



Business Management System Manual

Owner Name: Process Excellence Team (PeX)

Version: 2.1



Document History

Date	Version	Summary of Changes	Author	Approved By
May 10 '25	2.0	Updated release of business management system with all standards integrated and accommodating organizational Changes	Shalot Leely	Ambrish
June 23rd '25	2.1	<ul style="list-style-type: none">- Updated Address by including 5th floor - right wing and 6th floor- Added Climate in Context of Organization- Updated HSE KPI Targets	Shalot Leely	Ambrish

Statement of Confidentiality

This Neurealm Private Limited (formerly known as GAVS Technologies Private Limited) artefact and/or document and/or presentation is strictly confidential and it contains proprietary information intended only for recipients of Neurealm Private Limited (Neurealm). The recipient acknowledges and agrees that: (i) this artefact and/or document is not intended to be distributed (ii) the recipient does not have the right to implement, copy, reproduce, fax, print, publicly divulge, or further distribute it, in whole or in part in any form, without seeking the express written permission from Neurealm. Any unauthorized use of the contents of this artefact and/or document and/or presentation in any manner whatsoever, is strictly prohibited. The artefact and/or document and/or presentation represents Neurealm's current product offerings and best practices which are subject to change without notice. Please note that Neurealm collaborates in relation to some of its offerings.

All third-party trademarks used herein belong to their respective owners and may be protected by law. This artefact and/or document and/or presentation only refers to such trademarks under the doctrines of nominative and descriptive fair usage to illustrate and explain concepts without implying violation of any legal constraints. If any improper activity is suspected, all available information may be used by Neurealm for lawful purposes and to seek appropriate remedies. Neurealm complies with applicable privacy laws and regulations. Recipients are advised to handle the information contained in this Material in accordance with relevant privacy and data protection laws.

Contents

1. PURPOSE	7
2. NORMATIVE REFERENCE	7
3. TERMS AND DEFINITIONS	8
4. CONTEXT OF THE ORGANIZATION	9
Understanding the organization and its context	9
Understanding the needs and expectations of Interested Parties	9
5. LEADERSHIP	20
Leadership and Commitment	20
Compliance Officer	32
OHS Officer	32
6. PLANNING	33
7. SUPPORT	42
8. OPERATION	48
9. PERFORMANCE EVALUATION	59
10. IMPROVEMENT	64
Incidents, Nonconformity and corrective action	64
A. Organization chart	65
B. HSE Organization chart	66
C. HSE Requirements by Contractors including outsourced services (To be a part of contract documents)	67
Confined Space	67
Working at Height	68
Fall Prevention System	68
Fall Protection Systems	68
Scaffolding	69
Stairways and Ladders	69
Roof Work/Access	69
Overhead Work	69
Lifting Operations	69
Lifting Equipment and Accessories	70
Lockout Tag out (“LOTO”)	70
Barricades	70
Hot Works	71
Trenching, Excavating, Drilling and Concreting	71
Environmental Requirements Waste Management	71
Spills	71
Emissions	71

Introduction

Satisfied customers, motivated and committed employees as well as a positive atmosphere are pre-requisites for the durable economic success of our company. Market-driven prices, quality of products and services, plus stable tools and work-flows guarantee customer satisfaction and the protection of both employees and the environment.

To permanently meet this significant challenge, we have developed and implemented a Business Management System (also known as Quality Assurance System). This Apex level manual lays down the Business Management System (BMS) aligned to the requirements of PAS 99:2012 and it addresses all the requirements of ISO 9001, ISO 20000-1, ISO 27001, ISO 45001, and Best practices SEI-CMMi DEV & SVC. PAS 99:2012 has been taken as the basis for the nomenclature of the common requirements.

This business management system forms the basis and the means to ensure the operative implementation of our strategic objectives. It comprises all those main activities that guarantee customer benefit, sustainability, and stability. It is focused on our business processes, our work methods, and our corporate culture.

The business management system provides our customers, partners, employees, suppliers and shareholders with an insight into what we do and how we do it. While it is basically designed for the benefit of our customers, it also acts as a guideline for our employees to ensure successful action and interaction within our business processes.

This manual provides an overview of the integrated quality, information security and IT service management systems that have been established at Neurealm together with their structure and operations

[Ambrish Sethi](#)

Director – Delivery Excellence

1. PURPOSE

This document describes the business management system (BMS) of Neurealm Company.

The BMS has been established to

- a. Demonstrate Neurealm's ability to consistently provide product that meets clients and applicable legal, statutory and regulatory requirements
- b. Enhance client satisfaction through the effective application of the system, including processes for continual improvement of the system and the assurance of conformity to customer and applicable statutory and regulatory requirements.
- c. Eliminate or minimize risks to the environment, personnel and other interested parties who could be exposed to Occupational Health, Safety and Environment hazards associated with Neurealm's activities, products and services.
- d. Assure Neurealm of its conformity with its stated BMS Policy and
- e. Demonstrate Neurealm's conformity with the ISO 9001, ISO 20000-1, ISO 27001, OHSAS – ISO 45001 Standards, PCI-DSS and HIPAA

Note: Refer to Neurealm's Corporate Profile for more information.

2. NORMATIVE REFERENCE

The following reference is indispensable for the application of this document:

ISO 9000, Fundamentals and Vocabulary

ISO 9001 – Standard for Quality Management System

ISO 27001 – Standard for Information Security Management system

ISO 20000-1 - Standard for IT Service Management System

ISO 45001 – Occupational Health and Safety Management system

PCI-DSS – Payment Card Industry – Data Security Standard

HIPAA – Health Insurance Portability and Accountability Act

GDPR – General Data Protection Regulations

3. TERMS AND DEFINITIONS

For the purpose of this document, the terms and definitions given in ISO 9000, OHSAS – ISO 45001 apply, including

Abbreviations / Acronym	Description
Neurealm	refer to Neurealm Pvt Ltd Company
Product	Includes both the goods and services of Neurealm (where suitable),
BMS	refers to Neurealm’s Business Management System which is an integrated documented system covering all the standards mentioned under the scope in this document
HIPAA	Health Insurance Portability and Accountability Act
OHS	Occupational health and safety
ADM	Application Development Maintenance
IMS	Infrastructure Management Services
ISMS	Information Security Management System
OHSA	Occupational Health Safety Assessment Series
PCI-DSS	Payment Card Industry - Data Security Standard
Danger	A state or condition in which the personal injury is reasonably foreseeable
Emergency	A serious situation or occurrence that happens unexpectedly and demands immediate action as it has the potential to seriously harm the health, safety of a group of associates or has the potential of large environmental impact.
Hazard	Source or situation with a potential for harm and cause injury or ill health, impact the environment or a combination of these.
Interested	Individual or groups outside Neurealm concerned with or affected by the Health, Safety and Environment Management Systems performance of Neurealm
ERT	Emergency Response Team
CSM	Customer Success Manager

4. CONTEXT OF THE ORGANIZATION

Understanding the organization and its context

Neurealm has determined external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its Business Management System (BMS)

Evaluating the organisation's external context may include,

- Social and cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environment whether international, national, regional, Climate or location
- Relationship with, and perceptions and values of, external stakeholders
- Other factors and trends having an impact on the objectives of the organization

Evaluating the organisation's internal context may include,

- Governance, organizational structure, roles and accountabilities
- Policies, objectives and strategies that are in place to achieve them.
- Capabilities, understood in terms of resources and knowledge and competence
- Information systems, information flows
- Relationship with, and perception and values of, internal stake holders
- The organization's culture
- Standards, guidelines and models adopted by the organisation
- The form and extent of contractual relationship and
- Identifying key interface between systems, potential conflicts that may arise and process for resolving them
- Needs and expectations of workers and other interested parties

Understanding the needs and expectations of Interested Parties

Neurealm has determined the interested parties and impacts on them that are relevant to the Business Management System as per clause 4.1

Some of the internal and external interested parties are listed below are considered for understanding the needs and expectations.

Interested Parties	
Citizens	Organizations
Media	Customers
Management	Insurers
Top Management	Emergency Services
Government	Transport Services
Regulators	Dependents of staff
Stake Holders	Other staff and Contractors
Those who accountable for BMS Policy and its implementation	Those who Implement maintain BMS and Risk process
Competitor	Neighbour
Suppliers / Vendors	

Interested Party	Needs and Expectations	Process Implementation Indicator Reference
Employees (Full time , Contract, Retainer)	<ul style="list-style-type: none"> • Safe working environment • Job security • Competitive Salary • Training and development • Consultation • Communication • Participation • Recognition & Reward • Insurance coverage 	<ul style="list-style-type: none"> • Health & Safety Policy • Process for Performance Management • Process for Learning & Development • Process for Rewards & Recognition • Code of Conduct – Policy • Other HR policies available in Neurealm Intranet site
Legal / Regulatory/ Statutory Requirements from State / Central / Local Authorities	<ul style="list-style-type: none"> • Safety, Health & Welfare at work act • General application of regulations • Organization of working time • Maternity Protection Act • Employment Equality Act • Other legal / regulatory /statutory requirements are managed by HSE function, HR and Compliance (Finance) function 	<ul style="list-style-type: none"> • Occupational Health & Safety Policy • Process for Legal & Statutory compliance management
Contractors	<ul style="list-style-type: none"> • Provide Health and Safety environment and PPE when they are at work at Neurealm • Comply with contracts 	<ul style="list-style-type: none"> • Occupational Health & Safety Policy • Std. Practice for Administration
Customers	<ul style="list-style-type: none"> • Employees working for customer, their Health and Safety is ensured • Competitive price for the deliverable / services • Comply with all legal / statutory /regulatory / contractual requirements • Fulfilling the requirements as per the contract 	<ul style="list-style-type: none"> • Occupational Health & Safety Policy • Std. Practice for Administration • Std. Practice for Legal/Statutory Management • Std. Practices for Software Development & Service Delivery that are listed under ADM and IMS in Neurealm Policy Central
Neighbours	<ul style="list-style-type: none"> • Comply with Health & Safety norms to avoid any hazardous situation to the neighbour 	<ul style="list-style-type: none"> • Occupational Health & Safety Policy • Std. Practice for Administration
Co-tenants	<ul style="list-style-type: none"> • Comply with norms, terms and conditions agreed with building owner 	<ul style="list-style-type: none"> • Occupational Health & Safety Policy • Std. Practice for Administration

Visitors / Guests	<ul style="list-style-type: none"> • Provide Health and Safety environment and PPE when they are at work at Neurealm 	<ul style="list-style-type: none"> • Occupational Health & Safety Policy • Std. Practice for Administration
Suppliers / Vendors & Third party service providers	<ul style="list-style-type: none"> • Provide Health & Safe environment when they are at Neurealm. • Timely payments within the credit period, • Provide required support for the GST and other tax details if any required during the business deals. • Provide feedback on the service in a timely manner 	<ul style="list-style-type: none"> • Occupational Health & Safety Policy • Std. Practice for Administration • Policy – Third Party Management

The requirements of these interested parties are managed by the concerned functions to meet their expectation and satisfaction through business management system processes defined at the customer success management function and support function.

The customer and interested parties' requirements are identified and controlled through processes established in the BMS Manual and Processes to meet their expectation and satisfaction through the following measures

- ❖ Contract with customer / third parties
- ❖ Service Management Plan (SMP) / Software Development Plan
- ❖ Service Level Performance Reporting
- ❖ Issues, Risks, Ideas, Improvements
- ❖ Customer satisfaction Surveys
- ❖ Local and National Government Regulator / Grid Codes requirements and Legal requirements on OHS, and ISMS along with
- ❖ BMS Policy, objectives and systems in place

As part of continual improvement initiative, every function has an annual goal defined using the balanced score card approach that will have goals on the following perspectives, a) Customer b) Financial c) Internal Process d) Learning & Growth – Capability (Strategic, Tactical / Operational at various levels of the function). Performance of goals is measured every six months as part of the performance appraisal process. Annual goal sets are reviewed by the Leadership team every quarter with the respective function and account / engagement level as well as in the management review (quality council / security council or other review meetings). The leadership team has established a Customer success management platform to keep track of customer success goals / expectations, internal / external issues, risks, performance of BMS and improvement proposals. The CSM function will establish a Service Management Plan / Software development plan and use the CSM platform to keep track of the customer requirements / expectations, objectives / KPI target, internal / external issues, expectations of third parties & suppliers, risks/opportunities, issues, ideas / improvement proposals in achieving the intended outcome.

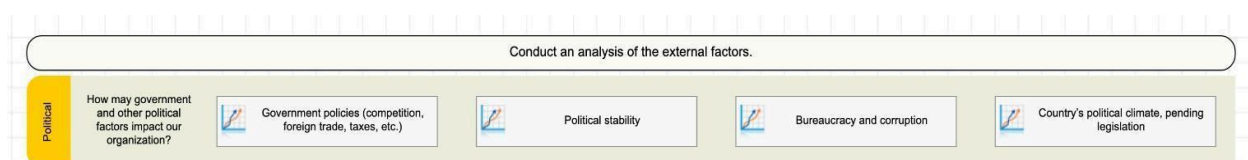
The concerned functions (internal group) of Neurealm have developed business processes to keep track of requirements, including legal, statutory and other requirements for ensuring relevant information is communicated to and from employees and interested parties regarding internal / external issues. Each department is responsible to capture discrepancies with respect to data/information flow with customers and address the same for timely mitigation.

The concerned departments have developed necessary mechanisms for identifying and accessing the legal and other requirements which are applicable as well as which may become applicable because of new legislation/or amendment of existing Acts/Rules. Mapping of legal requirements and processes is done by the head of department as and when there is a change in the process.

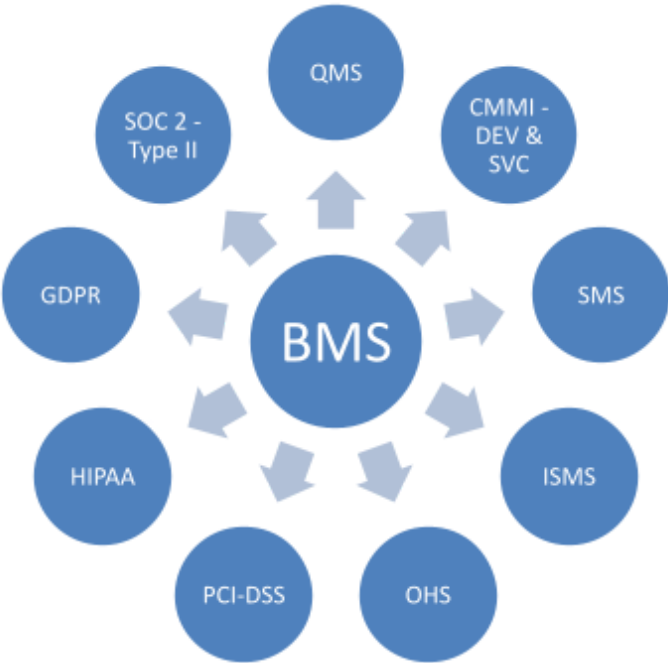
PESTEL framework should be used to identify an internal / external issues and associated risks./ opportunities

P	E	S	T	E	L
Political	Economic	Social	Technological	Environmental	Legal
<ul style="list-style-type: none"> Government policy Political stability or instability overseas Foreign trade policy Tax policy Labor laws Terrorism and military considerations Environmental laws Funding grants and initiatives Trade restrictions Fiscal policy 	<ul style="list-style-type: none"> Economic Growth Interest Rates Exchange rates Inflation Disposable income of consumers Disposable income of businesses Taxation Interstate taxes Wages rates Financing capabilities 	<ul style="list-style-type: none"> Population growth Age distribution Health consciousness Career attitudes Customer buying trends Cultural trends Demographics Industrial reviews and consumer confidence Organizational image 	<ul style="list-style-type: none"> Producing goods and services Emerging technologies Technological maturity Distributing goods and services Target Market Communication Potential Copyright infringements Increased training to use innovation Potential Return on Investment (ROI) 	<ul style="list-style-type: none"> The decline of raw materials Pollution and green house gas emissions Promoting positive business ethics and sustainability Reduction of their carbon foot print. Climate and weather Environmental Legislation Geographical location (and accessibility) 	<ul style="list-style-type: none"> Health & Safety Equal Opportunities Advertising Standards Consumer Rights and laws Product Labeling Product Safety Safety Standards Labor Laws Future Legislation Competitive Legislation

PESTEL tool Steps



Determining the scope of the Business Management System (BMS)
Neurealm has determined the boundaries and applicability of the BMS to establish its scope. When determining this scope, the organization has considered a. External and Internal issues referred to in 4.1 b. Requirements referred to in 4.2



S.No.	Site / Location	Applicability of ISO standard for certification	Applicability of other compliance requirements	Remarks / Exclusions if any
1.	Neurealm Private Limited 5th -right wing , 6th & 7th , Floor, Block B, Futura Tech Park, 334, Rajiv Gandhi Salai (OMR) Sholinganallur, Kancheepuram, Chennai - 600 119, Tamil Nadu	ISO 9001, ISO 20000-1, ISO 27001, HIPAA, PCI-DSS and ISO 45001	SOC 2 Type II HITRUST	No Exclusions.
2.	Neurealm N.A., Inc 155 Village Blvd, Suite 300, Princeton, New Jersey 08540 Tel no : 609-201-2565 Fax no : 609-201-2678	ISO 27001:2022, HIPAA	SOC 2 Type II	No Exclusion

