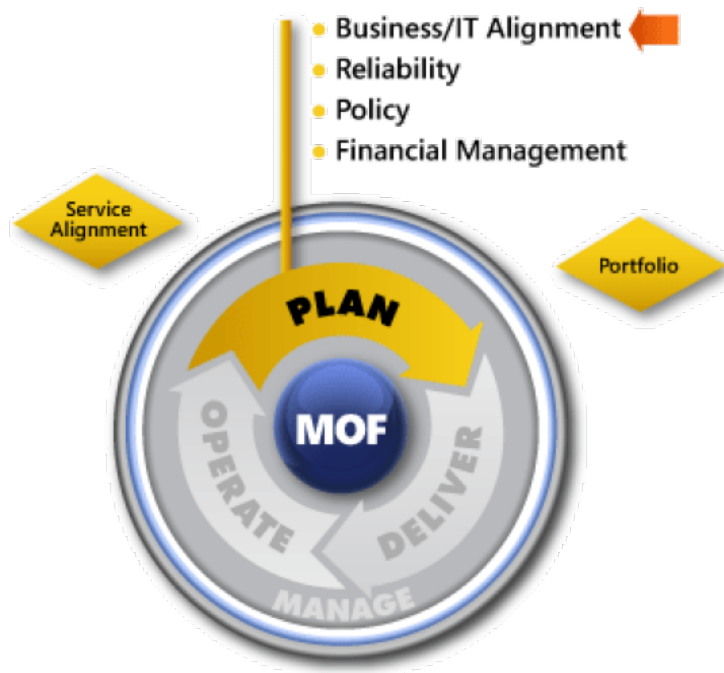
Plan Phase

Business/IT Alignment Function

Q: What do businesses want from SOC?

A: SOC that is reliable, compliant, and cost-effective, and that continuously adapt to ever-changing needs.

If you want to strengthen the alignment between your SOC department and the larger organisation, start with this list of questions. Your answers will determine which areas of this document can help you the most.

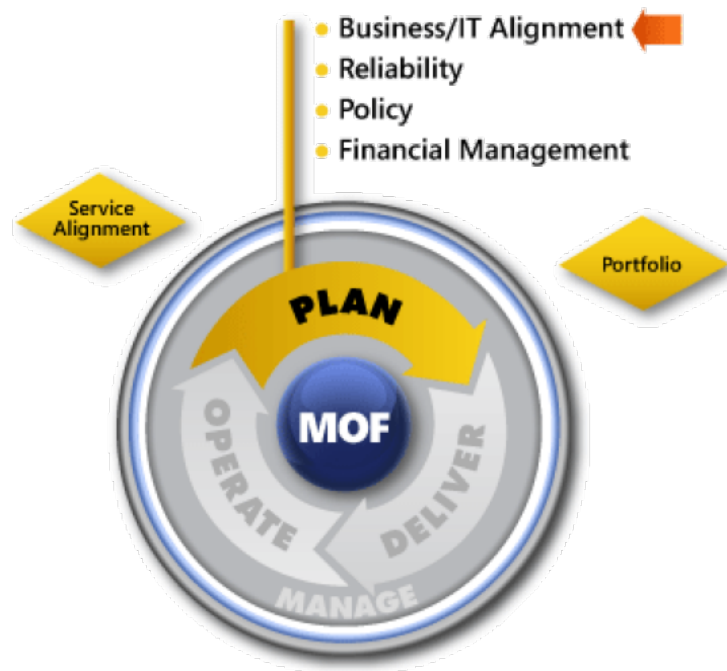


- Do you have an SOC strategy in place? Is it aligned to organisational objectives?
- Is the strategy communicated? Does everyone have a clear understanding of the strategy?
- Is the strategy measured, and are opportunities for improvement identified?
- Are there service level agreements (SLAs) in place for the SOC?
- Is there a process for identifying and approving new SOC concepts?
- Is there a published portfolio of SOC? Is it clearly communicated and understood the business representatives?
- Is there a clear connection between the strategy and SOC's portfolio of tasks and services?
- Is SOC service demand measured and analysed?
- Are new business requests accepted, organised, managed, and acted upon?

Attribution:

The Microsoft Operations Framework (MOF) 4.0 is provided with permission from Microsoft Corporation & these guidelines are prepared by OpsConfer. This documentation is licensed to you under the Creative Commons Attribution License. To view a copy of this license, visit [here](https://creativecommons.org/licenses/by/4.0/)

Plan Phase



Business/IT Alignment Function | Goals

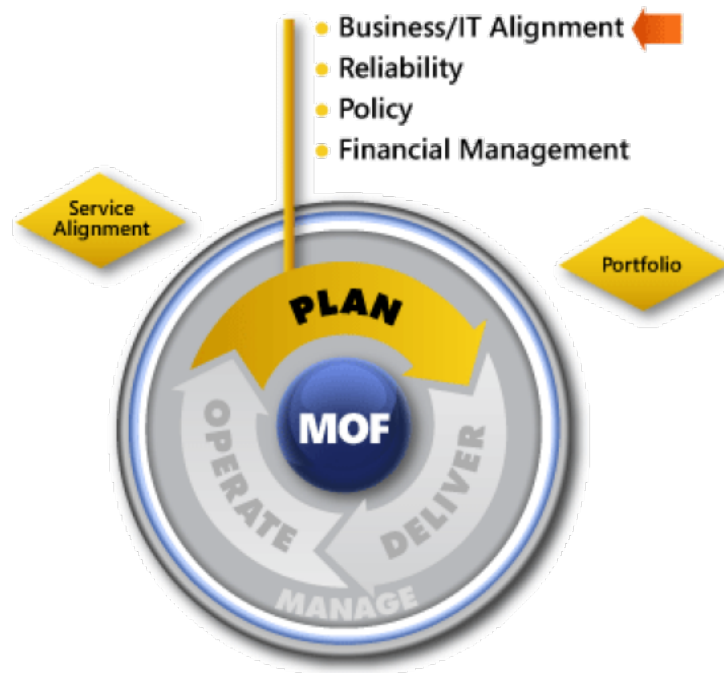
Goal	Measurements
The business considers SOC as a strategic asset.	<ul style="list-style-type: none"> The business continues to invest in enhancements of SOC. The business consults with SOC as part of strategic decisions, acquisitions, or new directions.
SOC has a strategic plan.	<ul style="list-style-type: none"> The business and SOC publish and measure an annual SOC service strategy. The strategy articulates the linkages between SOC goals and the business goals and outlines measurements, budget, risks, and a plan for execution.
SOC has an understanding of its capabilities and resources.	<ul style="list-style-type: none"> SOC has a predictable model for estimating resource consumption and the adoption of new technologies. SOC measures business demand of services offered and uses this information for planning purposes.
SOC has a set of defined services and tasks that support the strategic plan.	<ul style="list-style-type: none"> SOC has a published service portfolio that identifies all tasks. SOC has a published service catalog that identifies and describes all services offered to the organisation by SOC.

