“Welcome“ "स्वागतम“

GRID-INDIA INITIATIVES

towards

CYBER SECURED GRID OPERATION

Information & Data Exchange – typical Control Centre

IT SYSTEM

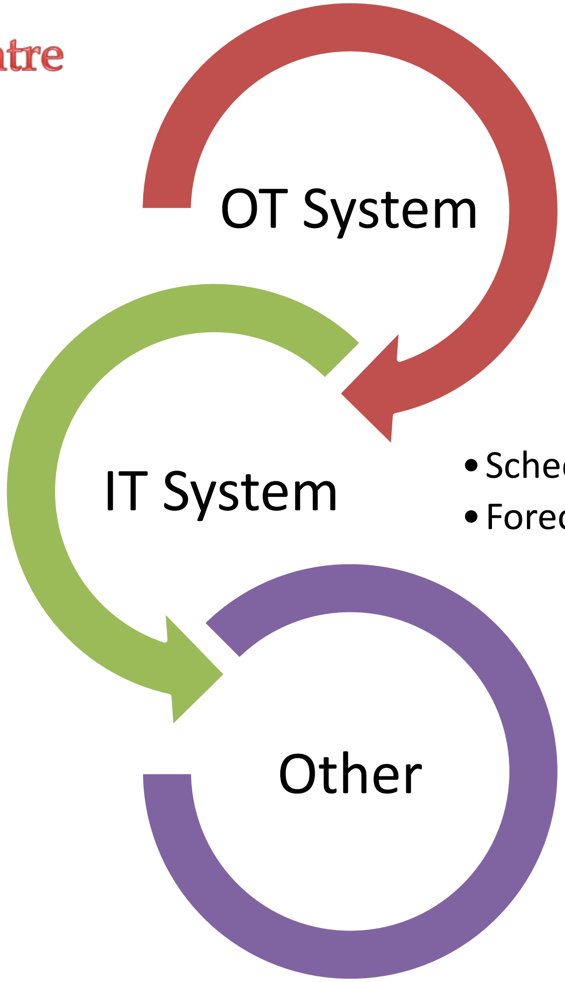
- Web based Energy Scheduling
- REC Mechanism
- Websites
- Reporting & Control Room Management

OT System

- SCADA System
- URTDSM System
- REMC System

Other Connectivity

- AMR System
- Inter RLDC Data Exchange
- PX Data
- NOAR



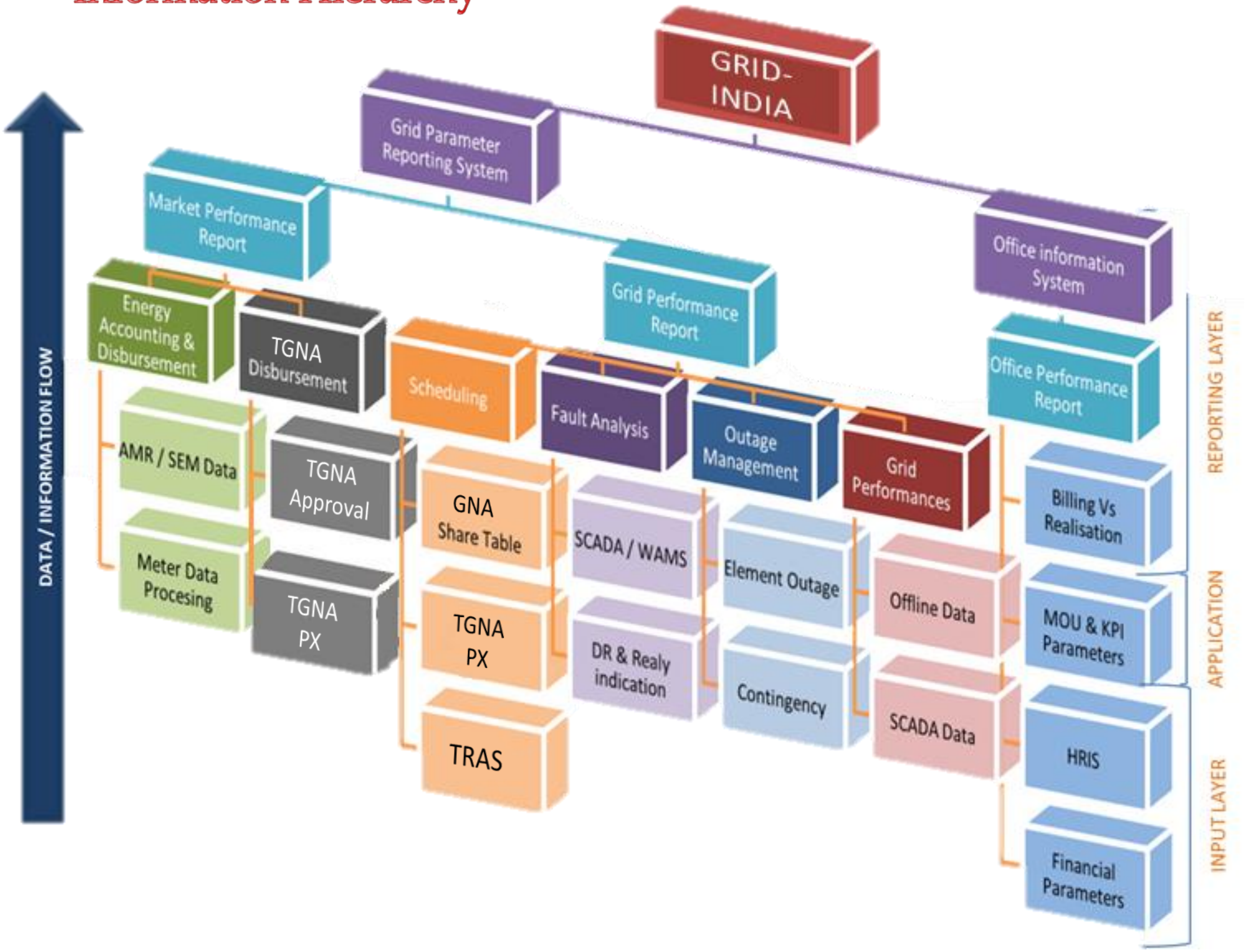
OT System
- Real-time Data
- REMC Schedule