Business Management System Manual

13

3.	Neurealm Private Limited 8th Floor, Amar Arma Genesis, Baner Road, Pune , Maharashtra, 411045, India	ISO 27001:2022	SOC 2 Type II	No Exclusion
4.	Neurealm Private Limited Office no. 119 to 126, 1st Floor Race Course Tower, Near Natubhai Circle Racecourse Road Vadodara , Gujarat, 390 005, India	ISO 27001:2022	SOC 2 Type II	No Exclusion

SITE NAME AND ADDRESS	SCOPE OF THE AUDIT	NO. OF EMPLOYEES ON SITE
Neurealm Private Limited 5th -right wing , 6th & 7th Floor, Block B, Futura Tech Park, 334, Rajiv Gandhi Salai (OMR) Sholinganallur, Kancheepuram, Chennai - 600 119, Tamil Nadu.	<p>ISO 9001:2015 : Provision of End-to-End Enterprise Solutions Services including IT Infrastructure Managed Services driven through AI and automation, Application Management Services, Product Engineering Services, Data Management Services, Quality Assurance & Testing Services, Information Security Services, Automation-led digital transformation services, IP led solution and Zero Incident Framework TM (ZIF) and IT Infrastructure Management Services.</p> <p>ISO 45001:2018 : HSE Management System applies to End-to-End Enterprise Solutions Services including IT Infrastructure Managed Services driven through AI and automation, Application Management Services, Product Engineering Services, Data Management Services, Quality Assurance & Testing Services, Information Security Services, Automation-led digital transformation services, IP led solution and Zero Incident Framework TM (ZIF).</p> <p>ISO/IEC 20000-1:2018 : Service Management System of Neurealm Technologies Private Limited which supports Managed IT Infrastructure Services, Virtualization Services, Automation Services, AI based Real-time IT Infrastructure Monitoring Services, Predictive Analytics</p>	1300

	<p>Services, Auto Discovery Services, Auto Self-healing Services, Digital Transformation Services and Machine Learning as a Service.</p> <p>HIPAA : Providing IT Infrastructure Managed Services Driven through AI and Automation, Virtual Desktop as a service, Application Management & Support Services, Product Engineering Services, Data Management Services, Information Security Service and IP led Solution using Zero Incident Framework TM (ZIF) for Healthcare Sector Customers.</p> <p>ISO/IEC 27001:2022 : Information Security Management System applies to End-to-End Enterprise Solutions Services including Infrastructure Managed Services Driven through AI and Automation, Application Management Services, Product Engineering Services, Data Management Services, Quality Assurance & Testing Services, Automation-led Digital Transformation Services, IP led Solution and Zero Incident Framework TM (ZIF) Supported by HR & Training, Physical & Environmental security, IT, Finance & Legal, Marketing, Quality and Senior Management Functions. This is in accordance with the statement of applicability Version 3.01 dated 10th November 2023.</p>	
<p>Neurealm N.A., Inc</p> <p>155 Village Blvd, Suite 300, Princeton, New Jersey, 08540, United States</p>	<p>ISO/IEC 27001:2022 : Information Security Management System applies to End-to-End Enterprise Solutions Services including Infrastructure Managed Services Driven through AI and Automation, Application Management Services, Product Engineering Services, Data Management Services, Quality Assurance & Testing Services, Automation-led Digital Transformation Services, IP led Solution and Zero Incident Framework TM (ZIF) Supported by HR & Training, Physical & Environmental security, IT, Finance & Legal, Marketing, Quality and Senior Management Functions. This is as per SoA Ver 3.01 dated 10th November 2023.</p> <p>HIPAA : Providing IT Infrastructure Managed Services Driven through AI and Automation, Virtual Desktop as a service, Application Management & Support Services, Product Engineering Services, Data Management Services, Information Security Service and IP led Solution using Zero Incident Framework TM (ZIF) for Healthcare Sector Customers.</p>	55
<p>Neurealm Private Limited</p> <p>8th Floor, Amar Arma Genesis, Baner Road, Baner, Pune , Maharashtra, 411045, India</p>	<p>ISO/IEC 27001:2022 : Information Security Management System applies to End-to-End Enterprise Solutions Services including Infrastructure Managed Services Driven through AI and Automation, Application Management Services, Product Engineering Services, Data Management Services, Quality Assurance & Testing Services, Automation-led Digital Transformation Services, IP led Solution and Zero Incident Framework TM (ZIF) Supported by HR & Training, Physical & Environmental security, IT, Finance & Legal, Marketing, Quality and Senior Management Functions. This is in accordance with</p>	126

	the statement of applicability Version 3.01 dated 10th November 2023.	
<p>Neurealm Private Limited</p> <p>Office no. 119 to 126, 1st Floor Race Course Tower, Near Natubhai Circle Racecourse Road , Vadodara , Gujarat, 390 005, India</p>	<p>ISO/IEC 27001:2022 : Information Security Management System applies to End-to-End Enterprise Solutions Services including Infrastructure Managed Services Driven through AI and Automation, Application Management Services, Product Engineering Services, Data Management Services, Quality Assurance & Testing Services, Automation-led Digital Transformation Services, IP led Solution and Zero Incident Framework TM (ZIF) Supported by HR & Training, Physical & Environmental security, IT, Finance & Legal, Marketing, Quality and Senior Management Functions. This is in accordance with the statement of applicability Version 3.01 dated 10th November 2023.</p>	1

Neurealm Chennai:

Areas covered under Neurealm Corporate Services are provided below

1. Inside Office buildings
 - a. 6th Floor - Training Room, TAG, Admin, Hub Room, Pantry, Facility room, Prayer room, Yoga room
 - b. 7th Floor
 - c. 5th Floor - Right Wing
2. Transportation
3. Housekeeping

Areas managed by Building Owner / Land Lord. However, the hazards identified will be reported to the Land Lord / Building owner for resolution.

1. UPS
2. Buildings and Surroundings
3. DG
4. STP
5. Lifts
6. Transformer
7. HT/LP Panels
8. RO Plant
9. Fire Alarm System
10. Solid Waste yard
11. AHU / Air Conditioners outside Neurealm Office
12. Emergency drill
13. Earth pit test

HIPAA Scope (HIPAA)

Healthcare applications management and IT Infrastructure services provided in the Healthcare projects functioning from Neurealm Private Limited, Chennai

PCI – DSS Scope

IT Infrastructure Management Services of FBB, Frontier and ZIF

As per PCI-DSS v4.0.1, the scope shall be reviewed semi-annually and additionally upon any significant infrastructure changes, to ensure continued relevance, effectiveness, and alignment with compliance and operational requirements

Location:

Neurealm Pvt Ltd
5th -right wing , 6th & 7th Floor , Block B, Futura Tech Park, 334, Rajiv Gandhi Salai
(OMR) Sholinganallur, Kancheepuram, Chennai - 600 119, Tamil Nadu

Business Management System

Top Management of Neurealm is committed to the BMS and Head of Delivery Excellence is responsible for development, implementation and maintenance of Business Management System (BMS), and continually improving its effectiveness. BMS is developed in accordance with the requirements of the ISO 9001, ISO 20000-1, ISO 27001, ISO 45001 standards, PCI-DSS, HIPAA, GDPR and SEI-CMMi DEV & SVC model. The Business Management System has been developed involving various departments to provide services to its internal and external customers.

As such, Neurealm has

- a) Determined the business processes needed for the BMS and the same has been documented in the form of Policies, Standard practices (also known as Process / Procedures), Check-list, Guidelines, Formats and templates along with their application throughout the organization,
- b) The document standard practice includes and is not limited to the sequence and relation / reference to processes, entry criteria, completion criteria, service level agreement and arrangement of resources required to support the business processes.

Neurealm monitors, measures where applicable, analyses and implements actions necessary to achieve planned results and continual improvement of these processes.

By default, Neurealm will not outsource the core product development, where Neurealm chooses to outsource any process that affects product conformity to requirements, it ensures control over such processes are managed using supplier

management processes. Outsourced processes are subject to the requirements of the BMS. Processes needed for the BMS referenced above include processes of management activities, provision of resources, product realization, management of OHS risks, measurement, analysis and improvement.

Neurealm's BMS documentation includes the following

- a) BMS Policy
- b) BMS Objectives consists of objectives & KPI set for Quality, Information Security, OHS, HIPAA and Service Management Systems
- c) BMS Manual
- d) Standard Practices and records required by the management system standards, and
- e) Documents, including records, format, check-list, guideline and template that are necessary to ensure the effective planning, operation and control of its processes.
- f) HIPAA Manual
- g) GDPR Policy

S.No.	BMS Objectives / Goals	Target	Remarks
1.	Overall (BMS) Process Health Compliance	>85%	This includes comply to Quality / ITSM / ISMS / PCI-DSS / HIPAA/ CMMi /HSE requirements
2.	ISMS Compliance	100%	
3	QMS Compliance	90%	
4	ITSM Compliance	90%	
5.	HSE Compliance	100%	
6.	PCI-DSS Compliance	100%	
7.	Customer Success Survey Score	Minimum 60% and above >= 4 Score	

Occupational Health & Safety:-

S. No.	Action	KPI	UOM	Target
1	Proact	No. of Near Miss Incidents reported	Number	Track Actuals
2		Emergency Drills once in a year	Number	1
3		Food Inspection every day	%	100%
4		Food Test conducted by external lab twice a year	Number	4

5	i ve	Availability of emergency equipment	%	100%
6		Number of Risk Assessment carried out - Once in a quarter	Number	0
7		No. of Hazards identified / reported	Number	Track Actuals
1	Rea cti v e	No. of Incidents reported & closed related to Safety	Number	Track Actuals
2		No. of Incidents reported & closed related to Health	Number	Track Actuals
3		No. of Fatal Accident	Number	0
4		No. of issues reported related to occupational health (Employees Data HR is Tracking)	Number	Track Actuals
5		No. of issues reported related to safety	Number	Track Actuals
6		No. of Non-compliance related to OHSE	Number	Track Actuals
1		No. of feedback reported by employee / customers / contractors / visitors	Number	Track Actuals
2		Comply with Legal / Statutory / Regulatory Compliance as per the target date (Finance / Admin / HR)	%	100%

5. LEADERSHIP

Leadership and Commitment

Top management of Neurealm has projected its leadership and commitment regarding BMS by direction of the organization

- Adequate integration of BMS requirements into the organization business processes.
- All the expectations / requirements are managed using Service Management plan / Software Development Plan throughout the life cycle of the BMS
- Every function head, CSM of the accounts has the authority to take decision on the BMS as defined in the process
- Ensuring every kind of resources availability for the BMS implementation

- Make decisions that consider OHS matter equal to cost, quality, morale and business operation.
- Communicating the importance of effective management and of conforming to the BMS requirements
- Ensuring that the BMS objectives, delivering value to customers are achieved and taking appropriate corrective action.
- Directing and supporting the persons to contribute to the effectiveness of BMS
- Promoting continual improvement
- Supporting other relevant management roles to demonstrate leadership as it applies to areas of their responsibility.
- Control of other parties, third parties involved in the BMS life cycle.
- Taking overall responsibility and accountability for the prevention of work-related injury and ill health as well as the provision of safe and healthy workplaces and activities
- Developing, leading and promoting a culture in the organization that supports the intended outcomes of the BMS
- Protecting workers from reprisals when reporting incidents, hazards, risks and opportunities
- Supporting the establishment and functioning of health and safety committees.

The Neurealm Leadership team reviews the performance of the internal group / support functions and each customer engagement either monthly or quarterly based on the status report or performance data made available in the CSM platform by the respective function / CSM of the customer engagement.

- Delivering value to customers
- Performance & Control of other parties involved in the BMS lifecycle
- Continual improvements
- Roles responsibilities as defined at the process document (std. practice) as well as RACI matrix where there is change or deviation from the defined std. practice / process
- Effect / Impact of BMS on account of any issue / change / risks in the any of other integrated processes



BMS Policy

Leadership team of Neurealm has established the BMS Policy and ensures that it

- a. Is appropriate to the purpose of the organization,
- b. Includes a commitment to meet customer requirements, eliminate hazards, prevention of pollution, injury, ill health, reduce risks and continual improvement in BMS management and performance,
- c. Provides a framework for establishing and reviewing business objectives,
- d. Is documented, implemented, maintained, communicated and understood within the organization
- e. Is communicated to all persons working under the control of and for the

- organization with the intent that they are made aware of their individual quality through Neurealm intranet platform
- f. Adherence to statutory, regulatory, legal, contractual requirements and other requirements which include but not limited to ISO 9001, 20000-1, 45001, 27001, HIPAA, GDPR, PCI-DSS and other standards
 - g. Is available to interested parties, and
 - h. Is reviewed periodically to ensure that it remains relevant and appropriate to the organization

Business Management System Policy of Neurealm

<div data-bbox="251 575 482 653"> <h3>Information Security Policy</h3> </div> <div data-bbox="251 659 730 711"> <p>The information Security Policy intends to protect information assets belonging to Neurealm, Information assets belonging to its clients that are entrusted to Neurealm and comply with information security requirements of interested parties</p> </div> <div data-bbox="267 743 513 768"> <p>The objective of the policy is to ensure</p> </div> <div data-bbox="258 785 686 1020"> <ul style="list-style-type: none"> • Protection of Confidentiality, Integrity, and Availability of the Information Assets • Business requirements for availability of information and systems are met • Intellectual property of Neurealm and that of its clients are protected • Comply with all regulative, legislative, statutory, and contractual requirements including: <ul style="list-style-type: none"> + HIPAA Security Rule, + State breach notification laws, + PCI Data Security Standard, • The information security program is reviewed no less than annually or upon significant changes to information security environment to ensure that they are continually improved </div> <div data-bbox="267 1050 362 1071"> <p>Enforcement</p> </div> <div data-bbox="258 1087 719 1182"> <ul style="list-style-type: none"> • Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties • Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties </div> <div data-bbox="258 1236 417 1272">  </div> <div data-bbox="636 1236 729 1272"> <p>Neeru Metha CPO</p> </div>	<div data-bbox="826 558 1261 638"> <h3>Service Management Policy</h3> </div> <div data-bbox="826 655 1448 695"> <p>The managed services provided to our customers are delivered with the commitment to fulfilling service requirements and against the following objectives</p> </div> <div data-bbox="834 726 1343 959"> <ul style="list-style-type: none"> • Provide the governance and framework to assure quality of service • Build relationships with customers • Develop a proactive strategy and roadmap with customers • Manage the costs for Service Delivery • Identify new business improvement opportunities for evaluation • Initiate service improvements to address issues relating to <ul style="list-style-type: none"> + Efficiency - Do it right the first time + Effectiveness - Meet customer requirements + Economy - Provide value for money </div> <div data-bbox="826 991 1464 1024"> <p><i>The IT Service Management Policy shall be reviewed and where necessary revised as a minimum during formal annual review to ensure that they are continually improved</i></p> </div> <div data-bbox="834 1247 1049 1283">  </div> <div data-bbox="1346 1247 1477 1283"> <p>Neeru Metha CPO</p> </div>
--	--

HIPAA Policy

Neurealm is committed to protect the personally identifiable information (PII) and Protected Health Information (PHI) of Individual in accordance with Privacy and Security Regulations established by Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the regulations disseminated there under. ISMS Policies and procedures shall be applied to safeguard the PII & PHI information created, stored, acquired, transmitted, or maintained by the designated functions of Neurealm and its affiliates.

All staff who work for Heath care projects shall go through the mandatory training programs within the timeline

Information Security & Privacy Risk Assessment shall be carried out as per the standard practice applicable for Risk Management

Quality Policy

Neurealm is committed to

- Achieving customer satisfaction consistently, by understanding the needs of the customer comprehensively and delivering on them efficiently
- Foster a culture of innovation and value creation to our customers through automation, process optimization and smart machines
- Comply and conform to all applicable parties' requirements, including legal and statutory, that affect our business operations
- Establish, implement, maintain and continually review our Quality Management System objectives at all relevant levels and functions with an aim to continual improvement
- Adopt, promote and implement a risk based approach in all our processes
- Apply and communicate the requirements of Quality Management System policy within the organization and to all relevant parties as appropriate and ensure they understand

The Quality Policy shall be reviewed and revised appropriately during the formal annual review to ensure continual improvements



Neeru Metha
CPO

Occupational Health, Safety and Environment (OHSE) Policy

Neurealm is committed to

- Prevent accidents, injuries and occupational ill health
- Maintain safe and healthy working conditions, provide and maintain facilities, equipment and machinery, and ensure safe storage/use of substances
- Comply with all applicable interested parties' requirements, including legal, regulations, international industry standard and statutory, that affect our business operations and occupational health and safety objectives
- Establish, implement, maintain and continually review our Occupational Health, Safety and Environment System objectives & targets at all relevant levels and functions for continual improvement
- Adopt, promote and implement a risk based approach in all processes to mitigate the impact of any foreseeable hazards
- Apply and communicate the requirements of OHSE policy within the organization and to all relevant interested parties as appropriate and ensure it is understood

We seek co-operation of all employees, customers, contractors, visitors and anyone else who may be affected by our operations

We encourage suggestions on our health and safety objectives to create a safe and healthy environment

The OHSE Policy shall be reviewed and where necessary revised appropriately during formal annual review to ensure continual improvement



Neeru Metha
CPO

Compliance Policy

Policy :- All staff involved in Health care projects are responsible to abide by Federal requirements. It is our responsibility to ensure that we do not contribute to fraud, waste and abuse. If we observe these practices, we have a responsibility to report them immediately to complianceofficer@neurealm.com

All staff who work for Healthcare projects shall go through the mandatory training programs within the timeline

Procedure :

- Staff shall participate in the mandatory training programs every year.
- Review OIG & GSA exclusion list for each provider and staff at the time joining Neurealm and annually. Review frequency shall be monthly where required
- Staff will sign a yearly conflict of interest statement (based on client request)

Change Management Policy

Policy :- The change management policy shall help to communicate the Leadership team's intent that changes to information and communication technology supported business services / processes will be managed and implemented in a way that shall minimize risk and impact to customer and other interested parties. All changes to IT systems shall be required to follow the established Change Management process. This requires that changes to IT systems / SMS / BMS be subject to a formal change management process that ensures or provides for a managed and orderly method by which such changes are requested, approved, communicated prior to implementation (if possible), and logged and tested.