Attribution:

The Microsoft Operations Framework (MOF) 4.0 is provided with permission from Microsoft Corporation & these guidelines are prepared by OpsConfer. This documentation is licensed to you under the Creative Commons Attribution License. To view a copy of this license, visit [here](https://creativecommons.org/licenses/by/4.0/)

Plan Phase

Business/IT Alignment Function | Roles & Responsibilities



Role	Responsibility
Service Provider Manager	<ul style="list-style-type: none"> Tracks & manages service provider who might provide supporting services and products
Portfolio Manager	<ul style="list-style-type: none"> Keeps a set of service offerings of SOC up to date and aligned to business needs Maintains the overall service catalog of SOC
Account Manager	<ul style="list-style-type: none"> Serves as a link between customer and the service provider Meets with the customer, discusses current issues, and makes sure that expectations are aligned
Service Level Manager	<ul style="list-style-type: none"> Acts as main interface between the business and the SOC service delivery organisation Handles all issues and development in Service Level Management, including development and agreement of SLAs, OLAs, and UCs Represents the business, but works with and within the SOC
Security Executive Officer (CISO)	<ul style="list-style-type: none"> Sponsors SOC initiatives Approves structures and overall SOC processes Owens metrics and benchmarking, board and executive relationships
SOC Manager	<ul style="list-style-type: none"> Manages processes Identifies and engages appropriate participants in decision process Manages risk and SOC business value realisation dependencies Owens business/SOC relationship
SOC Policy Manager	<ul style="list-style-type: none"> Sees that management decisions are informed by policy and that policy is effectively used across SOC
Change Manager	<ul style="list-style-type: none"> Manages the activities of the change management process for the SOC organisation

Attribution:

The Microsoft Operations Framework (MOF) 4.0 is provided with permission from Microsoft Corporation & these guidelines are prepared by OpsConfer. This documentation is licensed to you under the Creative Commons Attribution License. To view a copy of this license, visit [here](https://creativecommons.org/licenses/by/4.0/)

Plan Phase

Business/IT Alignment Function | Key Terms



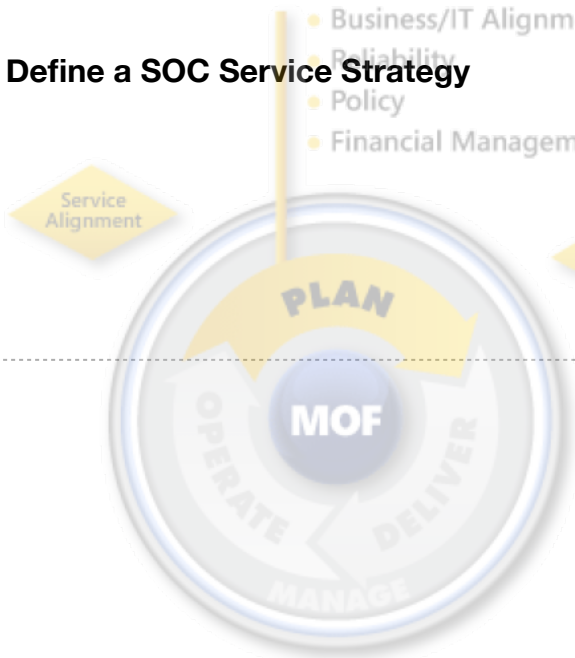
Key Terms	Description
Business relationship management	The ongoing process that ensures that the organisation and SOC remain in sync with respect to common goals and strategies
Demand management	The process of aligning an organisation's supply of SOC resources to meet service demands forecasted by the business
SOC service strategy	The plan that aligns an organisation's objectives, policies, and procedures into a cohesive approach to deliver SOC that support business strategy
Operating level agreement (OLA)	An internal agreement between one or more teams that supports the requirements set forth in the service level agreements (SLAs)
Service catalog	A comprehensive list of services, including priorities of the business and corresponding SLAs
Service Level Agreement (SLA)	A written agreement documenting required levels of service. The SLA is agreed upon by the SOC service provider and the business, or by the SOC service provider and a third-party provider. SLAs should list the metrics and measures that define success for both SOC and the organisation
Service Level Management	The process of defining and managing performance through monitoring, reporting, and reviewing the required, agreed-upon level of service
Service portfolio	An internal repository that defines SOC services and categories them as currently in service, in queue to be developed, or in queue to be decommissioned. All services support a specific business process or function
Underpinning contract (UC)	A legally binding contract in place of or in addition to an SLA. This type of contract is with a third-party service provider responsible for building service deliverables for the SLA

Attribution:

The Microsoft Operations Framework (MOF) 4.0 is provided with permission from Microsoft Corporation & these guidelines are prepared by OpsConfer. This documentation is licensed to you under the Creative Commons Attribution License. To view a copy of this license, visit [here](https://creativecommons.org/licenses/by/4.0/)

Plan Phase

Business/IT Alignment Function | Processes & Activities


Process	Description	Activities
<p>Define a SOC Service Strategy</p>  <p>Service Alignment</p> <p>Business/IT Alignment</p> <p>Reliability</p> <p>Policy</p> <p>Financial Management</p>	<p>A SOC service strategy determines which services are required to support business goals and objectives. Business and SOC management must carefully discern which initiatives offer the highest business value while ensuring the availability of necessary resources and the commitment to deliver on the investment.</p> <p>A successful service strategy will ensure that:</p> <ul style="list-style-type: none"> • SOC goals are aligned to business goals. • Annual SOC initiatives that support business goals have been identified. • There is agreement on both the strategy and a corresponding plan for achieving the goals and initiatives. • The strategy is assessed against business outcomes. • Opportunities for improvement are identified. 	<ul style="list-style-type: none"> • Aligning SOC goals to business goals. • Mapping and prioritising business functions to the SOC service portfolio. • Defining initiatives. • Finalising and agreeing on an annual strategy. • Managing performance.
<p>Identify and Map SOC Services</p>	<p>Service maps are used throughout the organisation to clarify the dependencies between SLAs, OLAs, technologies, customers, and the impact to the service delivery. They identify the resources necessary to deliver a service described in the service catalog, who delivers that service, and who consumes it.</p> <p>A service map represents a service from the perspective of the business and the user. It is divided into five sections:</p> <ul style="list-style-type: none"> • Customers. A categorised list of individuals and groups who use the service. • Hardware. The hardware platforms necessary for service delivery. • Applications. The operating system(s) and other applications the service requires. • Settings. The configuration settings necessary for the service to function. • Internal/external services. The components that help ensure availability for the service. 	<ul style="list-style-type: none"> • Identifying services and owners. • Identifying key customers and users. • Reviewing, classifying, and categorising key service component groups and service owners. • Publishing a service map.