IT System
- Schedule Data
- Forecasting

Other
- Meter Data
- Offline Data
- NOAR

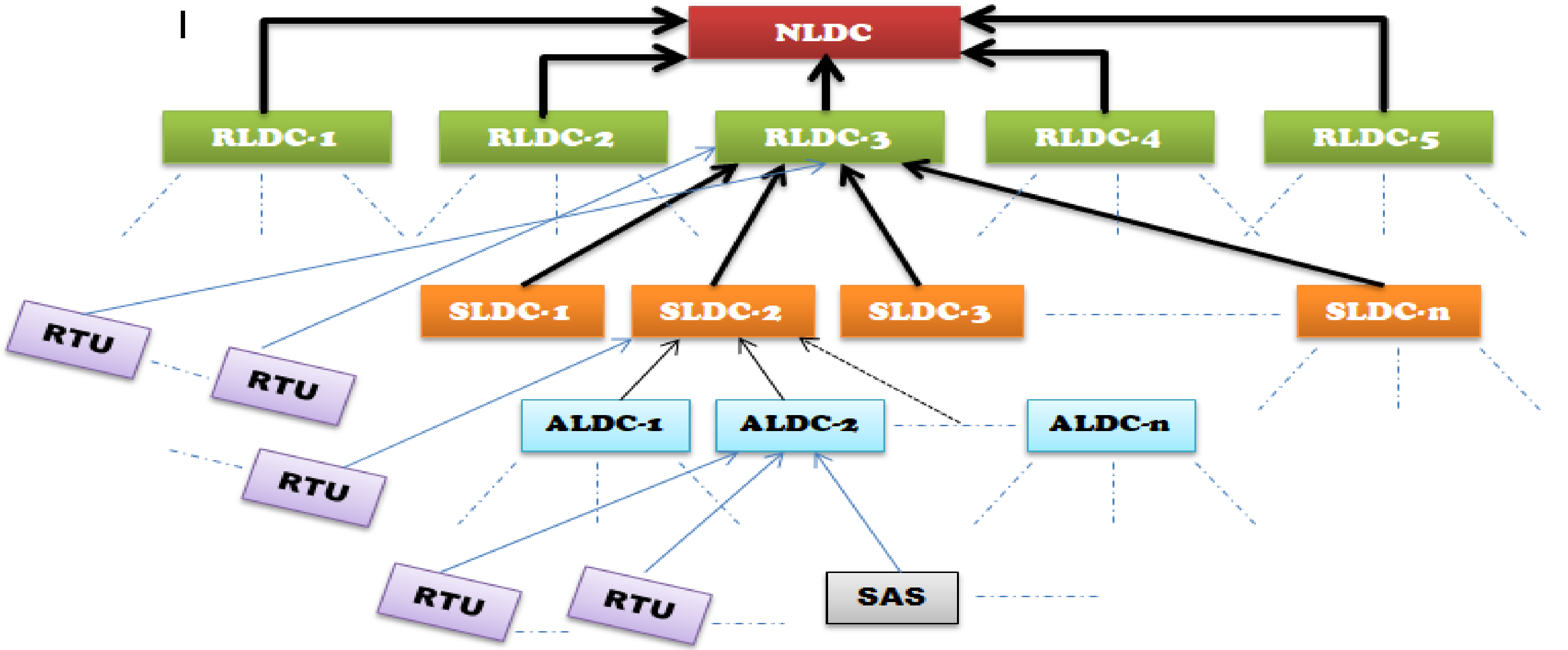
SCADA - Supervisory Control And Data Acquisition
REMC – Renewable Energy Management Centre
URTDSM - Unified Real Time Dynamic State Measurement
REC – Renewable Energy Certificate
AMR – Automated Meter Reading
PX – Power Exchange
NOAR – National Open Access Registry

Information Hierarchy



- ❑ No major connectivity with the Industrial Control Systems
- ❑ Cross-platform / Inter-application information sharing using Secured API
- ❑ Multiple data sources to correlate integrity of Data for accurate decision support
- ❑ Secured dedicated communication infrastructure for Inter-Control Centre data sharing