- A current baseline configuration of the information system, service management system and its service components shall be developed, documented and maintained.
- A current inventory of the information system, service management system and its service components along with the ownership shall be developed, documented and maintained.
- The baseline configuration of the information system, service management system and its service components shall be updated as an integral part of the information system component installation.
- Changes to the information system, service management system and its service components shall be authorized, documented and controlled by the use of formal change control procedure.
- Changes in configuration of the information system, service management system and its service components shall be monitored through configuration verification and assessment processes.
- The information system, service management system and its service components shall be configured to provide only essential capabilities and shall prohibit and /or restrict the use of specific functions, ports, protocols, and/or services. A list of prohibited and/or restricted functions, port, protocols etc. shall be defined and listed.
- Automatic mechanism / tools shall be employed to maintain an up-to-date, complete, reliable, accurate and readily available configuration of the information system, service management system and its service components
- Automatic mechanisms / tools shall be employed to initiate changes / change requests, to notify the appropriate approval authority and to record the approval and implementation details.
- The information system, service management system and its service components shall be reviewed at defined frequency to identify and eliminate unnecessary functions, ports, protocols, and/or services.
- Categories of changes – Standard, Normal, Emergency and other type of change shall be managed as per change management process.
- Criteria to determine changes with potential to have a major impact on customers or services shall be managed as per the change management process.

Neurealm is committed to:

- achieving customer satisfaction consistently, by understanding the needs of the customer comprehensively and delivering on them efficiently
- foster a culture of innovation and value creation to our customers through automation, process optimization and smart machines
- protect the privacy of Individual health information in compliance with the HIPAA and the regulations disseminated there under

- comply and conform to all applicable parties' requirements, including legal, regulatory and statutory, that affect our business operations and occupational health and safety objectives
- establish, implement, maintain and continually review our business management system objectives & targets at all relevant levels and functions with an aim to continual improvement
- adopt, promote and implement a risk based approach in all our processes
- apply and communicate the requirements of business management system policy within the organization and to all relevant interested parties as appropriate and ensure they understood
- taken responsibility and accountability to prevent accidents, injuries and occupational ill health as well as the provision of safe and healthy workplaces and activities
- maintain safe and healthy working conditions, provide and maintain facilities, equipment and machinery, and ensure safe storage/use of substances

This policy has been approved by top management and shall be reviewed annually. This policy has the endorsement at the highest level and is actively practiced by Neurealm members at all levels. The annual mandatory trainings are also considered as an acknowledgement of having gone through the Neurealm Policies

The BMS policy is made available Neurealm Intranet site (<https://stagingmygavs.neurealm.com>)

Organizational Roles, Responsibilities and Authorities

The leadership team of Neurealm ensures that responsibilities and authorities are defined in the standard practice document and communicated within the organization by publishing its Neurealm Intranet site.

Such information is contained in the following documents

- a. Organization chart
- b. BMS Manual and
- c. Standard Practice document (documented procedures) and service management plan / software development plan.

Role	Responsibility, Authority and Accountability
CEO	<ul style="list-style-type: none">• Define and approve the BMS Policies, and• Ensure the communication and understanding of the BMS Policies throughout the organization.• Has the responsibility and authority for the development, resourcing, implementation, review and continuous improvement of the Neurealm BMS
Chief Finance Officer	<ul style="list-style-type: none">• Authorize to approve / accept the risk of not having a signed SoW• Approve financial transactions.• Accountable for ensuring compliance

Chief Delivery Officer	<ul style="list-style-type: none"> Review and approve the BMS Policies, and Has the responsibility and authority for the development, resourcing, implementation, review and continuous improvement of the Neurealm BMS Reporting to top management on the performance and opportunities for improvement to the BMS Chair regular reviews of the suitability and effectiveness of the Business Management System
Management Representative	<ul style="list-style-type: none"> Ensure that the BMS is established including interface with other processes, implemented, and maintained, Assigning authorities, responsibilities for ensuring that BMS processes are designed implemented and improved in accordance with the policy and objectives for BMS, Ensure that assets, including licenses, used to deliver services are managed per statutory and regulatory requirements and contractual obligations Ensure that activities are performed to identify, document and fulfill BMS requirements Reporting to top management on the performance and opportunities for improvement to the BMS Chair regular reviews of the suitability and effectiveness of the Business Management System
Quality Head	<ul style="list-style-type: none"> Maintain BMS (QMS,ISMS, SMS, PCI-DSS, HIPAA and OHS), incorporating suitable changes to standard practice, templates and forms and check-in into version control system and make it available in Intranet site Conduct Induction program and Training to employees on BMS. Work with client and Neurealm project team where necessary in defining or redefining the process based on the scope of the project. Manage Internal Assessments covering Planning, Scheduling and execution; consolidating Internal Assessment Metrics and Presentation in the Quality Council Meet; Approval of assessment plan, process tailoring, and deviation if any. Manage External audits including co-ordination on the following activities <ul style="list-style-type: none"> a) Scheduling surveillance / re-certification audit b) Co-ordinate with auditors c) Prepare Corrective and Preventive action report (CAPA) in case of NC if any raised d) Review CAPA Manage presentation & co-ordinate with prospects / customers on Process and Information Security practices Coordinate improvements to the Business Management System.
Data Privacy Officer (DPO)	<ul style="list-style-type: none"> Overall accountability for maintaining Data Privacy compliance at Neurealm ; Defining a charter for Data Privacy program and communicating to Neurealm executive management.

HIPAA – Privacy Officer	Overall accountability for maintaining HIPAA compliance at Neurealm ; Defining a charter for HIPAA Compliance program and communicating to Neurealm executive management.
PCI-DSS Officer	<ul style="list-style-type: none"> Overall accountability for maintaining PCI DSS compliance at Neurealm ; Defining a charter for PCI DSS program and communicating to Neurealm executive management.
Chief Information Security Officer (CISO) -	<ul style="list-style-type: none"> Overseeing organization's information, cyber, and technology security. developing, implementing, and enforcing security policies to protect confidential / critical data and maintaining Information Security Compliance Roles and Responsibilities of the CISO in detail is available in the attached document communicating to Neurealm executive management Detailed responsibilities are listed in the appointment letter of CISO and available in the Annexure - E
Service Organization Control (SOC)	<ul style="list-style-type: none"> Document and maintain the BMS Policies, Ensure that the BMS is established, implemented, and maintained, Investigate security breaches in accordance with security incident management procedures Chair regular reviews of the suitability and effectiveness of ISMS and Coordinate improvements to the ISMS
Information Security Council	<ul style="list-style-type: none"> Review ISMS policies and procedures on regular basis Review performance of security objectives set
Functional Heads	<ul style="list-style-type: none"> Ensure BMS is implemented, monitored and reviewed within their function Obtain and communicate customer requirements on information security to the appropriate personnel or functional organization, Ensure that qualified, skilled, and trained personnel and other resources are available to implement the BMS, Ensure confidentiality, integrity and availability on the products and services offered to customers, and Ensure that staff complies with applicable BMS policy, standards, regulations, specifications, and documented procedures. Be responsible for the implementation of local H & S protocols relevant to staff and within the group Ensure Neurealm OHS MS is implemented in their area of responsibility
Supervisors	<ul style="list-style-type: none"> a safe workplace and assign safe work training and information Implement the process and procedures as stated in the Neurealm Business Management System / Processes Obtain and communicate customer requirements on information security to the appropriate personnel or functional organization, Ensure that qualified, skilled, and trained personnel and other resources are

	<p>available to implement the BMS,</p> <ul style="list-style-type: none"> • Ensure confidentiality, integrity and availability on the products and services offered to customers, and • Ensure that staff complies with applicable BMS policy, standards, regulations, specifications, and documented procedures
Staff	<ul style="list-style-type: none"> • work safely and not take risks • report unsafe conditions • wear the right safety equipment for the job • ask their employers about concerns regarding health and safety • Complies with BMS policy, standards and procedures • Participate in initiative related to but not limited Quality, ISMS, SMS, HIPAA, PCI-DSS and OHS • Co-operate and participate in all the Emergency response exercises carried out at the location • Operate in conformance with the requirements of the BMS, and • All staff have the authority to • Report incidents or violations that is related to BMS to soc@neurealm.com , facility@neurealm.com respectively • Raise / report health and safety issues • Stop work where there is an immediate and serious threat to the health and safety. • Accountability • All staff are accountable to their supervisor through: • Regular one-to-one meetings • The performance of OHS MS Key performance targets • Job descriptions •
First Aid Team	<p>In an emergency, all first aiders should be able to</p> <ul style="list-style-type: none"> <input type="checkbox"/> Manage the incident and ensure the continuing safety of themselves, bystanders and the casualty <input type="checkbox"/> Assess any casualties and discover the nature & cause of their injuries or illnesses <input type="checkbox"/> Arrange for further medical help or other emergency services to attend. Usually by making an emergency phone call. <input type="checkbox"/> If trained, prioritize casualty treatment based upon medical need <input type="checkbox"/> Provide appropriate first aid treatment that they have been trained to do, and that is reasonable in the circumstances <input type="checkbox"/> If able, make notes and record observations of casualties, ideally monitoring Vital Signs, and SAMPLE information <input type="checkbox"/> Provide a handover when further medical help arrives <input type="checkbox"/> Fill out any paperwork as required following the incident
Emergency Response Team	<p>The First Person at site</p> <ul style="list-style-type: none"> • The first person at site will typically serve as the Incident Commander (IC), until relieved by a more senior person. Responsibilities for the first person on-scene may include: <ul style="list-style-type: none"> <input type="checkbox"/> Taking appropriate personal protective measures • Notifying Supervisory Personnel and/or Incident Commander of the incident

	<ul style="list-style-type: none"> • Advising personnel in the area of any potential threat and/or initiate evacuation procedures • Eliminate potential ignition sources <p>Supervisory Personnel responsibilities may include:</p> <ul style="list-style-type: none"> • Initiate initial response actions if they are the first person on the scene (see above) • Restrict access to the incident scene and surrounding area as the situation demands Take any other steps necessary to minimize any threat to health and safety • Request medical assistance, if necessary • Verify substance released and obtain Safety Data Sheets, as necessary • Identify and isolate source to minimize product loss • Coordinate further response actions with Incident Commander and local responders <p>Incident Commanders</p> <p>Incident Commander responsibilities may include:</p> <ul style="list-style-type: none"> • Activate the Emergency Response team • Activate additional response contractors and local resources • Evaluate the Severity, Potential Impact, Safety Concerns, and Response Requirements based on the initial information provided by the First Person On-Scene • Confirm safety aspects at site, including need for personal protective equipment, sources of ignition, and potential need for evacuation. • Communicate and provide incident briefings to company superiors, as appropriate • Coordinate/complete additional internal and external notifications • Communicate with Emergency Response Team, as the situation demands • Direct response and clean-up operations
HSE Committee	<ul style="list-style-type: none"> <input type="checkbox"/> Provide a forum for committee members to discuss HSE issues. <input type="checkbox"/> Develop plans or procedures to resolve the identified issues. <input type="checkbox"/> Proactive Hazard Identification, Evaluation & Risk Assessment & Control <input type="checkbox"/> Plan for Safety, Health and Environment that include and not limited to recommend and track new safety & health rules and work practices <input type="checkbox"/> Ensure HSE Committee is effective not limited to the following practices include workers /staff to participate and consult where required <input type="checkbox"/> Recommend corrective actions to reduce hazards. <input type="checkbox"/> Address any additional health and safety issues. <input type="checkbox"/> Evaluate HSE KPI / Metrics <input type="checkbox"/> Plan for the HSE committee meeting and review follow-up action items

Contractors / Visitors / Third party /	<ul style="list-style-type: none"> <input type="checkbox"/> Take reasonable care for their own health and safety <input type="checkbox"/> Take reasonable care that their acts or omissions do not adversely affect the health and safety of others <input type="checkbox"/> Comply with reasonable instruction given by Neurealm <input type="checkbox"/> Report hazards and incidents <input type="checkbox"/> Not interfere with any safety equipment or equipment provided for emergency use <input type="checkbox"/> Stop work if there is a risk to theirs of other health and safety <input type="checkbox"/> Complete training, comply with controls and follow Neurealm OHS safety practices <input type="checkbox"/> Authority to commence an emergency response and raise health & safety issues
Privacy Officer (HIPAA)	<ul style="list-style-type: none"> <input type="checkbox"/> Maintain ongoing communication with Security Official (SOC) and all Privacy coordinators (Project Manager or Team Lead or Team Member as appointed by Delivery manager) <input type="checkbox"/> Coordinate training programs for the designated covered functions in cooperation with Privacy Coordinators <input type="checkbox"/> Respond to complaints regarding Neurealm policies, procedures and practices related to the privacy of health information <input type="checkbox"/> Maintain all policies and procedures in written or electronic form
Compliance Officer	<ul style="list-style-type: none"> <input type="checkbox"/> Implementation, Monitoring, Tracking & Control of Compliance plan <input type="checkbox"/> Prioritize efforts towards compliance and communicate priorities <input type="checkbox"/> Developing training programs and ensuring execution of training courses <input type="checkbox"/> Guide team to understand HIPAA compliance and how any changes will affect their specific duties <input type="checkbox"/> Monitoring HHS and the state's regulatory requirements when new regulations or guidelines are introduced, the Officer must adjust the organization's HIPAA compliance program to reflect the changes
OHS Management Forum (part of Quality & Security Council)	<ul style="list-style-type: none"> <input type="checkbox"/> The quality council & security council team will continue to look after OHS matters not limited to the following <input type="checkbox"/> To ensure the availability of resources for implementing and maintaining OHS Management systems which is part of BMS <input type="checkbox"/> Review the OHS Policy, objectives & performance of KPI / targets <input type="checkbox"/> Provide strategic guidelines to the OHS initiative
OHS Officer	<ul style="list-style-type: none"> <input type="checkbox"/> ensure the availability of resources for establishing, implementing and maintaining OHS Management systems which is part of BMS <input type="checkbox"/> Maintain ongoing communication with OHS matters <input type="checkbox"/> Review the OHS Policy, objectives & performance of KPI / targets <input type="checkbox"/> Provide strategic guidelines to the OHS initiative <input type="checkbox"/> Ensure requirement of OHS and interested parties are compliant
OHS Executive Team (Chennai Leadership Team)	<ul style="list-style-type: none"> <input type="checkbox"/> To lead & facilitate implementation of Health, Safety and Environment management systems <input type="checkbox"/> Grievance related to Health & Safety and Environment are discussed and addressed
OHS Manager	<ul style="list-style-type: none"> <input type="checkbox"/> Organizing, implementing and monitoring various HSE systems <input type="checkbox"/> Facilitate communication about OHS systems to Leaders and Employees. <input type="checkbox"/> Undertake Incident study and root cause analysis for OHS related incidents and submit the findings to OHS forum. <input type="checkbox"/> All internal communication is handled

	<ul style="list-style-type: none"> <input type="checkbox"/> Awareness program related to OHS is discussed and organized <input type="checkbox"/> Ensure planning for OHS implementation <input type="checkbox"/> Undertake periodic Risk Assessment & Hazard Identification <input type="checkbox"/> Define control procedures and Implement the OHS Management programs <input type="checkbox"/> Communicate significant changes, updates and other information to internal / external parties <input type="checkbox"/> Consider feedback of internal / external parties on a periodic basis to involvement in OHS <input type="checkbox"/> Encourage employee participation in the safety committee meetings and communicating any issues related to Health & Safety <input type="checkbox"/> Review and support the Risk assessments activities <input type="checkbox"/> <u>Accountability</u> <input type="checkbox"/> Regular reporting of the OHS Management System (OHSMS) performance <input type="checkbox"/> Provision of OHS Statistics (e.g. Hazard and Incident reporting, training attendance <input type="checkbox"/> OHSMS assessment reports
Facilities Management	<ul style="list-style-type: none"> <input type="checkbox"/> Management of Hazardous materials associated with building or infrastructure in accordance with statutory requirements <input type="checkbox"/> To ensure the general working environment is compliant with OHS Regulations <input type="checkbox"/> Management of First Aid processes <input type="checkbox"/> Manage emergency systems and processes <input type="checkbox"/> Provide principal contractors information around hazards and risks at the work place <input type="checkbox"/> Ensure safe work method statements are prepared and made available to staff / workers <input type="checkbox"/> Ensure the permit-to-work process is in place and used for FM based activities requiring a permit <input type="checkbox"/> Monitor and review FM based contractors and consultants to ensure continued compliance <input type="checkbox"/> Facility Management is accountable for OHS issues to the OHS Manager and OHS Officer
Accountability	<ul style="list-style-type: none"> <input type="checkbox"/> Accountability for health and safety responsibilities is monitored through <ul style="list-style-type: none"> • The health and safety committees (Chennai Leadership Meet that takes place on Thursday of every week) • Quality & Security Council Meet • Quarterly Health and Safety Statistics reports • Corrective actions • Internal Assessments

Management Representative / appointee

Top management of Neurealm has appointed a member of the organization management who, irrespective of other responsibilities, is responsible and has authority in

- a) Ensuring that processes needed for the BMS are established, implemented and maintained in accordance with the ISO 9001, ISO 20000-1, ISO 45001, ISO 27001 standard and SEI-CMMi DEV & SVC model

- b) Reporting to top management on the performance of the BMS and any need for improvement, and
- c) Ensuring the promotion of awareness of customer and OHS requirements through the organization.