Attribution:

The Microsoft Operations Framework (MOF) 4.0 is provided with permission from Microsoft Corporation & these guidelines are prepared by OpsConfer. This documentation is licensed to you under the Creative Commons Attribution License. To view a copy of this license, visit [here](https://creativecommons.org/licenses/by/4.0/)


Plan Phase

Business/IT Alignment Function | Processes & Activities

Process	Description	Activities
Identify Demand and Manage Business Requests 	<p>Demand and request management analysis is a process that articulates how SOC services are being used and requested by the organisation and how future trends might affect the services. Demand management data helps managers plan and account for their SOC expenditures, understand the SOC business services they are receiving in return, and participate in decisions about future projects and resource allocation.</p> <p>A fully matured demand and request management process will ensure that:</p> <ul style="list-style-type: none"> • There is a predictable process for managing requests. • There is a consistent model for measuring current demand. • There is a method of analysing requests and current service capacity. 	<ul style="list-style-type: none"> • Managing new requests. • Capturing current usage and demand. • Identifying and validating future trends. • Analysing demand and requests.
Develop and Evaluate SOC Service Portfolio	<p>When an organisation has finalised its SOC service strategy, the business and SOC must determine which projects and services best support that strategy. The SOC service portfolio is the list of those projects and services. Ensuring that the right services and projects are included in the portfolio requires the following components:</p> <ul style="list-style-type: none"> • Proposed projects aligned to SOC strategy initiatives • A list of projects in the queue, implemented services, and services slated for decommission • A prioritisation and approval process for new projects • A measurement system for determining the value of services in relation to business goals <p>The SOC service portfolio drives the alignment of SOC resource consumption, the operating budget, and investment strategies that support the SOC service strategy. The portfolio's primary users are the business and SOC leaders responsible for realising business value from the investment in SOC.</p> <p>Attribution:</p>	<ul style="list-style-type: none"> • Defining the structure and composition of the SOC service portfolio. • Measuring the value of SOC services in relation to business outcome. • Analysing and approving new project concepts. • Publishing a portfolio.

Plan Phase

Business/IT Alignment Function | Processes & Activities

Process	Description	Activities
 <p>Service Level Management</p>	<p>If SOC strategy is to be seamlessly aligned to the organisation's strategy, SOC must manage the ongoing delivery and enhancement of its services—this is the goal of Service Level Management. Service Level Management ensures that ongoing requirements, communications, and expectations between business and SOC are proactively managed. Service Level Management is also responsible for ensuring that internal SOC expectations are being met.</p>	
	<p>The service catalog sets the standards against which expectations, improvements, and performance metrics are measured. SLAs and operating level agreements (OLAs) ensure that agreements are in place to support the offerings within the service catalog.</p> <p>SOC Service Catalog:</p> <ul style="list-style-type: none"> • Communicates standard SOC services to customers in clear, familiar terms. • Provides a centralised channel through which end users can request standardised, typical SOC service bundles. <p>Operating Level Agreements (OLAs):</p> <ul style="list-style-type: none"> • Communicate and document the agreed-upon expectations of dependent SOC services. • Are agreed upon between different Internal teams. <p>Service Level Agreements (SLAs):</p> <ul style="list-style-type: none"> • Communicate and document the agreed-upon expectations of business-facing SOC services. • Are agreed upon between business and SOC representatives. <p>Underpinning Contract (UC):</p> <ul style="list-style-type: none"> • Ensures there is a contract between suppliers, third parties, and the organisation. • Communicates and documents the agreed-upon expectations between the suppliers, third parties, and the organisation. 	<ul style="list-style-type: none"> • Managing business relationships. • Tracking changing business needs. • Creating the service catalog. • Defining OLAs. • Defining UCs. • Defining SLAs.

Attribution:

The Microsoft Operations Framework (MOF) 4.0 is provided with permission from Microsoft Corporation & these guidelines are prepared by OpsConfer. This documentation is licensed to you under the Creative Commons Attribution License. To view a copy of this license, visit [here](https://creativecommons.org/licenses/by/4.0/)

Plan Phase

Reliability Function

Why Use the Reliability Function?

This function should be useful for anyone who wants to understand, set targets, and measure SOC service reliability.

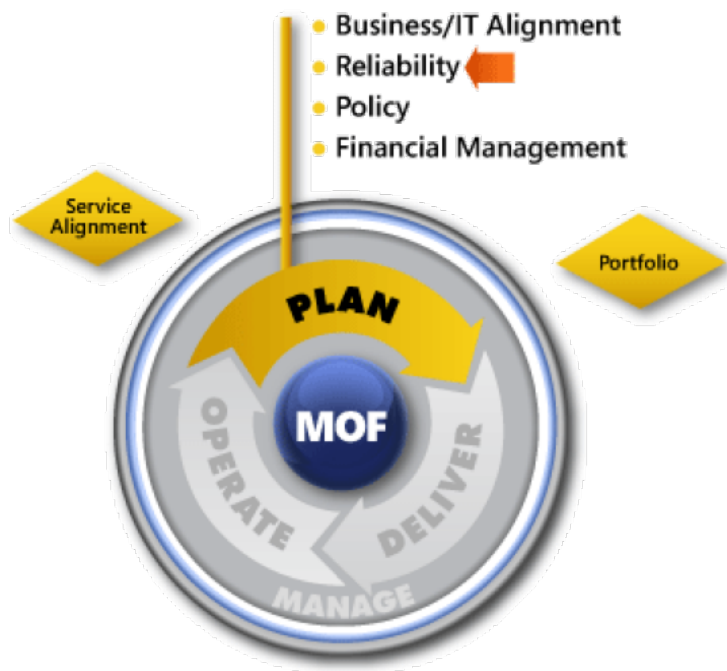
It addresses creating plans for the following:

- **Confidentiality**
- **Integrity**
- **Availability**
- **Continuity**
- **Capacity**

A reliable service or system is dependable, requires minimal maintenance, will perform without interruption, and allows users to quickly access the resources they need. These characteristics are not only true for business-as-usual conditions; they must also apply during times of business change and growth and during unexpected events.