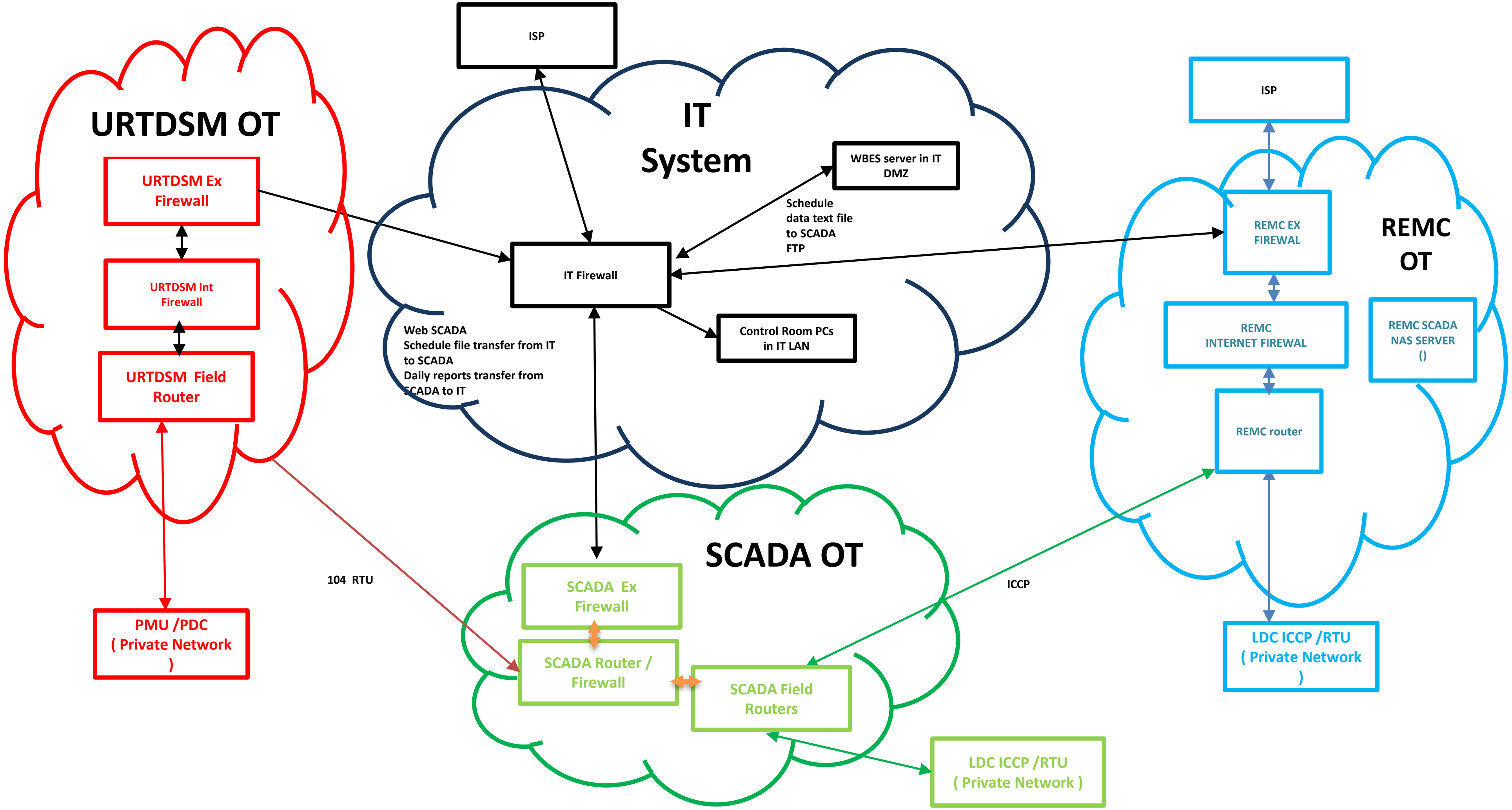
DATA FLOW ARCHITECTURE OF OT SYSTEM



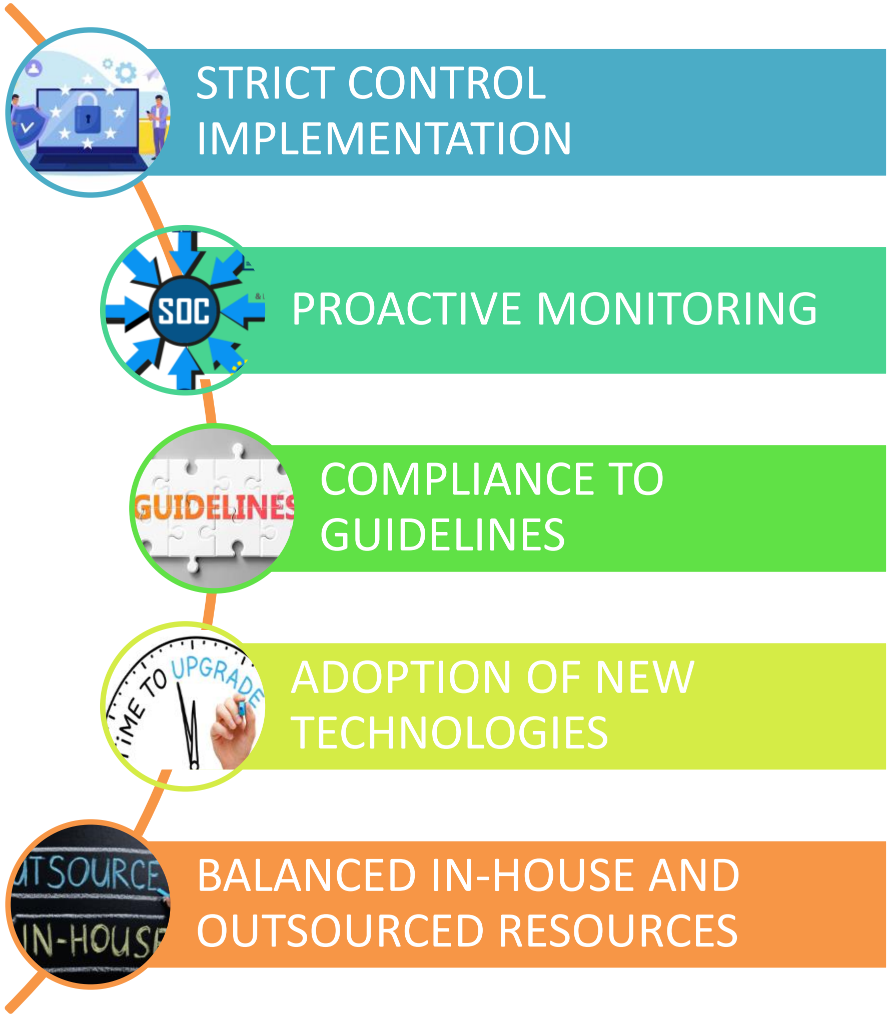
Indian Control Center hierarchy

Reporting of RTUs (or SAS)		
RTU /SAS Status	**Data Ownership**	**Hierarchical forward flow of Data**
Reporting directly to Sub LDC	Sub LDC	Sub LDC -> SLDC -> RLDC -> NLDC
Reporting directly to SLDC	SLDC	SLDC -> RLDC -> NLDC
Reporting directly to RLDC (or CPCC)	RLDC (or CPCC)	RLDC -> NLDC

DATA EXCHANGE REQURIEMENT BETWEEN IT & OT SYSTEM



Cyber Security Infrastructure & Administration



- STRICT CONTROL IMPLEMENTATION
- PROACTIVE MONITORING
- COMPLIANCE TO GUIDELINES
- ADOPTION OF NEW TECHNOLOGIES
- BALANCED IN-HOUSE AND OUTSOURCED RESOURCES