The identity of the top Management Representative is made available to all persons working under its control. The responsibility of the management representative includes liaison with external parties on matters related to the BMS.

OHS :- Consultation and participation of staff / employees through the standard practice applicable for HSE / Admin function. Leadership team shall ensure that

- involve employees / staff at various levels (CSM, PM, Project Lead / Team Lead) for consultation / participation in the safety committee and any issues / improvement related to OHS
- plan for a skip level meeting to understand concerns if any across employees / staff.
- Recognize and Rewards employees who contribute and participate in the BMS

CISO

The contact information for the CISO is as follows and subject to change

Mrs. [Kavitha Ayappan](#)

kavitha.ayappan@neurealm.com

Neurealm Private Ltd.,

Compliance Officer

Neurealm has designated a Compliance officer who is responsible for design, develop and manage a HIPAA compliance program as per the HIPAA requirements

Responsibility of the Compliance Officer include:

- Implementation, Monitoring, Tracking & Control of Compliance plan
- Prioritize efforts towards compliance and communicate priorities
- Developing training programs and ensuring execution of training courses
- Guide team to understand HIPAA compliance and how any changes will affect their specific duties
- Monitoring HHS and the state's regulatory requirements when new regulations or guidelines are introduced, the Officer must adjust the organization's HIPAA compliance program to reflect the changes.

- The contact information for the Compliance Officer is as follows and subject to change

Mr.Ambrish Sethi

ambrish.sethi@neurealm.com

Neurealm Private Ltd.,

OHS Officer

Neurealm has designated a OHS Officer who is responsible for the development and implementation of the Neurealm's policies and procedures related to the OHS as per OHSAS – ISO 45001 standard

Responsibilities of the OHS Officer include:

- Maintain ongoing communication with OHS matters
- To ensure the availability of resources for establishing, implementing and maintaining OHS Management systems which is part of BMS
- Review the OHS Policy, objectives & performance of KPI / targets
- Provide strategic guidelines to the OHS initiative
- Ensure requirement of OHS and interested parties are compliant

The contact information for the OHS Officer is as follows and subject to change

Mr.Aswin Narashimman



Aswin.Narashimman@neurealm.com

Neurealm Private Ltd.,

6. PLANNING

6.1 Actions to address risks and opportunities

While planning for the BMS, Neurealm has considered the issues referred to in 4.1 and 4.2, established standard practice for Risk Management to keep track of Risks / Opportunities using CSM platform (where not feasible will use Risks tracker) as a mechanism to identify the risk and opportunity that need to be addressed to

- a. Assure the BMS in place can achieve intended outcome

- b. Prevent, or reduce, undesired effects
- c. Achieve continual improvement of the BMS and the services
- d. Plan and prioritize actions to address risks and opportunities
- e. Plan evaluation of effectiveness
- f. Risks related to the organization, not meeting requirements, involvement of other parties
- g. Impact of risks and opportunities on customer
- h. Risk acceptance criteria
- i. Approach to be taken for the management of risks

Neurealm have established a tracker for tracking legal, statutory, regulatory and other third parties requirements pertaining to QMS, SMS, ISMS and OHSAS.

6.2 BMS Objectives and planning to achieve them

Every CSM function will follow through the processes applicable for the Service Delivery / Software development right from Project Kick-off to Project closure that is made available in Neurealm Policy Central (intranet platform) ensuring that the BMS objectives are met and improved. All the support functions that are contributing to the CSM function shall agree/communicate the operational level agreement (internal SLA) and targets on the services that have an impact on the services or service components delivered to customers.

Performance of BMS objectives would be reported by Quality function every quarter/month to the Quality Council team and if intervention is required then a meeting is scheduled with a specific account that needs intervention / guidance from the Leadership team. Outcome of these meetings shall be tracked using MoM in email format or through CSM platform. In the event of non-availability of an agreement / contract / SoW, the Chief Finance Officer has the authority to evaluate the risk and accept the risk or advise on the risk treatment plan.

The Neurealm Leadership team ensure that business objectives considering the BMS scope are established at relevant functions and levels within the organization using Balanced Score Card

framework. The business objectives are measurable, where practicable, and consistent with the BMS Policy, including the commitments to meet customer requirements, the prevention of pollution, injury and ill health, views of relevant interested parties, to compliance with applicable legal requirements, statutory requirements, regulatory requirements and with other requirements to which the organization subscribes and to continual improvement

Objectives	Target
Information Security Process Compliance	100%
Quality Management	90%
ITSM	90%
HIPAA Compliance	100%
OHSE Compliance	100%
PCI DSS Compliance	100%
CSAT Survey score	>=4 out of 5

For OHS

OHS Planning :- The below diagram represents the planning function pertaining to OHS



6.2.1 – Hazard Identification, risk assessment and determining controls

Identification of Hazard and Risk Assessment is performed for all routine & non-routine activities at Neurealm. Standard practice for Risk Assessment as stated in ISO 27001 standard is followed to evaluate the risk and risk rate are assigned to each hazard and acceptable risk is determined. Hazards which are related to OH&S legal requirements are considered as significant; Risks which are above acceptable risk rating are identified as Extreme risks, those are covered through BMS objectives to improve performance or controlled through operational control procedures, measuring & monitoring, training & awareness, emergency preparedness and response or combination thereof.

The extreme risks and aspects are reviewed quarterly by different departments to plan mitigation measures to minimize the impact by applying the following any of controls a) Elimination b) Substitution c) Engineering d) Administrative e) Personal Protective Equipment that is more effective.

Contingency preparedness and response planning

The various departments of Neurealm have developed standard practice (procedures) to ensure that the organization can respond to the accidents and foreseeable emergency and disaster situation and for preventing and mitigating the information security, quality, environmental and BS OHSAS impacts associated with them considering the total business risk on the organization.

After identifying the potential risks / environmental impacts or emergency situations and experience, action plans have been developed to overcome the emergency. In case of occurrence of such a situation an Emergency Support team is formed to analyse the risk and necessary corrective actions taken to prevent its recurrence.

Emergency Preparedness: -

In most instances the scope of the emergency plan will be limited to the emergencies listed below; however, depending upon the geographic location of the Site other types of catastrophes must be taken into consideration and emergency arrangements made proportionate to the identified risk

Consideration should be given to the following:

- ☐ Flooding
- ☐ Earthquakes Risk
- ☐ Lightning
- ☐ Wind
- ☐ War
- ☐ Emergency Health issue

Neurealm has established a business continuity plan at the org. level and service continuity plan at every account level which contains the possible risks and emergency response as a service continuity /business

continuity strategy

An emergency drill is conducted every year in which ERT (Emergency Response Team) will participate and ensure all the employees of the company participate in the drill. Also, set of employees are identified to undergo First Aid training to provide directions to employees/admin when there is an emergency health issues arise. (Giddiness, Increase in Blood pressure etc.,

For SMS

Plan the SMS

The contents of the service management plan shall consider the following but not limited to these following

1. List of services
2. Known limitations that can impact the SMS and the services
3. Obligations such as relevant policies, standards, legal, regulatory and contractual requirements
4. Human, Technical, Information and Financial resources necessary to operate the SMS and the services
5. Authorities and responsibilities
6. Approach to be taken for working with other parties involved in the service lifecycle.
7. Technology used to support the SMS
8. How the effectiveness of the SMS and the services will be measured, assessments, reported and improved
9. Internal / External Issues of interested parties / suppliers.
10. Scope of the SMS

The Neurealm Leadership team has established a focused group called Quality Council and Information Security Council to review every quarter on the compliance and performance of objectives set for Quality and Information Security, HIPAA, PCI-DSS and OHS.

Quality Council comprises Chief Operating Officer, Customer Success Managers, Quality Partners, and HR business partners.

Security Council comprises Chief Operating Officer, Head of IT Infrastructure, Head of Compliance Officer, Head of SOC, Head of Quality & Risk and Head of Global HR.

Performance of BMS Objectives is reported as part of the Quality Council reporting that goes from Quality function to the Quality Council team.

Compliance Management Programme(s)

Objectives and targets for the Compliance Programme are derived from HIPAA Policy and client requirements. The actual performance of targets for the compliance programme are reviewed quarterly for continual improvement and compliant to legal requirements of internal and external interested parties. The members who are responsible for the compliance program are part of the Security council that meets

quarterly to review the effectiveness of the implementation of the compliance management programme and recommended changes are tracked through process improvement proposal process.

Refer to HIPAA Manual for HIPAA Policies and Procedures

OHS Management Programme(s)

Objectives and targets for the OHS Programme are derived from OHS Policy, HIRA (Hazard Identification & Risk Assessment), requirements of internal / external parties and feedback of interested parties. OHS objectives and targets are consistent with OHS Policy and reflect our commitment to control / mitigate risks. The actual performance is analysed internally by the designated HSE leaders and where required RCA is done to ensure appropriate corrective action is implemented.

OHS Objectives and targets are defined, documents as applicable are reviewed quarterly for continual improvement and compliance to legal and other requirements of internal and external interested parties.

The OHS Programme is developed to achieve the set objectives and target for OHS. They address the delegation of responsibility to relevant functions of the organization, detailing appropriate resources and timeline to complete the task and for reviewing the programs.

The HSE forum meets quarterly to review the effectiveness of the implementation of the OHS Management system and performance against set targets. The forum can recommend suitable changes to the OHS management system and the objectives and targets after the review.

Neurealm formed an OHS Management Forum with a forum head as head of Quality Assurance for implementation and maintenance of the OHS Management system. The forum determines and ensures the availability of resources like competent personnel, proper working conditions and adequate infrastructure. OHS Management forum also provides timely resources to comply with legal requirements and other requirements.

Task level responsibility to manage, perform and verify OHS work is detailed in standard practice (process) applicable for relevant functions including for vendors and contract associates.

Composition of HSE Core Team : HSE Manager, Head – Admin, Head – HR, Head - QA

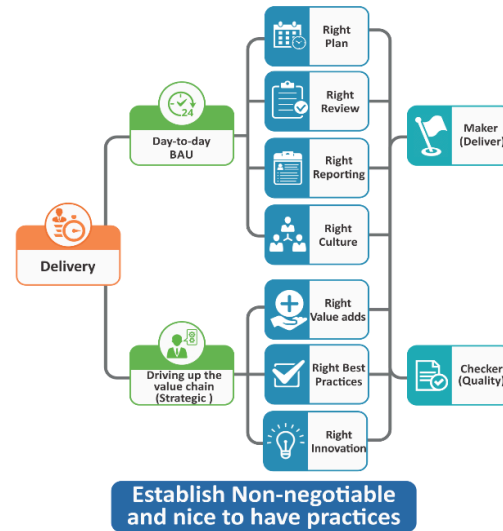
Right First Time framework

Neurealm Leadership team has established a Right First Time (RFT) framework across organization to emphasize on prevention approach to Quality and move away from detection approach to Quality. Any new project in Neurealm will be launched by holding a project kick-off meeting with Neurealm Leadership Team wherein RFT Launch check-list will be presented with the status of non-negotiable practices and nice-to-have practices. The diagram below depicts the RFT framework implemented at Neurealm.

Do it Right, the First Time, Every Time



RFT in Delivery



Early Warning Signal

An Early warning signal (EWS) system is established as part of Management Information System reporting such that Quality team will assess status and possibility of new risks and issues in all the projects executed in Chennai off-shore delivery centre and publish it as EWS as part of Delivery Health Dashboard Report to Neurealm Leadership team and Neurealm Delivery & Project Managers

Early Warning Signals - Account & Project Health Status as on DD-Month-Year				
Levels at Client	Sponsor			<ul style="list-style-type: none"> Yellow Star: AC-One - Proj-One Red Star: AC-Two - Proj-Two Orange Star: AC-Three - Proj-One
	BU	<ul style="list-style-type: none"> Yellow Star: AC-Four - Proj-Three Orange Star: AC-Five - Proj-Two 	<ul style="list-style-type: none"> Red Star: AC Four - Proj-Two 	
	PM	<ul style="list-style-type: none"> Green Star: AC-Four - Proj-One Orange Star: AC-Two - Proj-One 	<ul style="list-style-type: none"> Yellow Star: AC-Six - Proj-One 	<ul style="list-style-type: none"> Yellow Star: AC-Five - Proj-One
<div> <div>No Issue</div> <div>10 or 2 low Issues</div> <div>a) >= 1 High Issue</div> <div>b) > 2 Low Issue</div> </div> <div>on Quality, Client Satisfaction, Proactiveness</div>				
Priority				
<div>Low</div> <div>Medium</div> <div>High</div>				

Legend	
Red Star	Need Focus
Orange Star	Under Control
Yellow Star	Critical
Green Star	High
Blue Star	Medium
Light Blue Star	Low

The following accounts need attention from TAG team on the resource fulfillment:

- AC-One - Proj-Two

Reference to the ISO 9001:2015 - clause - 6.2 & 6.3

Plan the service management system

Service Management Plan (SMP) is established and maintained. The SMP shall consider the following

- a. service management policy
- b. service management objectives
- c. risks and opportunities
- d. service requirements and requirements of BMS
- e. list of services
- f. known limitations that can impact the BMS and the services
- g. obligations such as relevant policies, standards, legal, regulatory requirements
- h. human, technical, information and finance resources necessary to operate the BMS
- i. approach to be taken for working with other parties involved in the service
- j. technology used to support the SMS
- k. how effectiveness of the SMS and the services will be measured, assessed, reported and improved
- l. other planning activities shall maintain alignment with the service management plan

Planning of changes

Leadership team of Neurealm ensure that changes to BMS shall comply with standard practice applicable for change management

- a. The planning of BMS is carried out to meet the requirements given in 4.1 as well as the objectives, and
- b. The integrity of the BMS is maintained when changes to the BMS are planned and implemented using process improvement proposal tracker (PIP- Tracker)
- c. Organization and interested parties shall make decision on the approval and priority of requests for change
- d. Change management activities shall take the following into consideration during the decision-making:- risks, business benefits, feasibility and financial impact and potential impact of the change on
 - i. Existing services;
 - ii. Customers, users and other interested parties;
 - iii. Policies and plans required by the BMS
 - iv. Capacity, service availability, service continuity and information security
 - v. Other requests for change, releases and plans for the deployment

Legal and external requirements

Neurealm has established processes at every function level to identify and comply with legal and other requirements which are applicable. The objectives & targets are set in line with applicable legal and other requirements and compliance is ensured by the head of the function. Internal audit is carried out by Quality Assurance function as per internal Audit planner to assess the compliance.

7. SUPPORT

Resources

The leadership team reviews the resource requirements with each function including CSM function quarterly and as and when needed. Human resource related requirements are reviewed by the Leadership team with the Work force management function. All other resources requirements such as Office utilities / space, Infrastructure, Financial and Information systems are reviewed with concerned functions during their monthly / quarterly review. Weekly Resource Allocation & Availability Status meet and provide resources needed to

1. Implement and maintain the BMS and continually improve its effectiveness
2. Enhance customer satisfaction by meeting customer requirements, and
3. Protect the environment and the safety and health of persons under Neurealm's control.

Neurealm's personnel performing work affecting conformity to product and OHS requirements are competent based on appropriate education, training, skills and experience. The Neurealm Learning Academy would keep track of this information. The concerned function will be responsible for improve the competency and awareness and shall make a request to Neurealm Learning academy to arrange for required training.

Neurealm has determined, provided a suitable and conducive work environment as well as maintained the following infrastructure needed to achieve conformity to product and OHS requirements:

- A. Buildings, workspace and associated utilities,
- B. Process and OHS equipment (includes hardware, head phone), and
- C. Supporting services (such as transport, communication or information systems)

Organizational knowledge

At Neurealm, every function and project team determine the knowledge necessary for the operation / function of its processes to achieve conformity of products, OHS requirements, SMS requirements and services. The knowledge requirement is documented in Job description, Project Plan, Service Management Plan and as part of process where it is appropriate. The intellectual property, knowledge gained from experience, lessons learned during the project / operation, standards (including ISO, Coding standards, OHS etc.,) and Technology forum (Monthly event) are shared at various levels of employees appropriately towards achieving the organization objectives.

Neurealm has determined, provided and managed its finances needed to achieve conformity to product and OHS requirements.

Records from maintenance activities are maintained (see section 7.5.3)

Competence

Neurealm has established a function called Learning Management system to manage Awareness, Training & Competency development. Annual Training plan is established based on the business needs and published to employees. Certification on various topics at varying levels such as Level Zero / Level one is established and makes it mandatory to concerned employees to ensure that knowledge on the fundamentals are baselined.

Refer. Standard practice for Training which define the process for

- ❖ Determining the necessary competencies for personnel performing work affecting conformity to product and OHS requirements
- ❖ Providing training or taking other actions to achieve the necessary competence,
- ❖ Evaluating the effectiveness of the actions taken,

OHS

In case of OHS, required competencies are defined as part of the competency framework.