Ensuring reliability involves three high-level processes:

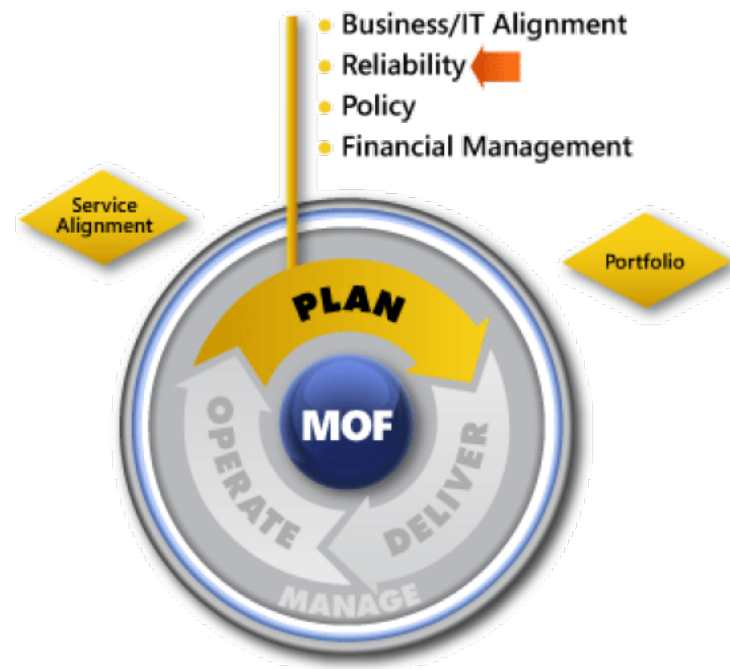
- **Planning.** Gathering and translating business requirements into IT measures of SOC
- **Implementation.** Building the various plans and ensuring that they can meet expectations
- **Monitoring and Improvement.** Proactively monitoring and managing the plans and making necessary adjustments



Attribution:

The Microsoft Operations Framework (MOF) 4.0 is provided with permission from Microsoft Corporation & these guidelines are prepared by OpsConfer. This documentation is licensed to you under the Creative Commons Attribution License. To view a copy of this license, visit [here](http://creativecommons.org/licenses/by/4.0/)

Plan Phase



Reliability Function | Goals

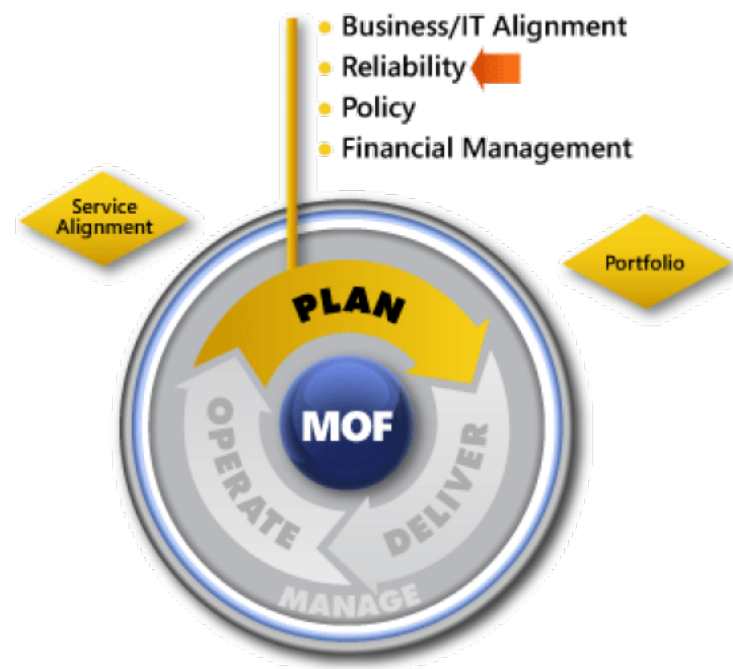
Goal	Measurements
SOC capacity aligned to business needs	<ul style="list-style-type: none"> Proactive capacity plan No capacity-related service disruptions Procurement/purchasing plan developed and adhered to
SOC Services available when needed	<ul style="list-style-type: none"> Proactive, cost-justified availability plan Reduction in service failures Minimized service disruption from anticipated failures
Critical SOC services available during significant failures	<ul style="list-style-type: none"> SOC disaster recovery aligned to business continuity plan Tested, trusted, recovery plan supported by the business
Data integrity and confidentiality maintained	<ul style="list-style-type: none"> Data classified and managed according to business policy No exceptions to data handling and integrity requirements

Attribution:

The Microsoft Operations Framework (MOF) 4.0 is provided with permission from Microsoft Corporation & these guidelines are prepared by OpsConfer. This documentation is licensed to you under the Creative Commons Attribution License. To view a copy of this license, visit [here](http://creativecommons.org/licenses/by/4.0/)

Plan Phase

Reliability Function | Roles & Responsibilities



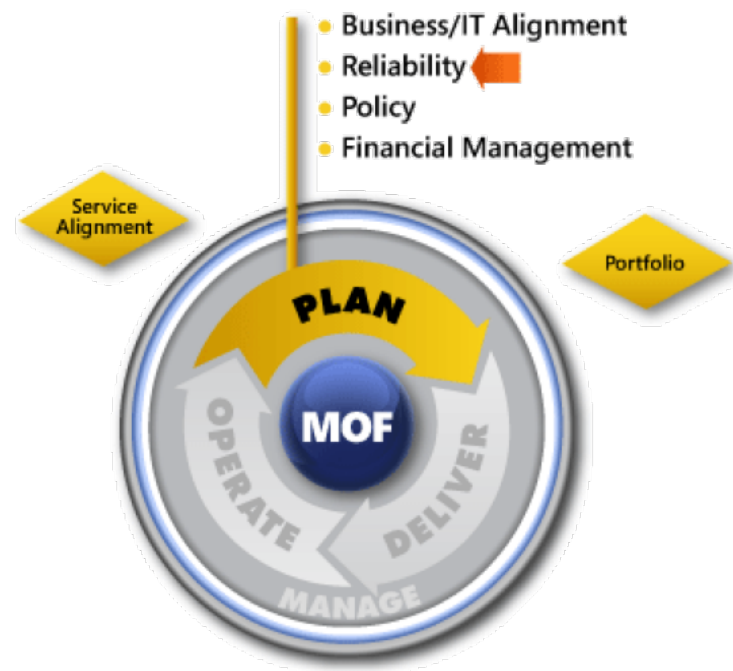
Role	Responsibility
Architecture Manager	<ul style="list-style-type: none">Accountable for ensuring creation and maintenance of architecture plan
Reliability Manager	<ul style="list-style-type: none">Uses input from Service Monitoring and Control Function to look at current bottlenecks and propose solutions
Architect	<ul style="list-style-type: none">Looks at future directions and solutions to propose across infrastructureDesigns future state

Attribution:

The Microsoft Operations Framework (MOF) 4.0 is provided with permission from Microsoft Corporation & these guidelines are prepared by OpsConfer. This documentation is licensed to you under the Creative Commons Attribution License. To view a copy of this license, visit [here](#)

Plan Phase

Reliability Function | Key Terms




Key Terms	Description
Availability management	The process of managing a SOC so that it is accessible when users need it. Availability is typically measured in percentage of uptime; downtime refers to periods of system unavailability.
Business continuity planning	The process for planning and practicing SOC's response to a disaster or disruptive event. These activities span the organisation; beyond just SOC functions.
Capacity management	In the context of SOC, capacity refers to the processing or performance capability of a service or system. Capacity management is the process used to ensure that current and future SOC needs are met in a cost-effective manner. This process is made up of three sub-processes: business, service, and resource capacity management.
SOC Service Continuity Management	The process of assessing and managing SOC risks that can significantly affect the delivery of services of SOC to the business.