- INTRUSION PREVENTION SYSTEM AT GATEWAY
- LAYERED NETWORK ARCHITECTURE
- ANTIVIRUS AND ANTI-MALWARE PROTECTION
- LEAST PRIVILEGE USER ACCESS
- ANTI-APT & VA-PT
- HARDENED IT / OT INTEGRATION
- PHYSICAL SECURITY
- DC-DR ARCHITECTURE

Integrated Information Security Policy & Procedures – Pan India

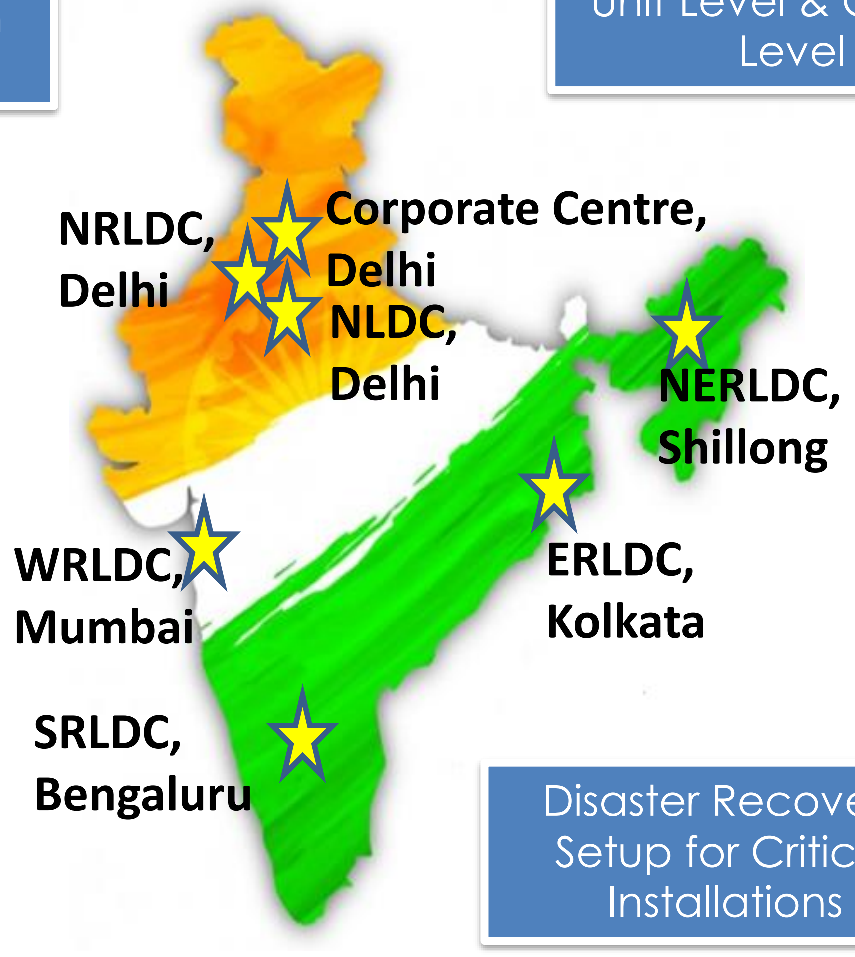
ISO27001:2013 Certified Institution since 2011

Defined Statement of Applicability of ISMS Controls

Monitoring & Compliance to ISMS Requirements

Declared as Critical Information Infrastructure

Regular Third party Audit and Risk Assessment



Identified CISOs at Unit Level & Central Level

Identified Information Security Management Forum

Customized Cyber Security Framework for IT infrastructure

Cyber Crisis Management Team at all locations

Emergency Preparedness Plan and Mock exercises

Disaster Recovery Setup for Critical Installations

Information Security Steering Committee

As per Para, 3(1) of the Information Technology (Information Security Practices and Procedures for Protected System) Rules, 2018 issued by MeitY

- *The organisation having "Protected System"* shall *constitute an Information Security Steering Committee (ISSC) under the chairmanship of Chief Executive Officer/ Managing Director/ Secretary of the organisation.*
- *The composition of Information Security Steering Committee (ISSC) shall be as under:*