Awareness

Neurealm has established the processes for ensuring that its personnel are aware of

- ★ All the employees will participate in the induction program to get to know Neurealm Policies, practices across the functions.
- ★ As per training policy, employees will go through a mandatory training program through Neurealm Learning Management System (online portal) and complete the assessment. Following are the mandatory training programs a) Principles of Quality b) Awareness on HIPAA c) ISMS d) PCI-DSS e) Records of education, training, skills and experience are maintained by HR function

OHS related training is conducted by Administration function, HR, Learning Academy and Quality Assurance. Quality function covers the OHS Policy, objectives, Admin function brief OHS practices which includes pertinent risks in respective work areas and operational controls to be followed and potential consequences of deviating from specified operating procedures.

OHS officers ensure that any employee(s) performing activities are aware of the potential risk associated with Health, Safety and Environment and are competent on the basis of education and/or training or experience to control/ mitigate them.

Induction Training

All new employees & contractors are to be told about the following as a minimum.

- ★ Security access/ egress control
- ★ Policy on Compliance, Quality ISMS, HIPAA, PCI-DSS & OHSAS, GDPR and SMS
- ★ General hazard and risk associated with the site activities

- ★ Requirements for first aid and welfare and how statistics are collected
- ★ HSE legal requirements and those standards imposed by Neurealm site / location
- ★ Work related significant risks and/ or environmental impacts and their personal contributions to safe and environmentally improved site
- ★ OHS policy and general site rules
- ★ Emergency plans and procedures
- ★ Disciplinary procedures

Communication

Neurealm Leadership team ensures that an appropriate communication plan is established within the organization and outside (external) to organization through email and in person as per the business needs. Neurealm has established a Leadership team and Customer Success Managers, Function Heads / Business Units Head who manages the internal & external communication in various channels as appropriate. In case of ISMS, expected requirements from CIA (Confidentiality, Integrity, Availability) is established through

Non-Disclosure agreement, Contract / SoW and Service / Deliverables. Status / Progress on the ISMS related services are communicated through Status / Progress reports through email.

All employees, including suppliers are encouraged to give their feedback on the effectiveness of the BMS through the suggestion feedback form. Participation of employees and Interested parties is be ensured through various programs including but not limited to the Behaviour Based Safety and Health program, OHS related events,

Incident reporting procedure.

OHS core team initiate Hazard Hunt event at least once in a year in which employees from various functions will participate to achieve the following

- Identify hazards exists in various work places and non-work places,
- assess the risk associated with hazard and determine the risk rating (Probability X Consequence)
- Quality Team announce the winner, runner-up and participants
- QA SPOC consolidate all the hazards and submit to OHS Manager for further review
- OHS Manager shall review and design appropriate controls to prevent or reduce the probability of hazard
- OHS Manager plan for appropriate improvement plan

The result of the Hazard Hunt event is reported to OHS Management forum along with action plan

All department managers are required to report all nonconformities, including potential nonconformities to the Management Representative - Refer to Standard practice for Corrective Action with regard to its OHS risks, Neurealm has established, implemented and maintained the OHS Communication, Participation & Consultation Process which specifies the following:

- a. Internal communication among the various levels and functions of the organization
- b. Communication with contractors and other visitors to the workplace
- c. Receiving, documenting and responding to relevant communications from external interested parties,

- d. The participation of employees by their appropriate involvement in OHS risk identification, risk assessments and determination of controls, appropriate involvement in incident investigation, involvement in the development and review of OHS policies and objectives, consultation where there are any changes that affect their OHS and representation on OHS matters,
- e. That workers are informed about their participation arrangements, including who is their representatives(s) on OHS matters, and
- f. Consultation with contractors where there are changes that affect their OHS
- g. Risks addressed will not be communicated to external community unless it is agreed with interested parties,
- h. Track of all relevant incoming and outgoing communication records on interested party concerns
- i. would be maintained under OHS Communication (Internal & External) folder in corporate repository

Communication with contractors on the OHS requirements are established and maintained through contracts / agreement and work permit.

Neurealm has ensured that, when appropriate, relevant external interested parties are consulted about pertinent OHS matters.

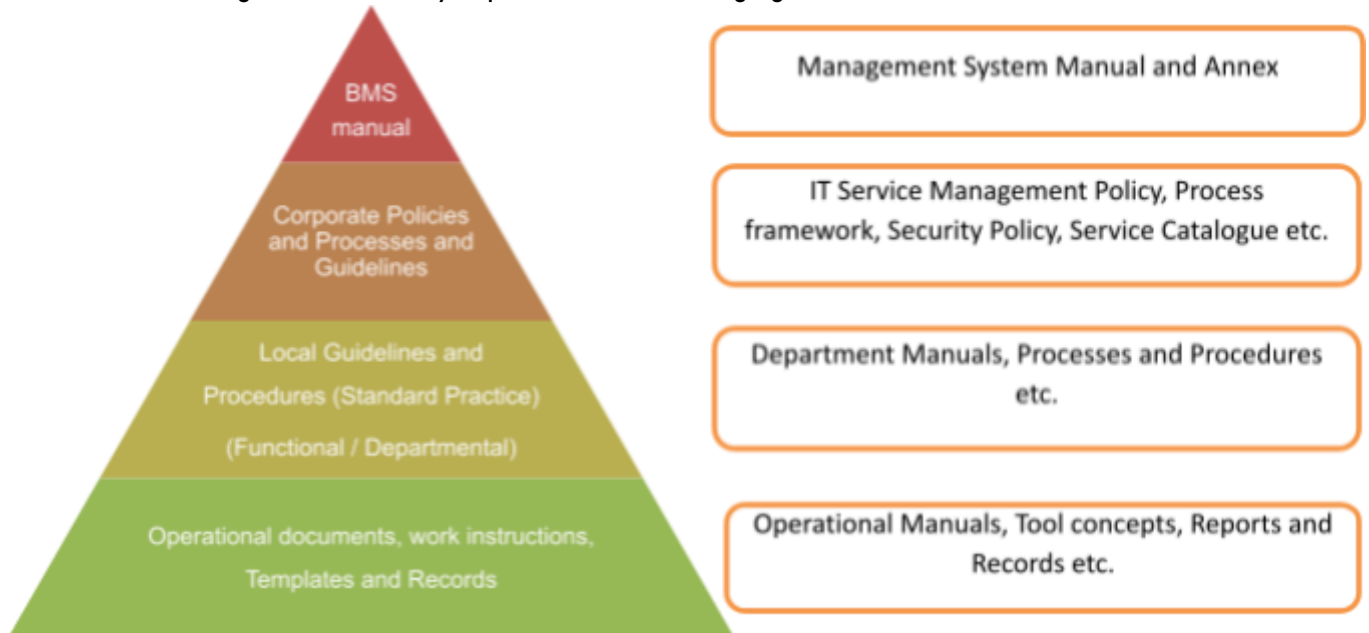
Records of these communications are maintained (see section 7.5)

Documented Information

Information required to be controlled and maintained and the medium on which it is contained is defined at the process / standard practice level and service management plan / software development plan. The documented information shall include the information created / stored / viewed / maintained in the CSM platform and other forms such word document / power point / excel file formats. The access to the documented information is controlled by the role of the employee in the function / project. The lowest level will have either no access or view access based on the need to know basis. Supervisor may have privilege to delete information in the CSM platform, however, the CSM platform will only mark the information as deleted and the data would be retained at the system level then archived as per document retention policy.

General:

Neurealm BMS is organised in the way depicted in the following figure.



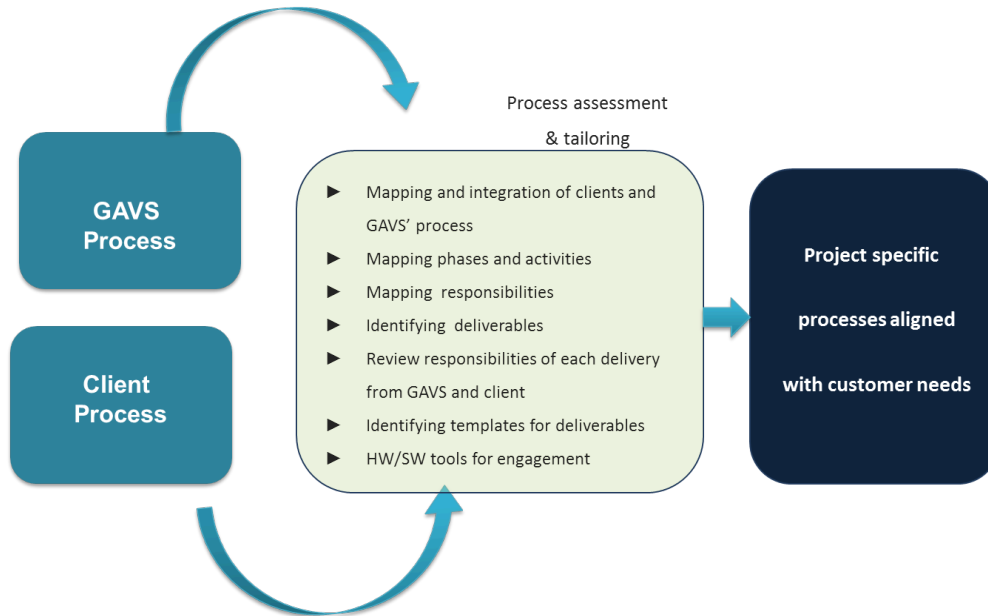
Neurealm's BMS documentation includes the following:

- BMS Policy
- BMS Objectives
- BMS Manual
- Standard Practice (documented procedures)
- Guidelines, Templates, Check-list, and
- Documents, including records, determined by Neurealm are necessary to ensure the effective planning, operation and control of its processes.

The Management system practiced in Neurealm is documented in the form of this Business Management System Manual. Supporting documentation is available in Standard Practice Document, Policies, Formats, Guidelines and Check-list.

The documented statement of Business Management policy is issued by the CEO, and objectives and targets are issued by department heads. The BMS manual is approved by Quality Head and standard practices are approved by concerned process owners.

Neurealm BMS has the flexibility of configuring client stated processes as part of Neurealm default standard processes in every project engagement



Business Management System Manual

Neurealm has established the Business Management System Manual that includes

- The scope of the BMS, including details of and justification for any exclusions,
- Reference to the documented procedures established for the BMS, and
- A description of the interaction between processes of the BMS

Creating and Updating documented information

Neurealm has established necessary processes (refer standard practice for Organization Process Definition and Change management) that includes

- Identification and description (e.g. a title, date, author, version number and release date)
- Format and media; and
- Review and approval for suitability and adequacy

Control of documented information

Documents required by the BMS are controlled and specified in the standard practices applicable for the respective processes.

Standard practice for change management and configuration management has been established to define the controls needed

- To approve documents to adequacy prior to issue,
- To review and update as necessary and re-approve documents,
- To ensure that changes and the current revision status of documents are identified,

- d. To ensure that relevant versions of applicable documents are available at points of use,
- e. To ensure that documents remain legible and readily identifiable,
- f. To ensure that documents of external origin determined by the organization to be necessary for the planning and operation of the BMS are identified and their distribution controlled and
- g. To prevent the unintended use of obsolete documents, and to apply suitable identification to them if they are retained for any purpose.
- h. To ensure that documents that not required are archived in a suitable manner

8. OPERATION

Quality Management System

Operational Planning and Control

Neurealm has planned; implemented and controlled those processes need to meet client requirements and has mechanisms in place to implement the actions determined in 6.1, by establishing

- a. Criteria for those processes
- b. Implementing the control of these processes in accordance with criteria
- c. Keeping documented information to the extent necessary to have confidence that the processes have been carried out as planned.
- d. In case of ISMS/GDPR implementation, the project plan will cover the life cycle of the service delivery or product delivery from a ISMS/GDPR point of view also.
- e. Verification and Validation processes are planned & executed as mentioned in the standard practice of software development, maintenance and service delivery management.

Neurealm have planned processes -Standard Practice for Software Development & Service Delivery Management related to service realization and applicable support services taking the following points into consideration:

- ☐ Information regarding characteristics of service
- ☐ Availability of required process for every services offered to client and business support functions
- ☐ Use of suitable equipment's
- ☐ Provisioning and Implementation of necessary monitoring and measuring instruments
- ☐ The implementation of release, delivery and post-delivery where applicable
- ☐ OHS aspects
- ☐ Service Level Agreements (SLA) and Non-Disclosure Agreements (NDA)

Service Portfolio :-

Service portfolio is used to manage the entire life cycle of all services including proposed services, those in development live services defined in the service catalogue(s) and services that are to be removed. The management of the service portfolio ensures that the service provider has the right mix of services. Service portfolio activities include planning the services, control of parties involved in the service lifecycle, service catalogue management, asset management and configuration management.

Solution & Strategy (S&S) function manages the service portfolio based on the inputs received from the function Marketing Sales & Strategy. S&S function has established a standard practice for service portfolio for managing the life cycle of service portfolio right from planning to removing the service. All the Service catalogue(s) are managed and maintained in a central corporate repository.

Service delivery :-

Service delivery is about operating the SMS and ensuring coordination of the activities and resources as well as performing the activities to deliver the services. CSM function deliver the services as per the processes applicable for Service Delivery – right from project kick-off to project closure as defined in the Neurealm Intranet site (<https://stagingmygavs.neurealm.com/>)

Service catalogue management :-

Service catalogue management requires the creation and maintenance of one or more service catalogs which are documented as Master Service Catalogue and managed by Solutions & Strategy function. The S&S function communicates the Service catalogue including new services to CSM functions, Sales team, Marketing team, Leadership team, Customers, and other interested functions.

Control of parties involved in the service life cycle :-

Neurealm is accountable regardless of which function or party is involved in the service life cycle. CSM functional will select and evaluate supplier / third parties as per the selection criteria defined at the Supplier Management process. Other parties include external supplier, internal supplier, customer acting as a supplier. The CSM function selects the supplier / other parties as per the customer requirements / service requirements and selects the supplier after the evaluation and application of selection criteria. CSM functional shall measure the performance and evaluate the process performance and effectiveness of services and service components of supplier / other parties.

Customer-related processes

Neurealm established a system of capturing client requirements right from the first interaction with client and followed a practice of documenting business requirements / functional requirements / system requirements in a standard document format that will be reviewed by Neurealm Internal team prior to committing the requirements to client.

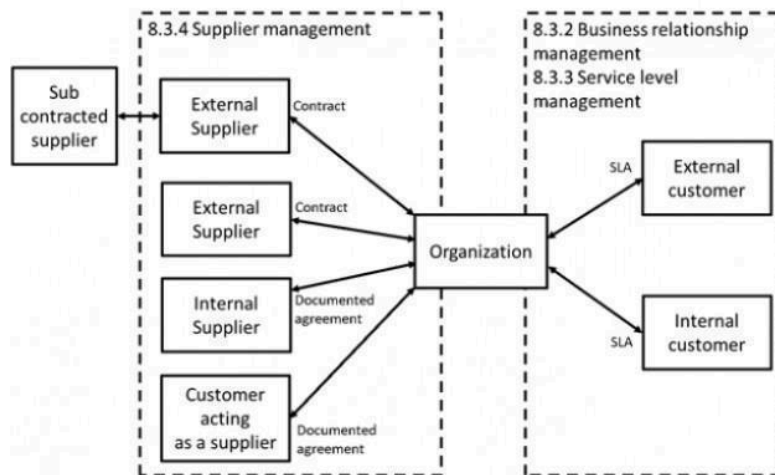
Based on the chosen software development life cycle model, the requirements are managed using appropriate tools. For example: Requirements are managed in the form of Product Backlog where a project has chosen an agile scrum life cycle model.

Relationship and agreement

Neurealm shall use suppliers to

- provide or operate services
- provide or operate service components
- operate processes, or parts of processes, that are in the organization's BMS

The following diagram illustrates the usage, agreements and relationships between business relationship management, service level management and supplier management.



Business relationship management

BRM is concerned with customer(s), a designated role called Customer Success Manager and Account manager responsible for managing the customer relationships and maintaining customer satisfaction. BRM is forward looking and strategic. The customers, users and other interested parties of the services identified are documented and managed through service management plan that include communication plan. The designated account manager connects with customers regularly once in a quarter if not lesser than a quarter to understand the current and future needs of customers. Customer Success survey is managed as a program and survey is initiated as an email with a URL for the customer to submit the feedback using the CSM platform. Quality function is responsible for initiating the survey every quarter and the concerned customer success manager is responsible for taking suitable corrective action including improvement plan and reporting the status of improvement as part of the status report submitted to customer.

The process addresses:

- 8.1. Identify business stakeholders, Service Requirements
- 8.2. Develop business relationship
- 8.3. Engage Leaders and provide strategic Consulting services
- 8.4. Align services to business objectives
- 8.5. Define communication model
- 8.6. Perform Quarterly Customer Success Survey
- 8.7. Handle Customer Complaints
- 8.8. Monitor Customer Complaints and share Corrective actions
- 8.9. Communicate IT Service Delivery Performance

The communication management processes include the activities of identifying processes, SLAs applicable for interested parties. The interested parties are Vendors/Suppliers, Client, internal support function within Neurealm. The performances of the interested parties are reviewed periodically per the planned and agreed frequency.

The communication, escalation methodology and levels, frequency of reporting and reviews will be documented in the communication management plan.

Service Level Management :-

The service and service level targets, volume of work – volume of transactions / tickets / no. of users supported are documented as part of the proposal / statement of work (SoW). The proposal / SoW shall contain when the SLA will not be applicable such as during the warranty period of a new service or during service continuity. The performance against SLA is measured and reported to customers monthly.