Attribution:

The Microsoft Operations Framework (MOF) 4.0 is provided with permission from Microsoft Corporation & these guidelines are prepared by OpsConfer. This documentation is licensed to you under the Creative Commons Attribution License. To view a copy of this license, visit [here](https://creativecommons.org/licenses/by/4.0/)

Plan Phase

Reliability Function | Processes & Activities


Process	Description	Activites
 <p>Planning</p>	<p>The first activity in planning for Reliability Management is to clearly understand and document the business requirements for the SOC. Understanding the business objectives allows SOC to prioritise and allocate resources to the service and to better align technology investment decisions with the organisation's priorities. SOC gathers these requirements by engaging the business through an ongoing relationship management process.</p> <p>The second activity in planning focuses on the effort and investment that SOC must make to ensure that business expectations are met. Doing this successfully involves understanding both the target SOC environment and the specifications for the new service: how these align with each other, how the new service will affect the current environment, and where there are significant technical or resource capability gaps.</p> <p>These activities should ideally occur during the design phase of a new service so that SOC operations can influence the specifications and ensure that the service is designed to operate reliably. A regular dialogue between SOC and the business is crucial because trade-off decisions will usually need to be made between an ideal state and a practical, cost-effective one.</p>	<ul style="list-style-type: none"> • Define service requirements of SOC • Plan and analyse business and technical requirements of SOC.

Attribution:

The Microsoft Operations Framework (MOF) 4.0 is provided with permission from Microsoft Corporation & these guidelines are prepared by OpsConfer. This documentation is licensed to you under the Creative Commons Attribution License. To view a copy of this license, visit [here](https://creativecommons.org/licenses/by/4.0/)

Plan Phase

Reliability Function | Processes & Activities


Process	Description	Activities
 <p>Implementation</p>	<p>Here we address the traditional objectives of availability, disaster recovery, capacity, data integrity, and monitoring functions of SOC. They can exist separately or be combined, depending on specific organisational requirements and scale.</p>	
	<p>For larger, more complex organisations, it might be appropriate to retain some or all of the traditional plans individually.</p>	
	<p>However, they should be managed collectively so as to take advantage of common objectives and technical solutions. This strategy helps the organisation achieve higher reliability more cost-effectively.</p>	<ul style="list-style-type: none"> • Develop availability plan • Develop capacity plan • Develop data security plan • Develop disaster recovery plan • Develop monitoring plan • Review and approve plans
	<p>SOC IT management uses the requirements from the planning process to build corresponding plans that will allow SOC to meet or exceed delivery expectations.</p> <p>Activities and tasks performed during this process can include:</p> <ul style="list-style-type: none"> • Analysis of existing infrastructure and how SOC will affect it. • Evaluation of new technologies that can help SOC achieve the desired outcomes. • Validating that the SOC meet delivery expectations and align to infrastructure standards. • Adapting plans as business needs change. 	

Attribution:

The Microsoft Operations Framework (MOF) 4.0 is provided with permission from Microsoft Corporation & these guidelines are prepared by OpsConfer. This documentation is licensed to you under the Creative Commons Attribution License. To view a copy of this license, visit [here](https://creativecommons.org/licenses/by/4.0/)

Plan Phase

Reliability Function | Processes & Activities

Process	Description	Activites
 <p>Monitoring and Improving Plans</p>	<p>This is an ongoing procedure that ensures that the first two processes have been followed, that metrics are reported on, that exceptions to targets are tracked, and that improvements are fed back into the Plan phase. Proper monitoring ensures that either the original objectives are being achieved or steps are being taken to improve reliability or adjust business expectations.</p> <p>Business requirements and technologies used by SOC are both subject to frequent change. This iterative review and reporting function helps to promote an ongoing alignment between actual service delivery of SOC and business requirements, ensuring that these reliability functions are up to date and relevant.</p>	<ul style="list-style-type: none"> • Monitor service reliability of SOC • Report and analyse trends in service reliability. • Review reliability of SOC.

Attribution:

The Microsoft Operations Framework (MOF) 4.0 is provided with permission from Microsoft Corporation & these guidelines are prepared by OpsConfer. This documentation is licensed to you under the Creative Commons Attribution License. To view a copy of this license, visit [here](#)

Plan Phase

Policy Function

Why Use the Policy Function?

This Function should be useful for anyone with responsibility for IT policy, which ultimately means everyone in the IT organisation. This is because policies are not only created and maintained, but they also need to be communicated, understood, and applied.

This Function provides sufficient context to understand the reasoning behind policies, the creation, validation and enforcement of policies, and how the policy management process communicates the policy and incorporates feedback about the policy.

The purpose is to help the SOC remain in compliance with directives.

For the sake of clarity, these are the policies that address people and process; these are not machine-based control policies such as Group Policy Objects.

This Function addresses how to:

- Determine areas requiring policy.
- Create policies.
- Validate policy.
- Publish policy.
- Enforce and evaluate policy.
- Review and maintain policy.



Attribution:

The Microsoft Operations Framework (MOF) 4.0 is provided with permission from Microsoft Corporation & these guidelines are prepared by OpsConfer. This documentation is licensed to you under the Creative Commons Attribution License. To view a copy of this license, visit [here](http://creativecommons.org/licenses/by/4.0/)

Plan Phase

Policy Function | What purpose does policy serve in SOC?

What can be done so Cyber Security Professionals find company policies helpful and enforceable? This function describes the process of translating and documenting organisational goals and values into written policies.

A policy explains what to do in a particular set of circumstances by providing necessary rules and requirements and by setting expectations about conduct. Policies help organisations clarify performance requirements, communicate management's intent for how work should be done, and establish accountability and the foundation for compliance.

Procedures break policies down into detailed steps that describe how work should be done and identify who should do what. To be effective, policies and procedures need to accurately reflect what the organisation wants done—they should clearly describe circumstances, rules, options, and activities in a way that is understandable and can be readily put into practice.

Although potentially wide-ranging, policy generally renters on the following topics:

- Policy governance
- Security
- Privacy
- Partner and third-party relationships
- Knowledge management
- Appropriate use



Attribution:

The Microsoft Operations Framework (MOF) 4.0 is provided with permission from Microsoft Corporation & these guidelines are prepared by OpsConfer. This documentation is licensed to you under the Creative Commons Attribution License. To view a copy of this license, visit [here](https://creativecommons.org/licenses/by/4.0/)

Plan Phase

Policy Function | Policy Management

Policy management includes writing policies, validating policies with stakeholders, and developing detailed procedures. It also helps determine how to implement and enforce policy and establishes the ongoing processes for policy improvement and maintenance.