I. IT Head or equivalent

II. Chief Information Security Officer (CISO)

III. Financial Advisor or equivalent

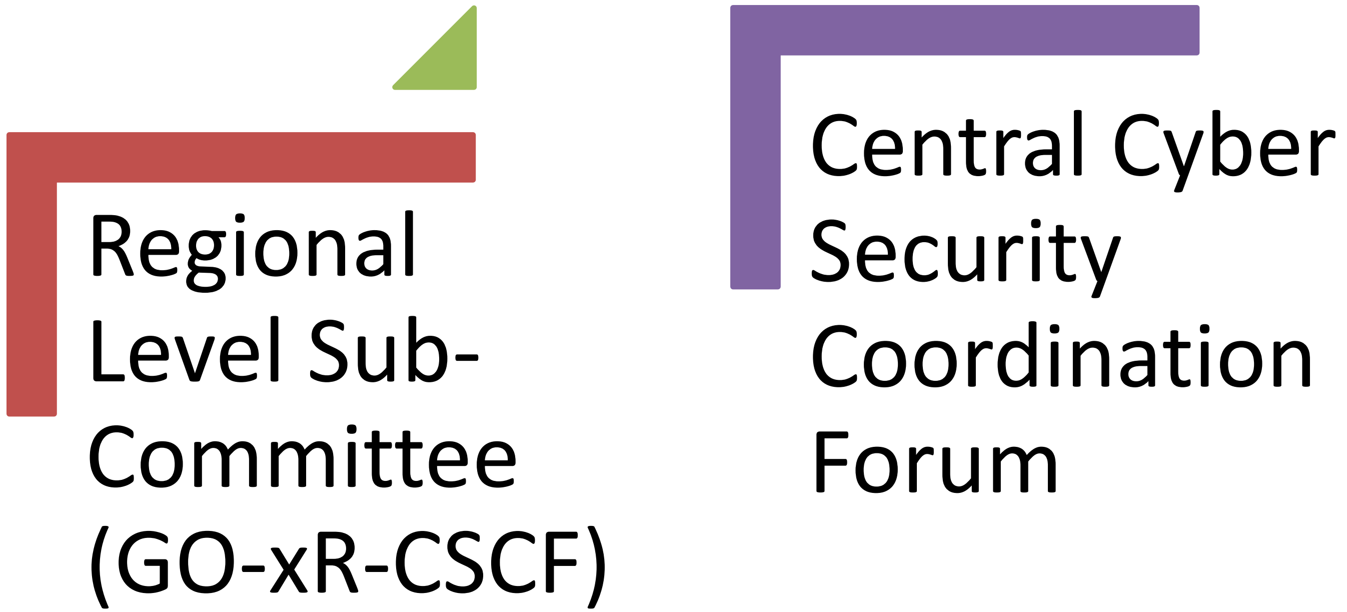
IV. Representative of NCIIPC

V. Any other expert(s) to be nominated by the organization

IEGC Chapter 8

53. CYBER SECURITY COORDINATION FORUM

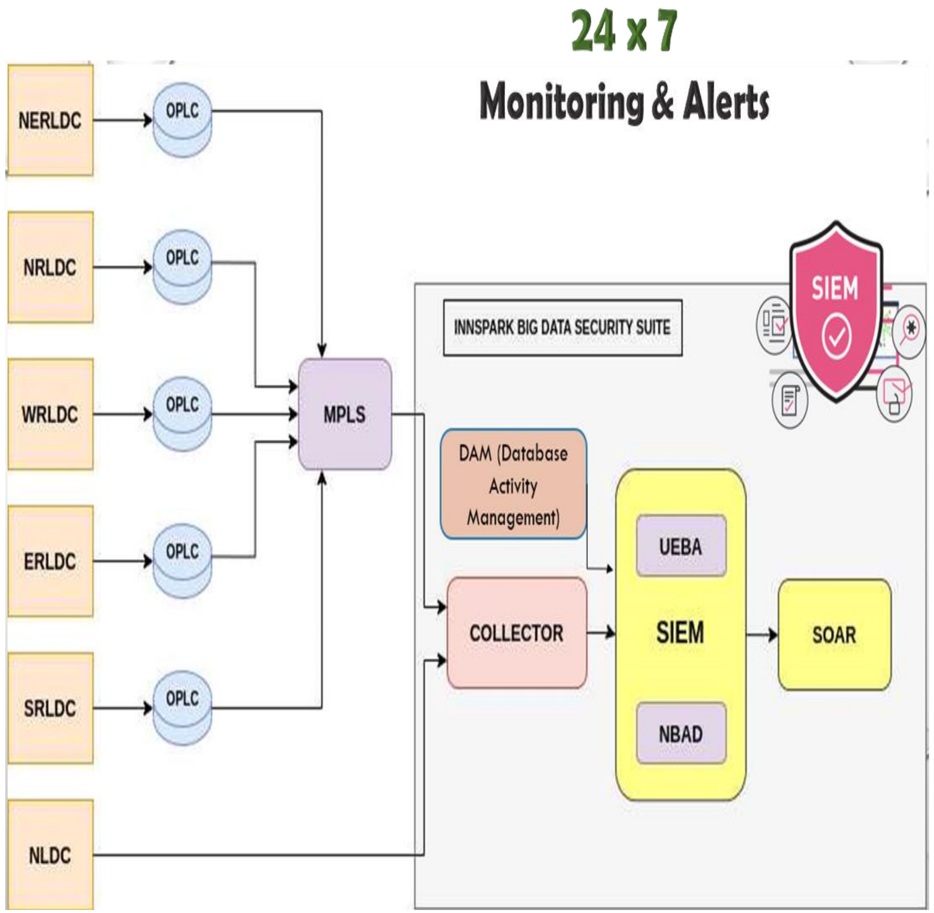
- The sectoral CERT shall form a Cyber Security Coordination Forum with members from all concerned utilities and other statutory agencies to coordinate and deliberate on the cyber security challenges and gaps at appropriate level.
- A sub-committee of the same shall be formed at the regional level.