Supplier Management**8.12.1 Management of external suppliers**

Neurealm ensures that one or more designated individuals are responsible for managing the relationship, contracts and performance of external suppliers. For each external supplier, there shall be a documented contract. All the process related to supplier management shall follow the standard practice for supplier management

The Supplier Management process aims to establish a service strategy for the supplier with whom the Neurealm has a contractual relationship in providing IT services to the customer. The strategy is defined; supplier SLA is aligned and performance measures are tracked based on the services provided by the supplier. The contract is periodically reviewed, and if necessary, amended based on the supplier's performance against established SLAs. Continuous monitoring and reviewing of contract ensures that the best possible levels of service quality and availability are maintained. Following reports are typically used in this process

- Performance Statistics Reports: detailing the SLA/OLA is prepared, and the level of compliance with them, average costs associated with the process, etc.
- Progress Reports: describing the monitoring activities carried out, their results and the level of customers' satisfaction with the service provided.
- Improvement Plans: specifying the actions proposed to improve the IT service and the Impact of these actions on quality of service.

8.12.2 Management of internal suppliers and customers acting as a supplier

For each internal supplier or customer acting as a supplier, service level targets, other commitments, activities and interfaces between the parties are defined in the standard practice (process document) applicable for the respective internal supplier (support functions & business support functions)

All the process related to supplier management shall follow the standard practice for supplier management

Supply and demand**Budgeting and accounting**

Budgeting, accounting and costing for services or group of services are managed by the respective customer success manager (CSM). A designated person from the finance function shall enable the CSM to access the required information to have effective control over the financial and decision-making for

services. CSM shall present / report to the respective BU Head on the financial performance in terms of budget, cost and variance once in a quarter and proposed action plan and track it to closure.

Demand management

Current demand and forecast future demand for services are determined at the start of the project and performance in terms of demand and consumption of services are monitored and reported every quarter. Capacity management process taken into consideration while managing the demand. Standard practice for Demand management shall be followed.

Capacity management

Capacity requirements for human, technical, information and financial resources are reviewed by the respective BU head with the concerned / designated manager and CSM of the function. The capacity plan shall include the following

- a) Current and forecast capacity based on demand for services;
- b) Expected impact on capacity of agreed service level targets, requirements for service availability and service continuity.
- c) Timeline and thresholds for changes to service capacity

The concerned BU Head shall provide sufficient capacity to meet agreed capacity and performance requirements. Internal supplier and concerned functions shall monitor capacity usage, analyze capacity and performance data and identify opportunities to improve performance. Standard practice for capacity management shall be followed.

Design and development

Neurealm established a system that required processes for software engineering practices to control the design and development of the product. The system shall ensure that during planning and design of the development stage determines the review and verification that are appropriate. Verification and Validation of requirements take place based on the software development life cycle model chosen.

A system is established to ensure that whenever any change is requested either in the already proven software or the software under development, the change impact is identified, reviewed and approved before undertaking any change. The records of review results, of change requests/analysis and the necessary actions taken shall be maintained

Purchasing

A system is established to evaluate and select suppliers based on their ability to supply product in accordance with the Neurealm requirements. Criteria for selection are established through a form called schedule of material wherein product/vendor for which need for registration/evaluation shall be mentioned. Records of the results of evaluations and any necessary actions arising from the evaluation are maintained.

Scope of the purchase is limited to products / materials that are required to produce the product either directly or indirectly. Purchase of real assets like Car, furniture etc., shall not be part of the scope of the purchase. All purchases will go through a review and approval process. Prior to accepting any of the

material, Neurealm carry out verification as per defined acceptance criteria.

Production and service provision

Neurealm established required processes to identify the status of the product, a project management tool that is used for the product will depict the status throughout the product realization life cycle. A system of tracking client requirements to design, code and Test cases has been established and records for the same are maintained.

Neurealm exercises care with customer property while it is under Neurealm's control or being used by Neurealm. A System is established to identify, verify, protect and safeguard customer property provided for use or incorporation into the product. If any customer property is lost, damaged or otherwise found to be unsuitable for use, this shall be reported to the customer and records maintained.

A system is established to preserve the conformity of product/constituent parts of a product during internal processing and delivery to the intended destination to maintain conformity to requirements. During the work-in-progress stage, all the work products that are check-in to version control tool) are backed on a daily basis.

Once the project is completed/closed, all the work products of the project are archived.

Control of monitoring and measuring equipment

The work products that are in maintained in the corporate server which is in the server location, the temperature of the server location is ensured that it is kept in the acceptable range which will not affect the CPU performance by any means

Operational planning and control

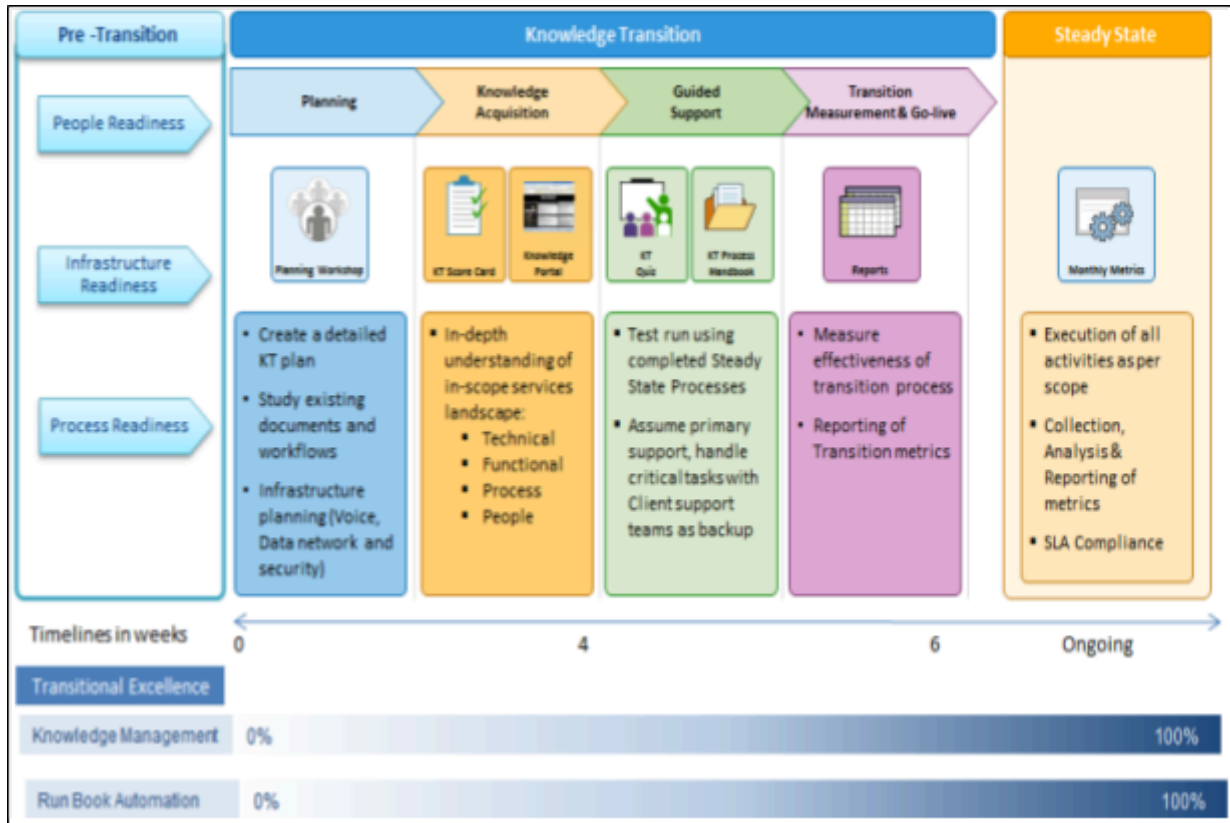
SMS is planned, implemented and controlled through service management plan (SMP). The SMP shall have performance criteria for the processes based on requirements and control process in accordance with the established performance criteria. The planned changes to SMS are controlled and consequences of unintended changes, action to mitigate any adverse effects are taken. Outsourced process also controlled.

Service Design, Build and Transition of new or changed services approach

The overall transition process is managed in line with the standard practice for Project / Transition Management. The key milestones in Neurealm transition model are:

- Pre-transition
- Planning
- Knowledge acquisition
- Guided support
- Transition measurement/ review & go-live

Reference :- Standard Practice for Service Design, Change Evaluation, Architecture, Project (Transition & Planning Support) management.



Change management

Change management is in 3 subclauses:

- Policy
- Initiation
- Activities

A change can be something new, a removal of a service (decommission, retirement), transfer of an existing service into or out of the organization, or something to be changed. A change introduced into SMS is managed through the Change Management process.

The main activities involved in **Change Management** will be

- Monitoring and directing the change process.
- Recording, evaluating and accepting or rejecting the **RFCs** received.
- Convene meetings of the **CAB**, except in the case of minor changes, for approval of **RFCs** and the drawing up of an **FSC (Future schedule of change)**.
- Coordinating the development and implementation and test of the change.
- Evaluating the results of the change and proceeding to close the change if successful
- In case of OHS, new products, services and processes, or changes to existing products, services and processes including work place locations and surroundings, work organization, working

conditions, equipment's, work force, changes to legal requirements and other requirements, changes in knowledge or information about hazards and OH&S risk, development in knowledge and technology

The goal of the change management process is to identify impactable items and intercept them before customers are impacted by them. Change Management processes are judged successful when changes are introduced into production operations without impact to business or their customers. In the case of OHS Management System, the risks associated with changes and hazards will be identified and assessed for further risk treatment.

Following are some of the metrics and reports used to evaluate the performance of the change management process.

- **RFCs** raised.
- Percentage of **RFCs** accepted and approved.
- Number of changes made, classified by impact and priority, and filtered by period.
- Average time taken for changes, as a function of impact and priority
- Number of emergency changes made.
- Percentage of changes that were successful at first attempt, second attempt, etc.
- Number of back-outs, with detailed explanations.
- Post-implementation evaluations.
- Percentages of changes closed without subsequent incidents.
- Incidents associated with changes made.
- Number of meetings of **CAB** with accompanying statistical information: number of attendees, length of meeting, number of changes approved per meeting, etc.

Release and deployment management

Release Management addresses large-scale changes to the environment such as installing a new database management system or managing widespread changes to a business application and it is closely integrated with the Change Management process. Thus, Release Management is concerned with managing many changes that will be introduced simultaneously into the production operating environment. Release and deployment process shall comply with standard practice for Release and deployment management.

Following are some of the metrics and reports are used to evaluate the performance of release and deployment management process:

- 1) Number of new versions launched
- 2) Number of back-outs, with reasons for them
- 3) Incidents associated with new releases
- 4) Compliance with deadlines set for each deployment
- 5) Allocation of resources in each case
- 6) Correctness and scope of the **CMDB**
- 7) Existence of illegal software versions
- 8) Proper recording of new releases in the **CMDB**
- 9) Incidents caused by incorrect use of the new release by users (due to inadequate training)

Availability of service during and after the release process

Service Delivery Process

Neurealm Service Delivery processes involve tailoring services to meet the client's specific business needs. It defines how to measure service outcome with meaningful metrics and using these metrics to drive continuous service improvement.

Service Assurance – (Refer – Standard Practice for Service Assurance)

Service Availability Management

Risks to service availability shall be assessed and documented as per agreed interval. Service availability requirements and targets shall be determined and documented as per the standard practice for Availability Management.

Service Continuity Management

Risks to service continuity shall be tested once in a year or after a major change to the service environment. Service continuity plan and test results are documented. SC Plan is updated if the test result warrants changes to SC plan. Service Continuity Plan and test report are prepared as per the Neurealm standard format.

Resolution and fulfillment

Incident and Service request management

The incident management process is about getting the service back up and running again as quickly as possible, not necessarily fixing the underlying cause unless there is no other way to bring back the service. An Incident can be an event that has not yet impacted the customer.

Management of an incident :- sequential activities of incidents *identification, logging, categorization, prioritization, initial diagnosis, escalation, investigation, resolution and recovery, closure*. The prioritization will be based on the impact/Severity/urgency on the operations/services. These incidents will be resolved quickly based on the agreed service levels and priorities to return to normal operation and minimize the impact on the business. Criteria to identify a major incident and non-major incidents are documented in the incident management process.

Service requests shall be recorded, classified, prioritized, fulfilled and closed. Records of service requests shall be updated with action taken.

Incident and Service requests shall be managed as per the standard practice for Incident & Service request management

Following metrics and reports are used to evaluate the performance of Incident Management process.

- **Service Level Management:** it is essential that customers have timely information about the level of compliance with SLAs and that corrective measures are taken in the event of non-compliance.
- **Monitoring the performance of the Service Desk:** determining the degree of satisfaction of the customer from the service delivered and supervising proper functioning of the first line of support and customer care.

- **Escalation Process Adherence:** managers need to know if the escalation process has followed the established protocols faithfully and if duplication has been avoided in the management process.
- **Identifying mistakes:** it may happen that the specified protocols are not right for the organization's structure or the customer's needs, meaning that corrective measures need to be taken.
- **Availability of Statistical Information:** which may be used to make future projections about the assignment of resources, additional costs associated with the service, etc.,
- **A knowledge base (KB)** allowing new incidents to be compared with logged and resolved incidents. An up-to-date (KB) allows unnecessary escalation to be avoided.

Problem Management

Problem Management process includes steps to detect, log, categorize, prioritize, investigate and diagnose, implement workarounds, document known errors, resolve and close problems. Problem Management process shall follow as per the standard practice applicable for Problem management. Some of the following metrics and reports are used to evaluate the effectiveness of problem management process

- **Reports on the Performance of Problem Management:** these should list the number of errors resolved, the effectiveness of the proposed solutions, response times and the impact on Incident Management.
- **Proactive Management Reports:** specifying the actions taken to prevent new problems and the results of the analysis performed on the suitability of the IT structures for the needs of the company.
- **Product and Service Quality Reports:** evaluating the impact on the quality of service of the products and services contracted. These may potentially enable informed decisions to be made on changes of suppliers, etc.

Control Process

Control of parties involved in the service lifecycle

The need for services from other parties such as internal suppliers, external suppliers or customers acting as a supplier are determined and evaluation criteria are applied in the service lifecycle. Other parties shall not provide or operate all services, service components or processes within the scope of the SMS. Control of parties involved in the service lifecycle are managed through service management plans.

Configuration Management

Configuration Management process includes establishing Configuration Management Plan by identifying the CI, level of control, owner, reviewers, baseline criteria, release criteria. An exhaustive CMDB will be developed and established.

The process helps in establishing a reliable repository of accurate information regarding IT components and understanding relationships between CIs, components and their impact on services. This process is closely integrated with the change management process.

In particular, the documentation generated include:

- ★ Scope and level of detail of the CMDB.
- ★ Deviations between the information stored in the CMDB and that obtained from the configuration assessments.
- ★ Information on CIs that have been involved in incidents.
- ★ Costs associated with the process.
- ★ Classification systems and naming conventions used.
- ★ Reports on un-authorized and/or unlicensed configurations.
- ★ Quality of the recording and classification process.
- ★ Statistical information and composition of the IT structure

Service Catalogue Management

Service catalogue is prepared and maintained by the solutions and strategy function. The service catalogue(s) shall include information for the organization, customers, users and other interested parties to describe services, their intended outcomes and dependencies between services. Service catalogue(s) / information about the services are made available through Neurealm Website and details are made available to the respective functions on a need basis. Standard practice for service catalogue management shall be followed.

Asset Management

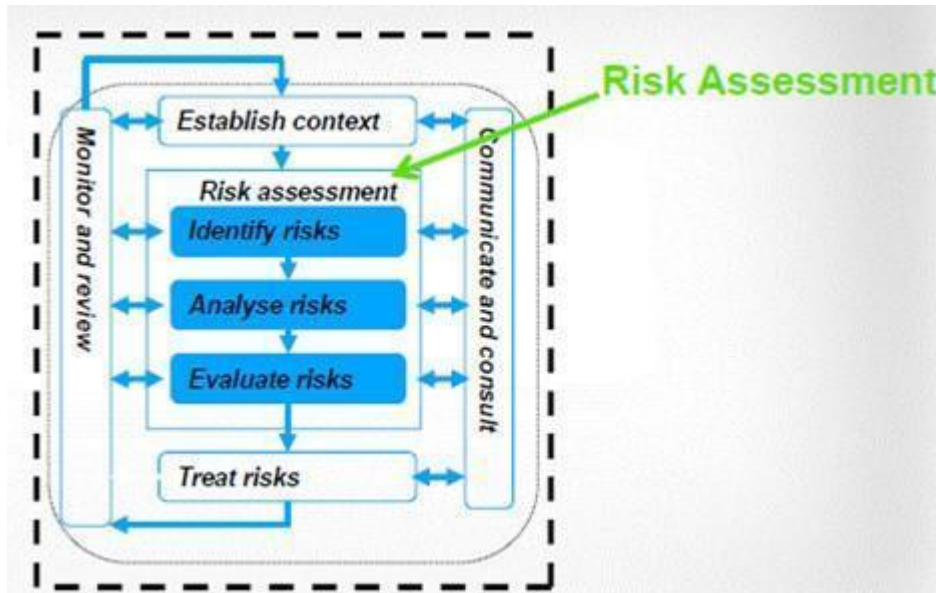
Assets are determined and managed throughout the SMS to deliver services and meet the service requirements and obligations. Standard practice for Asset management shall be followed.