Any organisation approaching policy management should be aware of the relationship between its policies and its internal control environment. When management considers a certain goal and its related risks, it must also consider whether to write a policy addressing that goal.

The purpose is to communicate a clear standard of behaviour to employees so that they know they will be expected to comply. Good policy management focuses policies on the right goals, ensures review and evaluation by the right people, and helps keep policies current.



Attribution:

The Microsoft Operations Framework (MOF) 4.0 is provided with permission from Microsoft Corporation & these guidelines are prepared by OpsConfer. This documentation is licensed to you under the Creative Commons Attribution License. To view a copy of this license, visit [here](https://creativecommons.org/licenses/by/4.0/)

Plan Phase

Policy Function | Policy Management

Policy management includes writing policies, validating policies with stakeholders, and developing detailed procedures. It also helps determine how to implement and enforce policy and establishes the ongoing processes for policy improvement and maintenance.

Any organisation approaching policy management should be aware of the relationship between its policies and its internal control environment. When management considers a certain goal and its related risks, it must also consider whether to write a policy addressing that goal.

The purpose is to communicate a clear standard of behaviour to employees so that they know they will be expected to comply. Good policy management focuses policies on the right goals, ensures review and evaluation by the right people, and helps keep policies current.



Attribution:

The Microsoft Operations Framework (MOF) 4.0 is provided with permission from Microsoft Corporation & these guidelines are prepared by OpsConfer. This documentation is licensed to you under the Creative Commons Attribution License. To view a copy of this license, visit [here](https://creativecommons.org/licenses/by/4.0/)

Plan Phase



Policy Function | Goals

Goal	Measurements
Policy supports management objectives	<ul style="list-style-type: none">Audits of policies indicate that they appropriately reflect management objectives.
Employees utilise policy	<ul style="list-style-type: none">There are no audit issues related to activities defined in policies.
Regulatory compliance	<ul style="list-style-type: none">All regulatory audits are passed with no deficiencies.
Organisational compliance	<ul style="list-style-type: none">All compliance audits are passed with no deficiencies (for example, security, privacy, or standards of conduct).

Attribution:

The Microsoft Operations Framework (MOF) 4.0 is provided with permission from Microsoft Corporation & these guidelines are prepared by OpsConfer. This documentation is licensed to you under the Creative Commons Attribution License. To view a copy of this license, visit [here](#)

Plan Phase



Policy Function | Roles & Responsibilities

Role	Responsibility
Security Executive Officer (CISO)	<ul style="list-style-type: none"> Approves the SOC's organisation's policies Approves policy content and the policy management process
SOC Manager	<ul style="list-style-type: none"> Manages effectiveness of policy communication and enforcement
SOC Policy Manager	<ul style="list-style-type: none"> Works with business, management, and legal resources to define policy requirements Responsible for industry regulatory knowledge Owens policy creation, publication, and maintenance
Change Manager	<ul style="list-style-type: none"> Manages the activities of the change management process for the SOC
Configuration Administrator	<ul style="list-style-type: none"> Tracks what is changing and its impact Tracks configuration items (CIs) and updates the Configuration Management System (CMS)

Attribution:

The Microsoft Operations Framework (MOF) 4.0 is provided with permission from Microsoft Corporation & these guidelines are prepared by OpsConfer. This documentation is licensed to you under the Creative Commons Attribution License. To view a copy of this license, visit [here](https://creativecommons.org/licenses/by/4.0/)

Plan Phase



Policy Function | Key Terms


Key Terms	Description
Policy	A deliberate plan of action to guide decisions and achieve rational outcomes. (This definition deals with human-readable descriptions of desired behaviour, not machine-readable descriptions).
SOC alignment	A state when the technical and business goals and strategies of the SOC completely match the goals and strategies of the overall business.
Procedure	A detailed description of how work will be done by people or systems. It is the method for applying and implementing policy.
Process	A set of interrelated tasks that, taken together, produce a defined, desired result. Policies are translated into systems, resources, and processes to operate the business.

Attribution:

The Microsoft Operations Framework (MOF) 4.0 is provided with permission from Microsoft Corporation & these guidelines are prepared by OpsConfer. This documentation is licensed to you under the Creative Commons Attribution License. To view a copy of this license, visit [here](https://creativecommons.org/licenses/by/4.0/)

Plan Phase

Policy Function | Processes & Activities


Process	Description	Activites
 <p>Determine Areas Requiring Policy</p>	<p>A key activity in Policy is the process of aligning the goals of the SOC to those of the overall business, then using that information to decide which areas need to have policies created.</p> <p>Organisational goals should be evaluated to determine possible risks. The impact of risks can be evaluated by considering what might happen if the expectations surrounding that risk are not made clear to everyone in the organisation. If an identified risk and its impact stand in the way of achieving a goal, then it will likely need to be addressed by a policy. In this way, management establishes clear guidelines that help ensure desired performance, fitting checks and balances, and appropriate workplace interactions.</p>	<ul style="list-style-type: none"> • Documenting goals. • Assessing current state. • Envisioning future state. • Performing gap analysis.

Attribution:

The Microsoft Operations Framework (MOF) 4.0 is provided with permission from Microsoft Corporation & these guidelines are prepared by OpsConfer. This documentation is licensed to you under the Creative Commons Attribution License. To view a copy of this license, visit [here](#)

Plan Phase

Policy Function | Processes & Activities

Process	Description	Activites
 <p>Create Policy</p>	<p>In this process, the group responsible for policy creation actually drafts the policies, often through the use of a standardised policy template.</p>	
	<p>Specific types of policies are used to address different topic areas. Security policies and privacy policies may result in detailed implementations and configurations of SOC infrastructure. This may be expressed through a Group Policy Object (GPO). When taken all together, GPOs establish allowable activities related to devices, users, or user role in an organisation. Because of this tight relationship between security and privacy policy and group policy this is an area where SOC has developed considerable expertise and collateral knowledge.</p>	<ul style="list-style-type: none"> • Creating policy governance policies. • Creating security policies. • Creating privacy policies. • Creating partner relationship policies. • Creating knowledge management policies. • Creating appropriate use policies.
	<p>Policy areas such as partner relationships, appropriate use, or knowledge management are often enforced through contracts and documents that are not directly machine-consumable.</p>	
	<p>In these areas SOC needs to assess the role of technology for gathering evidence of activity or prohibiting activity that would be in violation of policy. SOC should have an awareness of the goals of these broader policies, and then assist the business in understanding the technology implications for enforcement and evaluation.</p>	