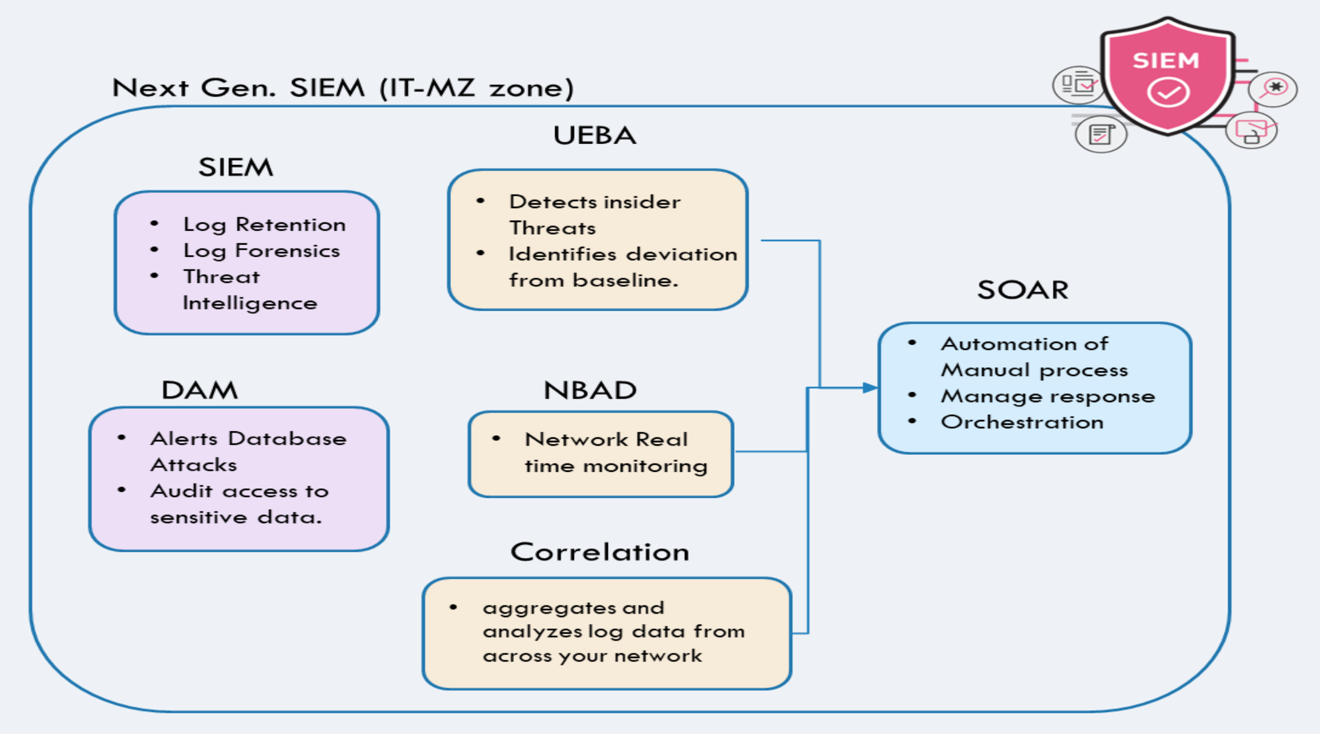


Central Cyber Security Coordination Forum

Regional Level Sub-Committee (GO-xR-CSCF)

24 x 7 Security Operation Centre since Oct’22





Next Gen. SIEM (IT-MZ zone)

SIEM

SIEM

- Log Retention
- Log Forensics
- Threat Intelligence

UEBA

- Detects insider Threats
- Identifies deviation from baseline.

SOAR

- Automation of Manual process
- Manage response
- Orchestration

DAM

- Alerts Database Attacks
- Audit access to sensitive data.

NBAD

- Network Real time monitoring

Correlation

- aggregates and analyzes log data from across your network

251
Integrated Devices

12-13K
Events / Second

700GB
Incremental Data

6
Different Locations

SIEM: Security Information and Event Management

UEBA: User Entity Behavior Analysis
DAM: Database Activity Monitoring

NBAD: Network Behavior Anomaly Detection

OPLC: On-Premise Log Collector

MPLS: Multiprotocol Label Switching

Coordination with SLDCs – CERT-Go Functions

Sectoral Computer Emergency Response Team (CERT) for Grid Operations (GO)

- Grid-India declared as CERT-GO in March’2021 – CERT-GO started coordinating with all SLDCs to ensure Cyber Security initiatives in all LDCs

On-boarding of Load Despatch Centres on Cyber Swatchhta Kendra

- Public Interface of all LDCs have been on-boarded with Cyber Swatchhta Kendra
- Monitoring and predictive measures to eliminate vulnerabilities in LDC systems

FOLD Working Group On Cyber Security

>380 Manpower Trained on Cyber Security

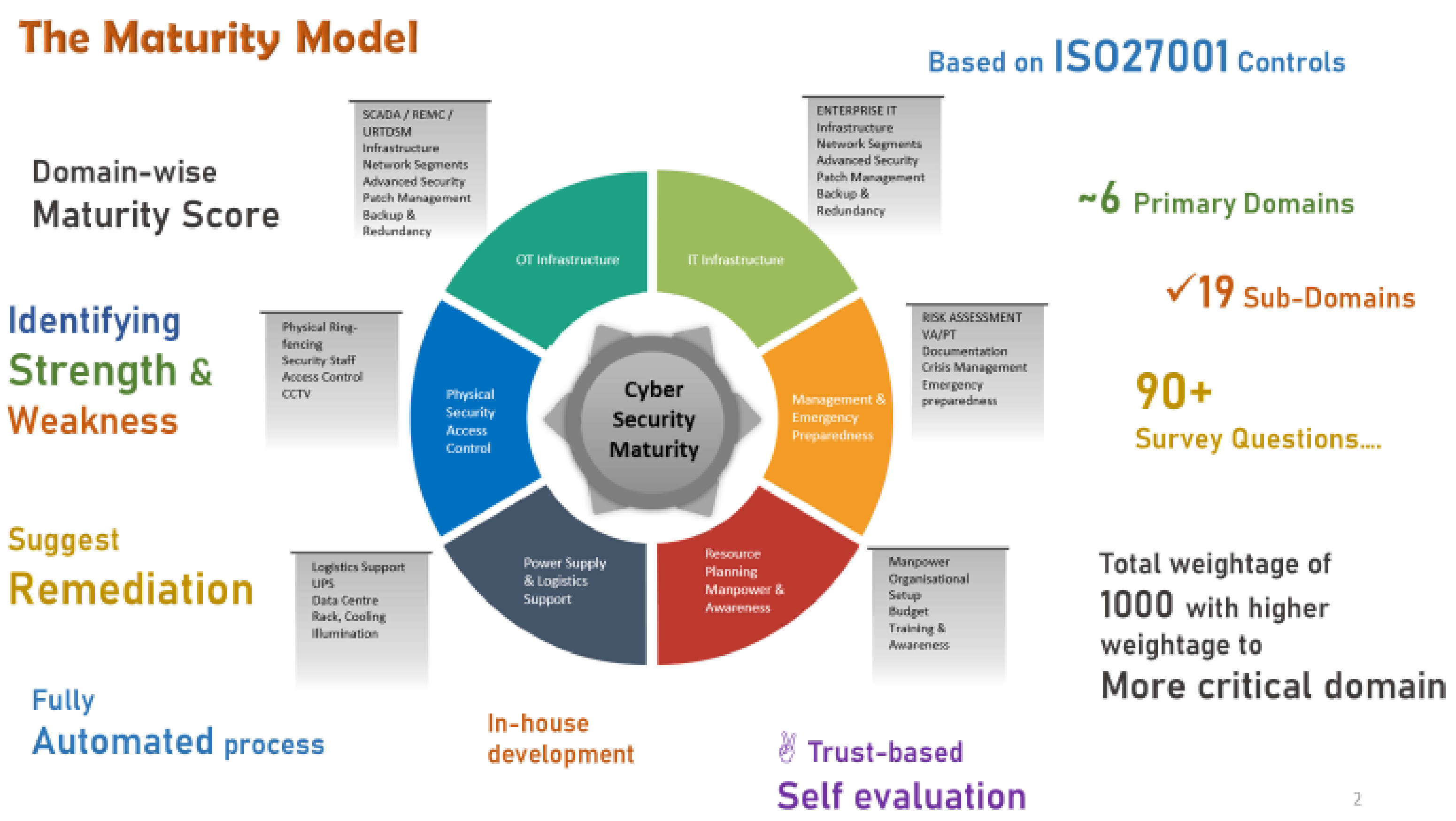
Weekly IOC intimation from SOC to all SLDCs