Information Security Management System

Neurealm have established a comprehensive system for Information Security Management System as per ISO 27001 standard and developed Policies and standard practices to ensure the security of the information and information processing facilities are meeting requirements of client, stakeholders and interested parties. The policies and standard practices are reviewed at defined intervals. The Risks are managed as per the standard practice for Risk Management.

All the security requirements are identified at the start of a project / service and documented as part of project management plan / service management plan. All these security requirements are monitored throughout the duration of the project and compliance status are assessed periodically. Neurealm has mechanisms in place to control planned changes and unintended changes by acting to mitigate any adverse effect as necessary. Neurealm has ensured that it manages changes and its operation to ensure

that any new risk introduced are controlled Information security incidents shall be managed as per the incident management standard practice.



9. PERFORMANCE EVALUATION

Monitoring, Measurement, analysis and evaluation

Monitoring and measurement of Process

Neurealm Leadership team regularly monitor the performance of BMS objectives set using Balanced Score Card framework (Refer 6.1.4 and standard practice for Organization Process Performance). BMS objectives and targets that are reviewed during the Management review meeting which is part of security council meet / quality council. In addition, all the OHS activities are monitored by the respective function and assessed by Quality Assurance at every quarter.

The standard practice provides:

- Both qualitative and quantitative measures, appropriate to the needs of the organization,
- Monitoring of the extent to which the BMS objectives are met
- Monitoring the effectiveness of BMS processes and their controls
- Proactive measures of performance that monitor conformance with the BMS programmes, controls and operational criteria,
- Reactive measures of performance that monitor customer complaints and satisfaction levels, environmental impacts, ill health, incidents (including accidents, near-misses etc.,) and other historical evidence of deficient BMS performance

- f. Recording of data and results of monitoring and measurement sufficient to facilitate subsequent corrective action analysis

These measures demonstrate the ability of the processes to achieve planned results. When planned results are not achieved, correction and corrective actions are taken, as appropriate. The output of this requirement is documented as MoM in email format or in the CSM Platform under the MoM / Action item section..

Monitoring and measurement of product

Neurealm monitors and measures the characteristics of the product to verify the product requirements have been met. . This is carried out at an appropriate stage of the product life cycle process in accordance with the planned arrangements

Evidence of conformity with the acceptance criteria is maintained to indicate the person(s) authorizing release of product for delivery to the customer

The release of product and delivery of service to the customer does not proceed until the planned arrangements have been satisfactorily completed, unless otherwise approved by a relevant authority and, where applicable, by the customer.

Customer Success Management platform (<https://csm.neurealm.com/login>) is launched for the purpose of monitoring the performance of Customer success goals through the CSM Platform. CSM platform used by the Customers and Customer Success Management team to keep track of the following

- a. Customer Success Goals and associated KPI performance
- b. Risks & Issues
- c. Ideas & Innovations
- d. Success Survey result
- e. Process Compliance
- f. Action items

Analysis & Evaluation

Neurealm determines, collects and analyses appropriate data to demonstrate the suitability and effectiveness of the BMS and to evaluate where continual improvement of the effectiveness of the BMS can be made.

Methods of the analysis of data include, where appropriate:

- a. Line chart / Trend Chart / Control Chart – used to detect the trends and unusual activities within the data set.
- b. Pareto Chart Analysis – used to analyse the different components that make up the data value in a descending order, complete with the cumulative percentage line superimposed on it.
- c. SWOT Analysis – used to analyse process strengths, weaknesses, opportunities and threats based on the characteristics of the data set – whether internal or external,

- d. Arithmetic average or mean – used to identify the average performance value of the process,
- e. Median – used to identify the actual middle value of the data set,
- f. Mode – used to identify the most frequent value occurring within the data set,
- g. Range – used to determine the difference between the lowest and highest values of the data set,
- h. Cause and Effect Analysis – used to analyse the causes and effects of a given data set,
- i. Risk Analysis – used to identify potential risks given the actual data set, and
- j. Other analysis methods, as appropriate.

The analysis of data provides information relating to

- a. Customer satisfaction
- b. Conformity to product requirements
- c. Effectiveness of QMS, ISMS, SMS and OHS performance
- d. Characteristics and trends of processes and products, and
- e. Supplier performance

RCA shall be performed and initiate a corrective action plan when the achievement of BMS Objectives / KPI value goes less than against the target.

Evaluation of Compliance

Compliance with relevant OHS legislation, regulations and other requirements are documented and tracked by the respective function (Admin, Finance, HR) and compliance status is reviewed in the OHS Management forum. Legal and other requirements are identified and updated through regular interactions with concerned authorities and/or by subscribing to the Central and State Government gazettes and CIL. Copies of the updated legal and other requirements and a Register of these requirements are maintained in the compliance tracker (register)

Incidents, Accidents, Non-Conformance's and Corrective & Preventive

Actions Incident Investigation

All the incidents reported are investigated and completed within seven business day by the Admin team as per incident management procedure considering the following

- 1) Determination of underlying OHS deficiency and other factors that might or contribute to the occurrence of incidents
- 2) Need for corrective action
- 3) Opportunities for preventive action & continual improvements
- 4) Document the investigation result as part of the Incident report

Internal Process Assessments (a.k.a Audits)

Internal Process assessments are regularly carried out as per the standard practice for Internal Process Assessment to determine whether the BMS

- a. Conforms to the business management system requirements and requirements of the ISO 9001, ISO 20001, ISO 27001 standards, OHSAS – ISO 45001, PCI-DSS v4.0, HIPAA and SEI-CMMi DEV & SVC model
- b. Is effectively implemented and maintained

Annually, an internal assessment plan is prepared, taking into consideration the status and importance of the processes, areas and OHS risks to be assessed as well as the results of the previous assessments. The assessment criteria, scope, frequency, assessor and methods of assessment are defined appropriately in the internal assessment schedule and the assessment plan. Refer to standard practice for Internal Process Assessment.

The selection of assessors and conduct of assessments always ensures objectivity and impartiality of the assessment process where assessors are ensured to observe the assessment principles and not to assess their own work.

The standard practice for internal process assessment has been established to define the responsibilities and requirements for planning and conducting assessments, establishing records and reporting results. Also, the internal assessment process highlights the risks and impact of the assessment findings.

Records of the assessment and their results are maintained in the Customer Success Management platform under the SQA Management module.

The management responsible for the area being assessed ensures that any necessary corrections and corrective actions are taken without undue delay to eliminate detected nonconformities and their causes.

Follow-up activities include the verification of the actions taken and the reporting of verification results

Management System Review

Neurealm Leadership team review the BMS performance every quarter through Quality Council, Information Security Council and Account / Engagement level performance review to ensure its continuing suitability, adequacy and effectiveness. This review includes assessing opportunities for improvement and the need for changes to the BMS, including the BMS Policy and objectives.

9.3.1 Review Input

The Management Representative is responsible for providing the following inputs for the management reviews:

- a. Status of actions from previous management reviews (Quality/Security Council meeting),
- b. Changes in external and internal issues that are relevant to the ISMS
- c. Changes in needs and expectations of interested parties that are relevant to the ISMS
- d. Relevant communications from customers and other external interested parties, including feedback and complaints
- e. Feedback on the BMS performance, including the following

- i. Process Compliance, Security Compliance, HIPAA Compliance, SMS, OHS and PCI-DSS
- ii. Non-conformities, ISMS & OHS Incidents and corrective actions;
- iii. Monitoring and measurement results;
- iv. Assessment/audit results;
- v. Fulfilment of BMS objectives (Quality, Security, HIPAA, SMS and OHS)
- vi. Process performance & Product conformity
- vii. Performance of the services, objectives, policies
- f. Feedback from interested parties,
- g. Results of risk assessment and the effectiveness of action taken to address risks & opportunities
- h. Opportunities for Continual Improvement
- i. Evaluation of compliances with applicable legal, statutory, regulatory requirements and with other requirements to which the organization subscribes
- j. Current and forecast human, technical, information and financial resource levels, and human and technical resource capabilities

9.3.2 Review Output

The output from the management reviews include any decisions and actions related to

- ★ Changes to BMS policy, objectives, needs and expectations of interested parties that are relevant to BMS
- ★ Decisions & Directions for the continuous Improvement / effectiveness of BMS
- ★ Improvement of product / service related to customer requirements
- ★ Improvement on QMS, ISMS, SMS, OHS, HIPAA, PCI-DSS compliance and
- ★ Accepted Risks
- ★ Resource needs
- ★ Action Items

The Management Representative maintains the Minutes of the Meeting for the Management Reviews

Service Reporting

Service Reporting:

The performance and effectiveness of service shall be reported to customer and interested parties as agreed. Decisions and actions related to service reporting shall be tracked through MoM / Action items through CSM platform.

The service reporting will address the following performance reports but not limited to:

1. Performance against service targets
2. Incidents – severity and priority based (Major/Minor/Low)
3. No. of changes /RFCs
4. Operational disruptions – IT Service continuity execution status
5. Volume metrics
6. Trend on SLA Adherence % (as applicable)

7. Risks (High Impact)
8. CAPA – Action items status
9. Performance measures – ex Response time, Resolution time, availability
10. User CSAT Survey (if agreed with client)

10. IMPROVEMENT

Incidents, Nonconformity and corrective action

Neurealm ensures that product which does not conform to product requirements is identified and controlled to prevent its unintended use or delivery. Neurealm takes action to eliminate the causes of nonconformities to prevent recurrence.

Where applicable, Neurealm deals with nonconforming product by one or more of the following ways:

- In case of incidents, suitable action is taken to control and correct it; and deal with consequences.
- Take corrective action to eliminate the detected nonconformity by determining the causes of the nonconformity and if similar nonconformities exist or could potentially occur.
- Review Corrective actions taken is appropriate to the effects of the nonconformities encountered; and
- Review existing assessment of BMS risks and implement an appropriate action including corrective actions.
- Make changes to BMS / concerned processes, if necessary
- Evaluate with the participation of staff and involvement of other relevant interested parties, the need for corrective actions to eliminate the root cause(s) of the incident or nonconformity in order that it does not recur or occur elsewhere by a) investigating the incident or reviewing the nonconformity b) determining the cause(s) of the incident or nonconformity d) determining if similar incidents have occurred, if nonconformities exists, or if they could potentially occur

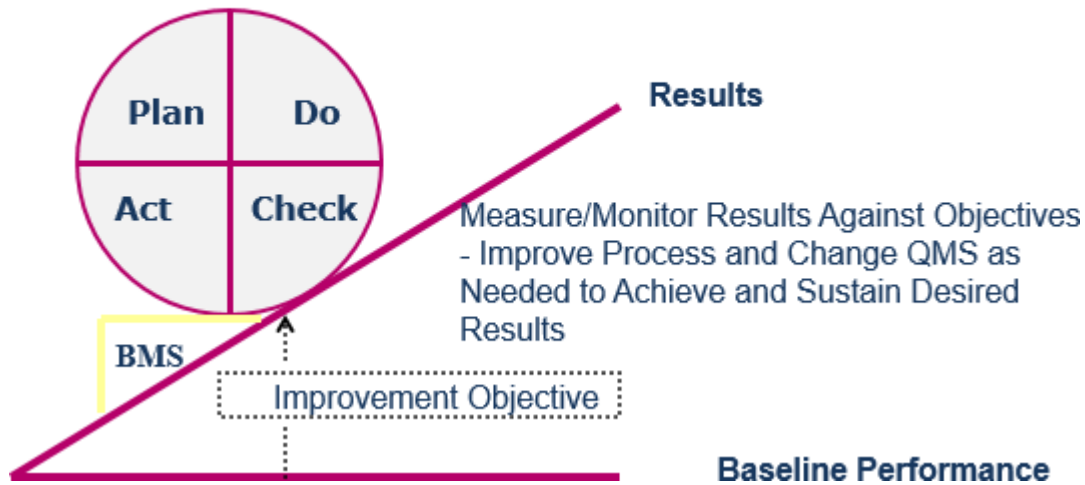
When nonconforming product is corrected, it is subject to re-verification to demonstrate conformity to the requirements.

Records of the nature of nonconformities and any subsequent actions taken, including concessions obtained, are maintained.

Continual Improvement

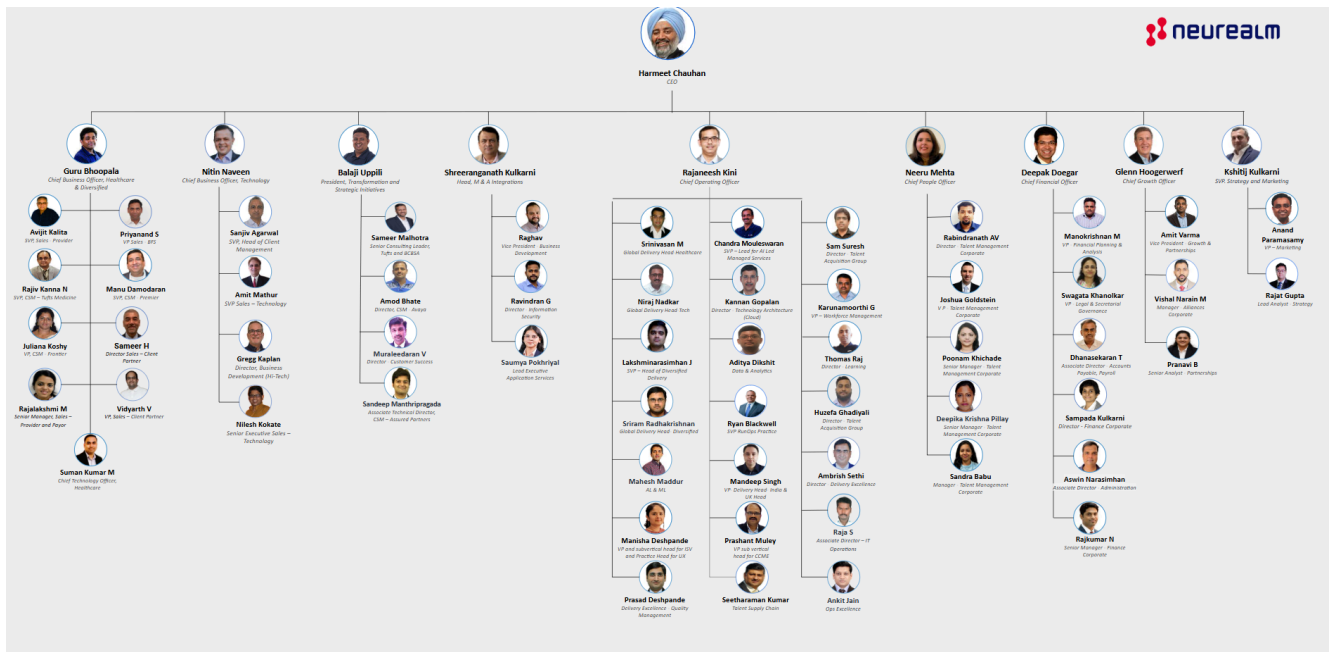
Neurealm continually improves the effectiveness of BMS using BMS Policy, objectives, assessment results, analysis of data, corrective actions and management review using PDCA principles. The process owners are responsible for the continual improvement of their respective process, product, and service. Standard Practice for Process Management supports a structured approach to identify improvement potential and take appropriate measures. All agreed actions become part of Process Improvement Proposal (PIP) tracker, which is introduced in order to continually improve the processes, as well as to document, monitor and check the effectiveness of the improvement measures.