Attribution:

The Microsoft Operations Framework (MOF) 4.0 is provided with permission from Microsoft Corporation & these guidelines are prepared by OpsConfer. This documentation is licensed to you under the Creative Commons Attribution License. To view a copy of this license, visit [here](https://creativecommons.org/licenses/by/4.0/)

Plan Phase

Policy Function | Processes & Activities

Process	Description	Activites
Validate Policy	In this process, policies must be validated with all stakeholders of the business. Because an organisation's policies may have serious legal implications, validation requires careful attention to detail.	<ul style="list-style-type: none"> Performing policy review. Reviewing comments and revising policies. Managing policy configuration.
Publish Policy	In this process, policies are published for the organisation to use. Although the process is fairly simple, the effects of poor publication can be difficult to recover from. The business must be notified in advance of the pending policy release, provided with the location of policies that everyone can find, and given the opportunity to become trained on the policies.	<ul style="list-style-type: none"> Publish policy
Enforce and Evaluate Policy	In this process, policies are enforced, and then evaluated for their effectiveness. Without an evaluation exercise, organisations may find that certain policies are actually impeding people's ability to get work done; often an increase in the number and severity of violations is an indicator that policies need to be adjusted.	<ul style="list-style-type: none"> Enforcing the policy. Requesting corrective action. Analysing policy enforcement. Evaluating policy effectiveness. Requesting policy change.




Attribution:

The Microsoft Operations Framework (MOF) 4.0 is provided with permission from Microsoft Corporation & these guidelines are prepared by OpsConfer. This documentation is licensed to you under the Creative Commons Attribution License. To view a copy of this license, visit [here](https://creativecommons.org/licenses/by/4.0/)

Plan Phase

Policy Function | Processes & Activities

Process	Description	Activites
 Review and Maintain Policy	<p>Policies are only as effective as the relevance and accuracy of their information; policy violations increase when that information is out of date or doesn't address what the user is seeking.</p> <p>To ensure that policies stay current and relevant, the organisation should schedule regular policy reviews and make adjustments and changes as a result of those reviews.</p> <p>Because policy change often has legal considerations, the process should include documentation indicating that changes have occurred, why they happened, and who approved them.</p>	<ul style="list-style-type: none"> • Reviewing policy. • Controlling policy configuration. • Changing pol

Attribution:

The Microsoft Operations Framework (MOF) 4.0 is provided with permission from Microsoft Corporation & these guidelines are prepared by OpsConfer. This documentation is licensed to you under the Creative Commons Attribution License. To view a copy of this license, visit [here](http://creativecommons.org/licenses/by/4.0/)

Plan Phase

Financial Management Function

Why Use the Financial Management Function?

Lets start with some question.

How does your organisation...

- Determine the value of SOC services?
- Weigh financial risk and return to understand the value SOC provides?
- Strike the desired balance between risk and expected financial contribution to the business?

Competent financial management will help you accomplish these objectives.

The goal of this Function is to provide SOC-relevant activities and considerations that improve financial management practices.

When management makes decisions about changes to SOC infrastructure, systems, staffing, or processes, it uses financial data to justify the cost. However, cost tells only part of the story; value must be considered as well. The concept of value reflects service levels, business impact, and both hard and soft benefits. Financial management ensures that SOC services and solutions have agreed-upon value delivery expectations, as well as metrics for tracking and realising value, cost justification, and adequate budgetary support.



Attribution:

The Microsoft Operations Framework (MOF) 4.0 is provided with permission from Microsoft Corporation & these guidelines are prepared by OpsConfer. This documentation is licensed to you under the Creative Commons Attribution License. To view a copy of this license, visit [here](http://creativecommons.org/licenses/by/4.0/)

Plan Phase



Financial Management Function | Goals

Goal	Measurements
SOC cost accounting	<ul style="list-style-type: none"> SOC costs accounted for and tracked Costs reviewed and improvements in progress
Delivered business value	<ul style="list-style-type: none"> Each project evaluated for expected business value Project benefits consistently realised
SOC cost recovery	<ul style="list-style-type: none"> Customers charged fairly Charging model relevant and appropriate for the organisation
Accurate SOC budget	<ul style="list-style-type: none"> Comprehensive financial understanding of SOC Actual budget is close to projected budget, without surprises

Attribution:

The Microsoft Operations Framework (MOF) 4.0 is provided with permission from Microsoft Corporation & these guidelines are prepared by OpsConfer. This documentation is licensed to you under the Creative Commons Attribution License. To view a copy of this license, visit [here](http://creativecommons.org/licenses/by/4.0/)

Plan Phase



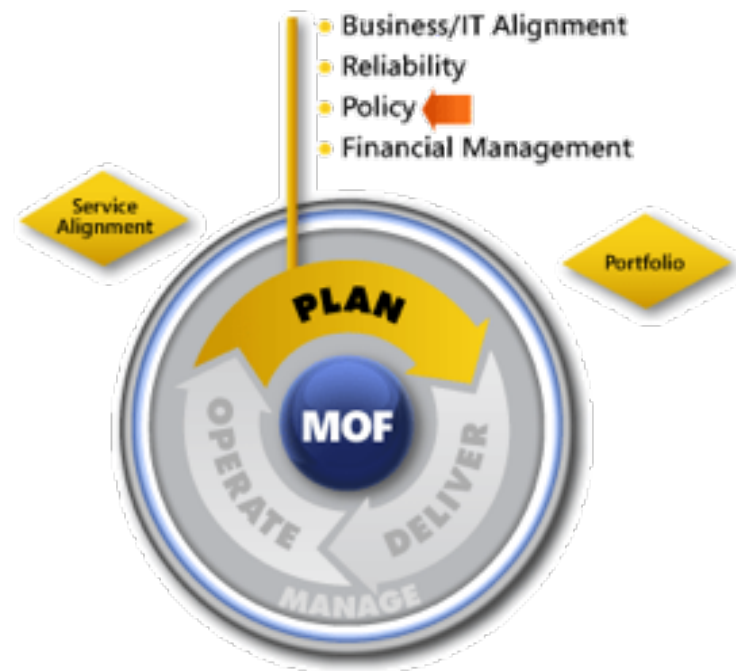
Financial Management Function | Roles & Responsibilities

Role	Responsibility
SOC Manager	<ul style="list-style-type: none">Manages the overall business value realization process for SOC.Manages risk and approves expenditures
SOC Finance Manager	<ul style="list-style-type: none">Manages the financial aspect of the SOC organisation
Business Relationship Manager	<ul style="list-style-type: none">Acts as communication interface between SOC and the business and customers

Attribution:

The Microsoft Operations Framework (MOF) 4.0 is provided with permission from Microsoft Corporation & these guidelines are prepared by OpsConfer. This documentation is licensed to you under the Creative Commons Attribution License. To view a copy of this license, visit [here](#)

Plan Phase



Financial Management Function | Key Terms


Key Terms	Description
Operational costs	Costs resulting from the day-to-day running of SOC—for example, staff costs, hardware maintenance, and electricity. Also referred to as non-discretionary spending.
Return on investment (ROI)	The ratio of money gained or lost on an investment relative to the amount of money invested.
Total cost of ownership (TCO)	The total cost of an item over its useful lifetime. TCO takes into account not only the purchase price, but also implementation and training costs, management costs, and support costs.
Value realisation	The identification, definition, monitoring, and evaluation of targeted business benefits that result from planned SOC activities.