Visit to LDCs AND RE Plants

Regular Advisory to SLDCs

Periodic Meetings & Interactions

Cyber Security Capability Evaluation of LDCs



The Maturity Model

Based on ISO27001 Controls

Domain-wise Maturity Score

Identifying Strength & Weakness

Suggest Remediation

Fully Automated process

In-house development

✌ Trust-based Self evaluation

~6 Primary Domains

✓19 Sub-Domains

90+ Survey Questions....

Total weightage of 1000 with higher weightage to More critical domain

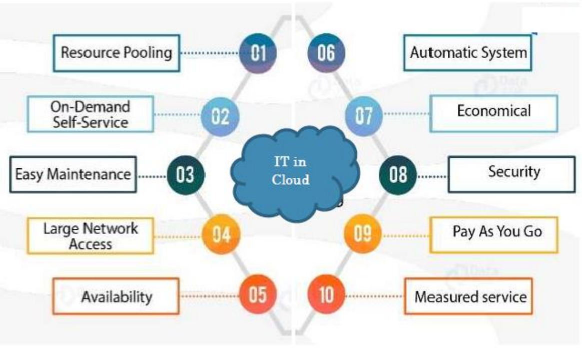
Cyber Security Maturity
OT Infrastructure
IT Infrastructure
Management & Emergency Preparedness
Resource Planning Manpower & Awareness
Power Supply & Logistics Support
Physical Security Access Control
SCADA / REMC / URTDSM Infrastructure Network Segments Advanced Security Patch Management Backup & Redundancy
ENTERPRISE IT Infrastructure Network Segments Advanced Security Patch Management Backup & Redundancy
RISK ASSESSMENT VA/PT Documentation Crisis Management Emergency preparedness
Manpower Organisational Setup Budget Training & Awareness
Logistics Support UPS Data Centre Rack, Cooling Illumination
Physical Ring-fencing Security Staff Access Control CCTV
2

- ❑ 1st. Phase Report submitted to Ministry during October 2022
- ❑ Iimprovement actions taken up by SLDCs based on suggestive measures
- ❑ Revised score with SLDC improvement actions presented to Ministry during April 2023
- ❑ Iinitiative taken by NCIIPC in collaboration with IIT-Kanpur to frame Maturity Model framework
- ❑ GRID-INDIA is participating actively as Subject Matter Expert with NCIIPC & IIT-Kanpur

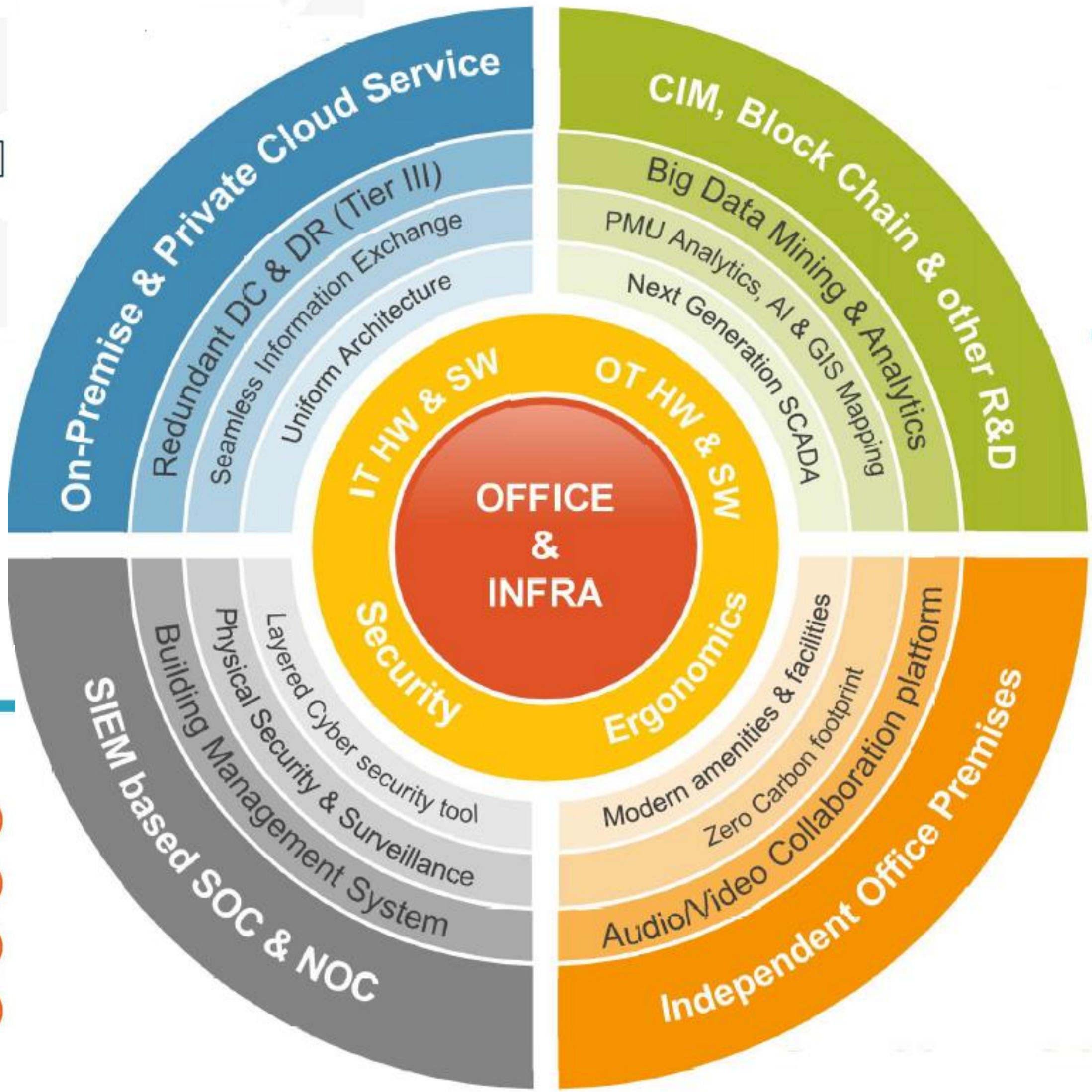
Collaboration at National & International Arena