Improve Process through PDCA Cycle



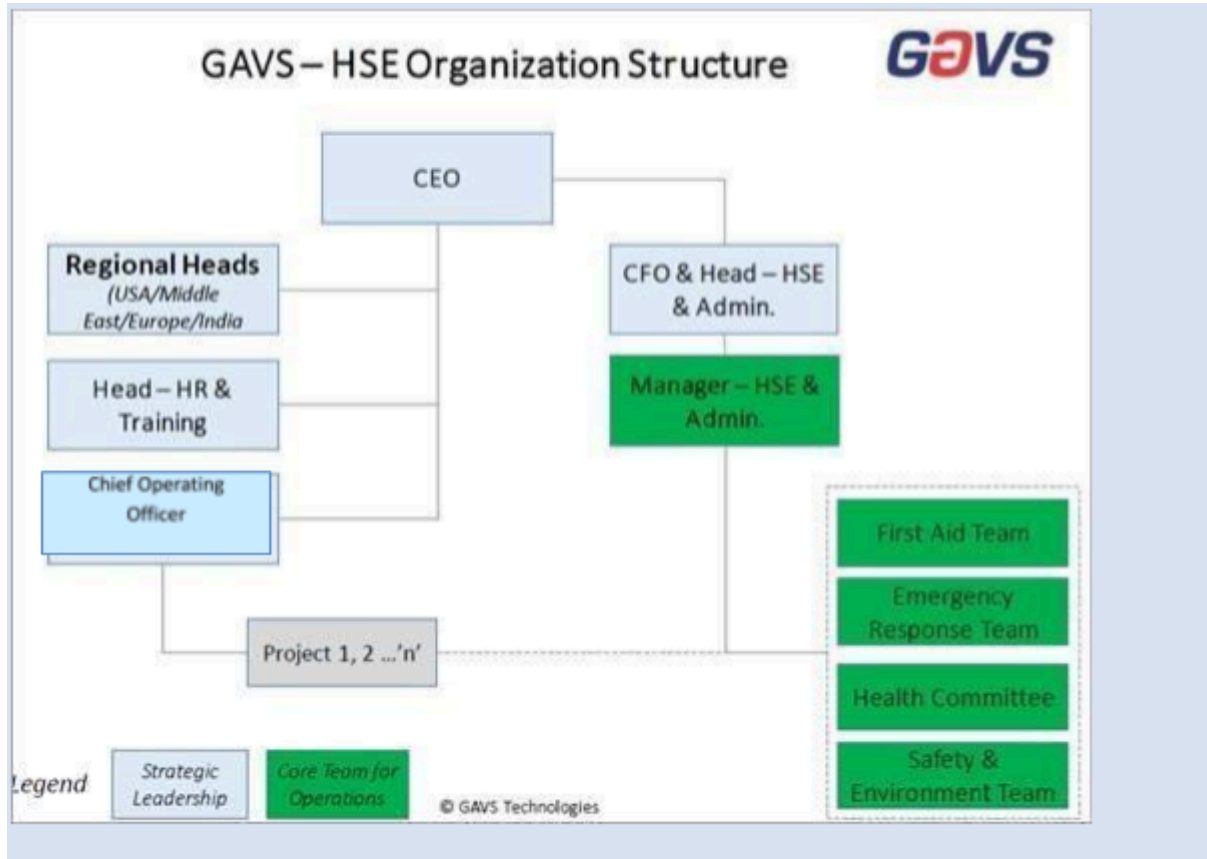
Annexures

A. Organization chart



B. HSE Organization chart

Location:Neurealm Chennai



Guideline to classify Threats & Weakness (earlier it was referred as Major NC / Minor NC)

Threats	Weakness
Total breakdown of system, control, or procedure. Absence of a BMS requirement	Failure to conform to a requirement which (based on judgment and experience) is not likely to result in BMS failure
A number of minor non-conformances related to the same clause	A single observed lapse or isolated incident

<p>An nonconformity that would result in probable delivery of nonconformity or un-inspected product</p> <p>A condition that may result in the failure or materially reduce the usability of product for intended purpose;</p> <p>A nonconformity that experience and judgment indicate will likely result in QMS failure or materially reduce its ability to assure controlled processes and products</p>	<p>Minimal risk of nonconforming product or service</p>
<p>Majors represent serious problems in the system that must be addressed with attention and resources on a priority basis. It puts the business at risk with customers.</p>	<p>Minor nonconformities have little likelihood of allowing nonconforming product or service to be delivered or causing a breakdown of system control. It does indicate that there are occasional lapses that must be formally addressed through corrective action.</p>
<p>Failure to take corrective or preventive action</p>	<p>One or a few individuals (out of many) do not use a procedure correctly</p>
	<p>Procedures needs minor changes to be effective</p>
	<p>One or a few records incomplete</p>

C. HSE Requirements by Contractors including outsourced services (To be a part of contract documents)

Housekeeping

Contractors shall ensure that their work area is kept clean, tidy and free from debris. The work areas must be cleaned daily. Any disposal of waste shall be done by the Contractor.

All equipment, materials and vehicles shall be stored in an orderly manner. Access to emergency equipment, exits, telephones, safety showers, eye washes, fire extinguishers, pull boxes, fire hoses, etc. shall not be blocked or disturbed.

Confined Space

Before commencing Work in a confined space the Contractor must obtain from Neurealm a Permit to Work, the Permit to Work will define the requirements to be followed.

As minimum Contractors must ensure the following:

- i. Confined spaces are kept identified and marked by a sign near the entrance(s).
- ii. Adequate ventilation is provided
- iii. Adequate emergency provisions are in place
- iv. Appropriate air monitoring is performed to ensure oxygen is above 20%.
- v. Persons are provided with Confined Space training.
- vi. All necessary equipment and support personnel required to enter a Confined Space is provided.
- vii. Tools, Equipment and Machinery

The Contractor must ensure that all tools & equipment provided for use during the Work is: suitable for its intended use; safe for use, maintained in a safe condition and where necessary inspected to ensure this remains the case (any inspection must be carried out by a competent person and records shall be available);

Used only by people who have received adequate information, instruction and training to use the tool or equipment.

Provided with Earth leakage circuit breaker (ELCBs) at all times when using electric power cords. Use of electrical tape for temporary repairs is prohibited.

Working at Height

Any Work undertaken where there is a risk of fall and injury is considered to be working at height.

For any Contractor Personnel working at height, Contractors shall provide fall prevention whenever possible and fall protection only when fall prevention is not practicable. Before commencing Work in a height the Contractor must obtain from Neurealm a Permit to Work, the Permit to Work will define the requirements to be followed. Supervisor must be present at all point of time, to ensure no deviation occurs during the course of work.

Fall Prevention System

Fall prevention systems (e.g. fixed guardrails, scaffolds, elevated work platforms) must provide protection for areas with open sides, including exposed floor openings.

Fall Protection Systems

Where fall protection systems are used then the Contractor must ensure the following is applied:

- i. Only approved full body harness and two shock-absorbing lanyards are used,
- ii. Prior establishment of a rescue plan for the immediate rescue of an employee in the event they experience a fall while using the system,
- iii. Anchorage points must be at waist level or higher; and capable of supporting at least the attached weight,
- iv. Lifeline systems must be approved by NEUREALM before use.

- v. Use of ISI marked industrial helmets at all points of time.

Scaffolding

All scaffolds shall subject to a documented inspection by a competent person and clearly marked prior to use. The footings or anchorage for scaffolds shall be sound, rigid and capable of carrying the maximum intended load without settling or displacement. All scaffolding materials should be of MS tubular type.

Guardrails and toe-boards shall be installed on all open sides and ends of scaffold platforms. Scaffolds shall be provided with an access ladder or equivalent safe access. Contractor Personnel shall not climb or work from scaffold handrails, mid-rails or brace members.

Stairways and Ladders

Ladders should only be used for light duty, short-term work or access in line with the below and the Site Requirements.

- a. Fabricated ladders are prohibited.
- b. Ladders will be secured to keep them from shifting, slipping, being knocked or blown over.
- c. Ladders will never be tied to facility services piping, conduits, or ventilation ducting.
- d. Ladders will be lowered and securely stored at the end of each workday.
- e. Ladders shall be maintained free of oil, grease and other slipping hazards
- f. Ladders will be visually inspected by a competent person and approved for use before being put into service. Each user shall inspect ladders visually before using.
- g. Ladders with structural defects shall be tagged "Do Not Use," immediately taken out of service, and removed from the Site by the end of the day.

Roof Work/Access

Roof work and access to roofs must not be undertaken without prior authorization from Neurealm.

Overhead Work

A secure exclusion zone shall be maintained by Contractor below overhead work to prevent access. It is forbidden to work beneath a suspended load.

Lifting Operations

Cranes and Hoisting Equipment

Contractors shall operate and maintain cranes and hoisting equipment in accordance with manufacturers' specifications and legal requirements.

Only Contractor Personnel trained in the use of cranes and hoists are permitted to use them.

Lifting Equipment and Accessories

All lifting equipment / accessories e.g., slings, chains, webbing, chain blocks, winches, jacks etc. shall be indicated with their safe working load, have an identification number visible on the unit and be inspected and tested in accordance with legal requirements.

Damaged equipment / accessories and equipment shall be tagged “out of use” and immediately removed from Site.

Lockout Tag out (“LOTO”)

Prior to performing work on machines or equipment, the Contractor shall ensure that it is familiar with LOTO and Permit to Work procedures and that all of its affected Contractor Personnel receive the necessary training.

Barricades

Floor openings, stairwells, platforms and walkways, and trenching where a person can fall any distance shall be adequately barricaded and where necessary, well lit. Where there is a risk of injury from a fall then rigid barriers must be used.

Barricades must also be used to prevent personnel entering an area where risk of injury is high e.g., during overhead work activity or electrical testing etc. Such barricading must provide clear visual warning..

Compressed Gas Cylinders

Gas cylinder shall be securely stored and transported, and identified and used in line with the local requirements. Hose lines shall be inspected and tested for leaks in line with local requirements. Flash Back arrestor to be used to prevent any explosion due to back fire.

Electrical Safety

Prior to undertaking any work on live electrical equipment the Contractor must obtain a Permit to Work from NEUREALM. Wherever possible live work should be avoided. Any control measures highlighted shall be implemented prior to work commencing.

The below measures will be taken:

- ❖ Work practices must protect against direct or indirect body contact by means of tools or materials and be suitable for work conditions and the exposed voltage level.
- ❖ Energized panels will be closed after normal working hours and whenever they are unattended. Temporary wiring will be de-energized when not in use.
- ❖ Only qualified electrical Contractor Personnel may enter substations and/or transformer and only after being specifically authorized by NEUREALM.

Hot Works

A Permit to Work must be obtained from NEUREALM prior to any hot works (welding, grinding, open

flame work). Suitable fire extinguishing equipment shall be immediately available. Objects to be welded, cut or heated shall be moved to a designated safe location, or, if they cannot be readily moved, all movable fire hazards in the vicinity shall be taken to a safe place. Personnel working around or below the hot works shall be protected from falling or flying objects.

Prior to the use of temporary propane or resistance heating devices approval must be obtained from NEUREALM.

Trenching, Excavating, Drilling and Concreting

A Permit to Work must be obtained from NEUREALM and all underground lines, equipment and electrical cables shall be identified and located prior to beginning the work. The Contractor shall assign a competent Contractor Personnel to all trenching and excavation work.

Safe means of access and egress shall be located in trench excavations. Daily inspections shall be conducted by a competent Contractor Personnel for evidence of a situation that could result in possible cave-ins, indications of failure of protective systems or other hazardous conditions.

Physical barriers shall be placed around or over trenches and excavations. Flashing light barriers shall be provided at night.

Environmental Requirements Waste Management

The Contractor is responsible to remove any waste generated by the work being done on the Site. The Contractor must dispose of the waste in line with the relevant local legislative requirements. The waste disposal route shall be documented and made available for NEUREALM to review at any time and may be subject to NEUREALM's prior approval.

Wastes (includes rinse from washing of equipment, PPE, tools, etc.) are not to be poured into sinks, drains, toilets, or storm sewers, or onto the ground. Solid or liquid wastes that are hazardous or regulated in any way are not to be disposed of in general site waste receptacles.

Spills

The Contractor is responsible for the provision of adequate spill kits/protection and the clean up and disposal costs arising from such spills.

Emissions

The Contractor shall identify and quantify any emission sources associated with the Works. The control measures associated with these emission shall be subject to the approval of NEUREALM. Emissions include but are not limited to noise, dust, fumes, vapors.

Annexure – E

Roles and Responsibilities of CISOs

CISOs shall, inter alia, be responsible for the following:

- o Maintaining and updating the threat landscape for the organisation on a regular basis including staying up to date about the latest security threat environment and related technology developments.
- o Establishing a cyber security program and business continuity programme and for drafting of various security policies e.g., Information security policy, Data governance and classification policy, Access control policy, Acceptable use of assets
 - and asset management, Risk assessment and risk treatment methodology, Statement of Applicability, Risk management framework including third parties, Cryptography, Communications security, Information Security awareness programs for all personnel in the organisation and Incident management. This would also include:
- Ensuring review of the Information Security Policy by internal and/or external subject matter experts to check for the adequacy and effectiveness of the ISMS programme
- Reviewing and updating the cyber security policy documents.
- Defining rules for secure and acceptable use of communication channels for the business requirements of the department/organization.
- o Developing and implementing a security architecture for the organisation by leveraging technology and understanding of threat landscape.
- o Establishing and reviewing the Risk Assessment methodology and selection of appropriate controls for risk mitigation by leveraging technology and an understanding of the threat landscape in the organisation.
- o Interacting with regulatory bodies and external agencies that could be of help to maintain information security for the organization, e.g. CERT-In
- o Ensuring that the following activities are carried out at regular intervals, either directly or through the deployment of subject matter experts:
 - Log review, analysis and exception reporting
 - **Vulnerability Assessment & Penetration Testing (VAPT)** of all websites, portals and IT systems, on a quarterly basis at a minimum; ensuring that websites are GIGW compliant
 - **Web Application Security Assessment (WASA)** and white-listing of all web applications in use by the organisation, annually at a minimum

- o **2.6.4 Software Development Lifecycle (SDLC) Audit and periodic Code Reviews** to ensure that applications continue to be secure
 - 2.6.5 **Information Security Audit** of IT Systems and controls, including site audits as appropriate, where online operations span multiple locations. The audit should ensure the following:
 - 2.6.5.1 No unsupported operating systems are in use in the department
 - 2.6.5.2 CISO prescribed hardening guidelines, patch management guidelines, anti virus / malware guidelines, no privilege access on endpoints, regular review of access privileges, acceptable configuration guidelines and procedures are properly implemented;
 - 2.6.5.3 Ensure defined principles of secure software development process is followed for all software applications and the same is reflected in contracts, if software development is outsourced;
 - 2.6.5.4 Citizen / customer data privacy to be ensured in case if citizen / customer data is captured and maintained;
- o Periodic assessment / audits of third party service providers to assess risks to you organisation;
- o Certify that the time synchronization of the Network Time Protocol in the organisation has been done with the National Physical Laboratory.
- o **Issuing and periodic review** of device hardening guidelines, patch management guidelines, anti-virus / malware guidelines, User Access Management guidelines, privilege access management guidelines, end point management guidelines, connectivity guidelines for Trading partners and external agencies, controls on mobile devices and wireless technology
- o **Authorising an Acceptable Use policy for software packages and freeware** in consonance with the organisation's risk/threat landscape, business objectives and Security Policy & Procedures
- o Adopting a suitable IT Governance framework for implementing supporting processes such as **Configuration Management, Change Management, Incident Management and Problem Management** etc. CISO should ensure that appropriate instructions are issued for adherence to processes within the organisation and that no authorised changes are carried out to online systems without specific Change Approval.
- o Ensuring that the IT infrastructure deployed for online operations is kept up to date as per policy and is always under maintenance and technical support so that security patches and bug fixes are regularly applied to protect the infrastructure from vulnerabilities.
- o Ensuring that clauses pertaining to Information Security are incorporated into contracts/agreements/MoUs with service providers.

- o Securing senior management approval for emergent/urgent procurements necessary to keep the infrastructure safe from attacks and exploits
- o Developing and Implementation of scenario-based **Incident Response plans to deal with Cyber crises, contingencies and disasters, attack on IT systems** etc. This should include incident containment, assessment, root cause analysis, mitigation/ prevention, continuous monitoring, forensics and reporting as required. This should include the following:
 - Ensuring that Incidents, especially repeat incidents are investigated and corrective action taken as identified through a comprehensive Root Cause Analysis (RCA)
 - Ensuring that information security incidents are reported to CERT-In
- o Coordination with stakeholders in all matters related to internal and external security and covering the following aspects:
 - Assessing the adequacy of controls for Confidentiality, Integrity and Availability of all the Information Systems;
 - Explaining exceptions, if any, to security policies and procedures along with the risk to business;
 - Systematically identifying and managing security risks from an end-to-end perspective on a periodic basis;
 - Assessment of the maturity and effectiveness of the security program;
 - Steps proposed to remediate gaps identified, if any; and
 - Impact of the incidents and breaches on the organisation from a business perspective.
- o Establishing a **Cyber Crisis Management Group** with the head of organisation (or his appointed representative) as its Chairman and to prepare a list of contact persons to be contacted during crisis e.g. internal: financial, personnel etc. and external: law enforcement agencies, CERT-In etc. complete with up-to-date contact details. CCMG should authorise a **Cyber Crisis Management Plan (CCMP)** outlining roles and responsibilities of organisational stakeholders. Implementing the CCMP, including security best practices and specific action points:
 - Planning and executing periodic disaster recovery drills/simulation exercises in order to establish the adequacy of the Business Continuity Plan
 - Ensuring that periodic tests are conducted to evaluate the adequacy and effectiveness of technical security control measures, especially after each significant change to the IT applications/systems/networks as well as after any major incident
 - The geographical spread of IT Systems and online operations spans multiple locations across the country, identifying personnel responsible for implementation of information security at the local level as well as for periodic reporting as required to the CISO.
- o Coordinating all matters related to security internally and externally while providing regular reports to the head of the organisation covering the following aspects:

- Assessing the adequacy of controls for confidentiality, integrity and availability of all the information systems;
- Explaining exceptions, if any, to security policies and procedures along with the risk to business;
- Systematically identify and manage security risks from an end to end perspective on a periodic basis;
- Assessment of the maturity and effectiveness of the security program;
- Steps proposed to remediate gaps identified, if any; and
- Impact of the incidents and breaches on the organisation from a business perspective.
- o Develop and implement ICT disaster recovery and security incident management processes, which consists of following activities:
 - To coordinate response to security incidents;
 - To prepare evidence for legal action following an incident; and
 - To comply with the security suggestions provided to them in incidents' analysis' reports;
 - To analyze incidents in order to prevent their recurrence; and
 - To report information about security incidents without delay to CERT-In.

This is the end page. Leave this page blank.



About Neurealm

Neurealm is the right-sized partner for Engineering, Modernization, and RunOps, blending human intelligence with the latest technologies to help businesses across industries such as Healthcare, Technology, Manufacturing, Retail, Telecom, and BFSI make smart progress.

With offerings in Digital Platform Engineering, Data, AI, Cybersecurity, and Technology Operations, and delivery centers in India and the US, we empower 250+ global enterprises. Driven by an engineering mindset and powered by Neurealm Labs—our innovation engine—we transform ideas into real-world impact through new-age offerings, cutting-edge solutions, frameworks, and accelerators. Our strong technology alliances and academic partnerships further power the future-ready ecosystems we build for our clients.