Attribution:

The Microsoft Operations Framework (MOF) 4.0 is provided with permission from Microsoft Corporation & these guidelines are prepared by OpsConfer. This documentation is licensed to you under the Creative Commons Attribution License. To view a copy of this license, visit [here](https://creativecommons.org/licenses/by/4.0/)

Plan Phase

Financial Management Function | Processes & Activities


Process	Description	Activities
Establish Service Requirements and Plan Budget 	<p>Proactive and strategic use of technology requires that SOC do more than simply account for costs. SOC must understand the broader drivers affecting the organisation and translate these into SOC service initiatives.</p> <p>When SOC's expected contribution to business results is understood, these expected benefits need to be tracked and managed through a process called value realisation.</p>	<ul style="list-style-type: none"> • Addressing service requirements and business strategy. • Planning a budget. • Conducting a budget review. • Managing SOC value realisation.
Manage Finances	<p>This process includes many traditional financial management activities, such as budgeting, costing models, charge-back models, cost allocations, cost management, and reporting.</p> <p>SOC can manages its own finances, but that responsibility lies with corporate finance.</p> <p>The process also involves preparing and managing a SOC budget that reflects the business priorities identified earlier in the process. Most budgets are loosely categorised into three areas:</p> <ul style="list-style-type: none"> • Ongoing operations and maintenance spending (non-discretionary spending). • Project spending (discretionary spending) • Innovation—a focus on investments in improving the efficiency and effectiveness of ongoing operations and/or improvements to business value 	<ul style="list-style-type: none"> • Managing SOC finances. • Creating SOC budget. • Determining maintenance and operations costs. • Developing innovation and improvement initiatives. • Determining project costs. • Establishing value realisation awareness across SOC.

Attribution:

The Microsoft Operations Framework (MOF) 4.0 is provided with permission from Microsoft Corporation & these guidelines are prepared by OpsConfer. This documentation is licensed to you under the Creative Commons Attribution License. To view a copy of this license, visit [here](https://creativecommons.org/licenses/by/4.0/)

Plan Phase

Financial Management Function | Processes & Activities

Process	Description	Activites
 <p>Perform SOC Accounting and Reporting</p>	<p>The final process in the Financial Management Function involves SOC accounting, reporting, and cost recovery.</p>	
	<p>The guidelines and frameworks for these activities have already been established, so the activities in this process are mostly focused on tracking and reporting the actual costs.</p>	
	<p>The information recorded in this process provides financial managers with:</p> <ul style="list-style-type: none"> • Costs to use in budget comparisons. • Service usage reports that can be used as the basis for cost recovery (if this is the model that the IT organisation employs). • The actual derived benefits to the business for the services that are delivered. 	<ul style="list-style-type: none"> • Perform SOC Accounting and Reporting

Attribution:

The Microsoft Operations Framework (MOF) 4.0 is provided with permission from Microsoft Corporation & these guidelines are prepared by OpsConfer. This documentation is licensed to you under the Creative Commons Attribution License. To view a copy of this license, visit [here](https://creativecommons.org/licenses/by/4.0/)

OpsConfer Project Management Module

**Manage the complete SOC Project using Project Management Framework of OpsConfer.
Its 100% customisable based on your project needs. Reach to us on services@opsconfer.com to know more.
It helps you document and track the following.**

Management:

The Management Section helps us establish an integrated approach to service management activities through the use of risk management, change management, and controls. It also provides guidance related to team management.

Phase:

Here you can add all the activities and processes involved in managing a service (its conception, development, operation, maintenance and ultimately - its retirement) into separate distinct phases.

Functions:

Here we organise activities and processes into Functions which provide operational guidance for capabilities within the service management environment. And each Function is anchored within a related phase.

Goals:

Functions also contain a unique set of goals supporting the objectives of those phase. Management can use this to provide efficient management reviews This will help organisations ensure that their technology services are on track to deliver expected business value.

Roles:

Roles gives an Indication on who is responsible for each functions. Also we use this to provide role based access control towards tasks around those functions.

Key Terms:

This will show all the important terms that are used on each function.

Process:

Process is a set of activities that interact to achieve a result. This is more of a high level information.

Activity:

Activity is a set of tasks that interact to achieve a result. This will be more specific compared to Process.

Task:

This is the work that is done to complete an Activity. Resources will be assigned based on the role that are assigned on the function level.

Attribution:

Thank you

This is a heavily modified version based on Microsoft® Operations Framework (MOF) and this consists of integrated best practices, principles, and activities that provide comprehensive guidelines for achieving reliable SOC based on my experience.

This framework provides question-based guidance that allows you to determine what is needed for your organisation now, as well as activities that will keep the SOC running efficiently and effectively in the future.

This documentation encompasses all of the activities and processes involved in planning a Security Operations Centre. Here we organised activities and processes into Functions, which were again grouped together in plan phase.

Each Functions contained a unique set of goals and outcomes supporting the objectives of that phase. We can easily consider that this plan phase is completed can be considered after ensuring that all the goals mentioned are achieved in an appropriate fashion.

If you liked this work, you can follow us on Facebook, twitter & linked-in as mentioned below; more similar documentations are on its way.

Look for further documentations on Deliver, Operate and Manage Phase/sections of SOC Implementation Project. It will also continue similar documentation style.

We are an IT startup that is based at Bangalore, India and we focus on Cyber Security, Cloud & Security services. We also work with MSSPs and work towards setting up a matured SOC.

At any point if you need any assistance, please feel free to reach to us on services@opsconfer.com. We we will be happy to assist you.

Thank you,
Ashwin Venugopal

Website: www.opsconfer.com

Facebook: <http://facebook.com/opsconfer/>

Twitter: <http://twitter.com/OpsConfer>

Linked-in: <http://linkedin.com/company/opsconfer/>

Attribution:

The Microsoft Operations Framework (MOF) 4.0 is provided with permission from Microsoft Corporation & these guidelines are prepared by OpsConfer. This documentation is licensed to you under the Creative Commons Attribution License. To view a copy of this license, visit [here](http://creativecommons.org/licenses/by/4.0/)