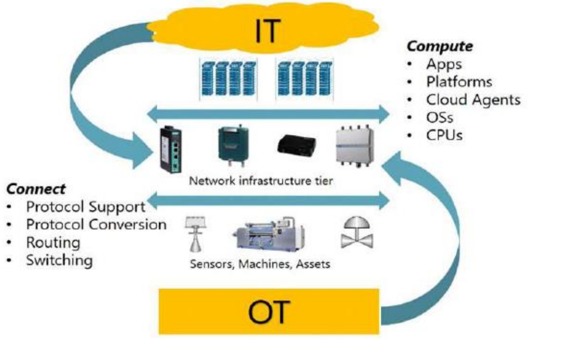
- Committee Member in various GoI initiatives
- Regular feedback to Statutory Bodies
- Information sharing with stakeholders on Indication of compromises based on SOC intelligence
- Participation in various CIGRE D2 activity & working groups
- Publication of Paper & Innovative works in CIGRE / IEEE conferences
- Visit to SLDCs, RE Plants etc. for knowledge sharing & hand-holding
- Collaboration with academia for R&D projects
- Active part in CEA/MoP initiatives towards reform

Vision 2030



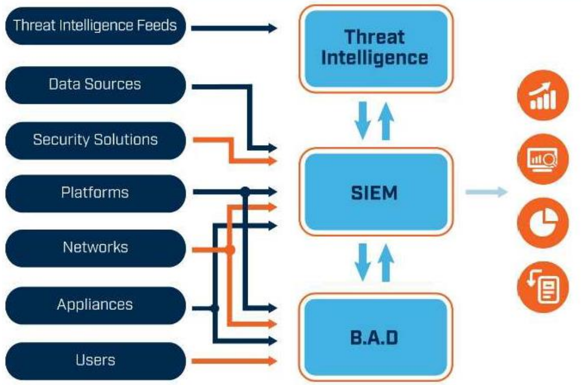
Cloud computing


OFFICE & INFRA
On-Premise & Private Cloud Service
Redundant DC & DR (Tier III)
Seamless Information Exchange
Uniform Architecture
IT HW & SW
CIM, Block Chain & other R&D
Big Data Mining & Analytics
PMU Analytics, AI & GIS Mapping
Next Generation SCADA
OT HW & SW
SIEM based SOC & NOC
Building Management System
Physical Security & Surveillance
Layered Cyber security tool
Security
Independent Office Premises
Audio/Video Collaboration platform
Zero Carbon footprint
Modern amenities & facilities
Ergonomics



Integrate IT & OT

SIEM Infrastructure - SOC



State of the art - Infrastructure

Imperatives

- 24 X 7 mission critical operations
- Expanding functional areas
- Belongingness Loyalty, Pride
- Gen Z Zeal to excel

Hygiene Factors

- Independent, Secure premises
- Zero carbon footprint
- Connected and IT enabled
- Well-equipped control room, State of the art
- Modern amenities
- Ergonomic workspace

Thank you

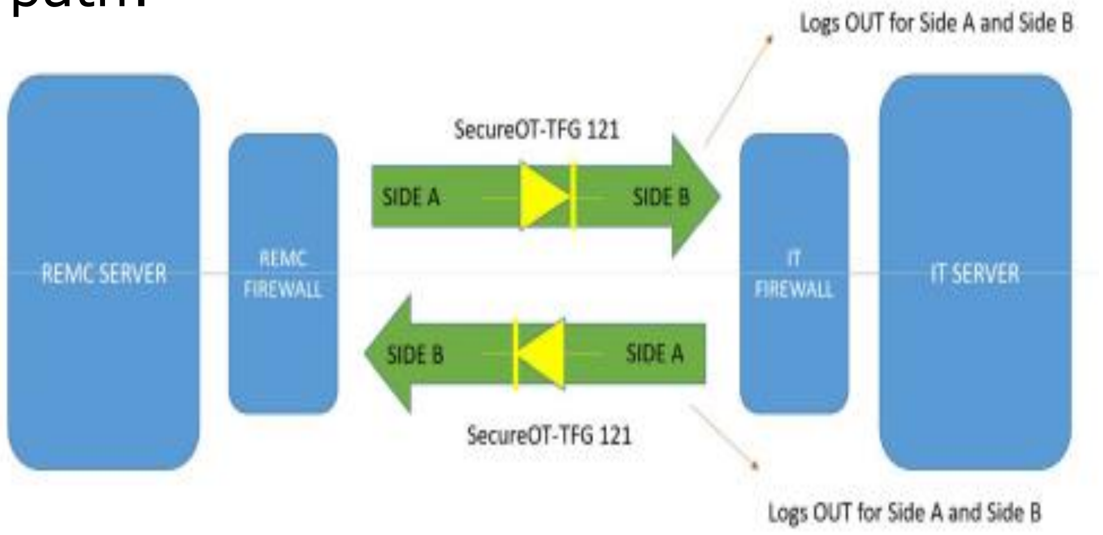
POC of Data-Diode

POC conducted successfully in NRLDC, ERLDC, WRLDC & SRLDC between IT & REMC AND IT & SCADA Network

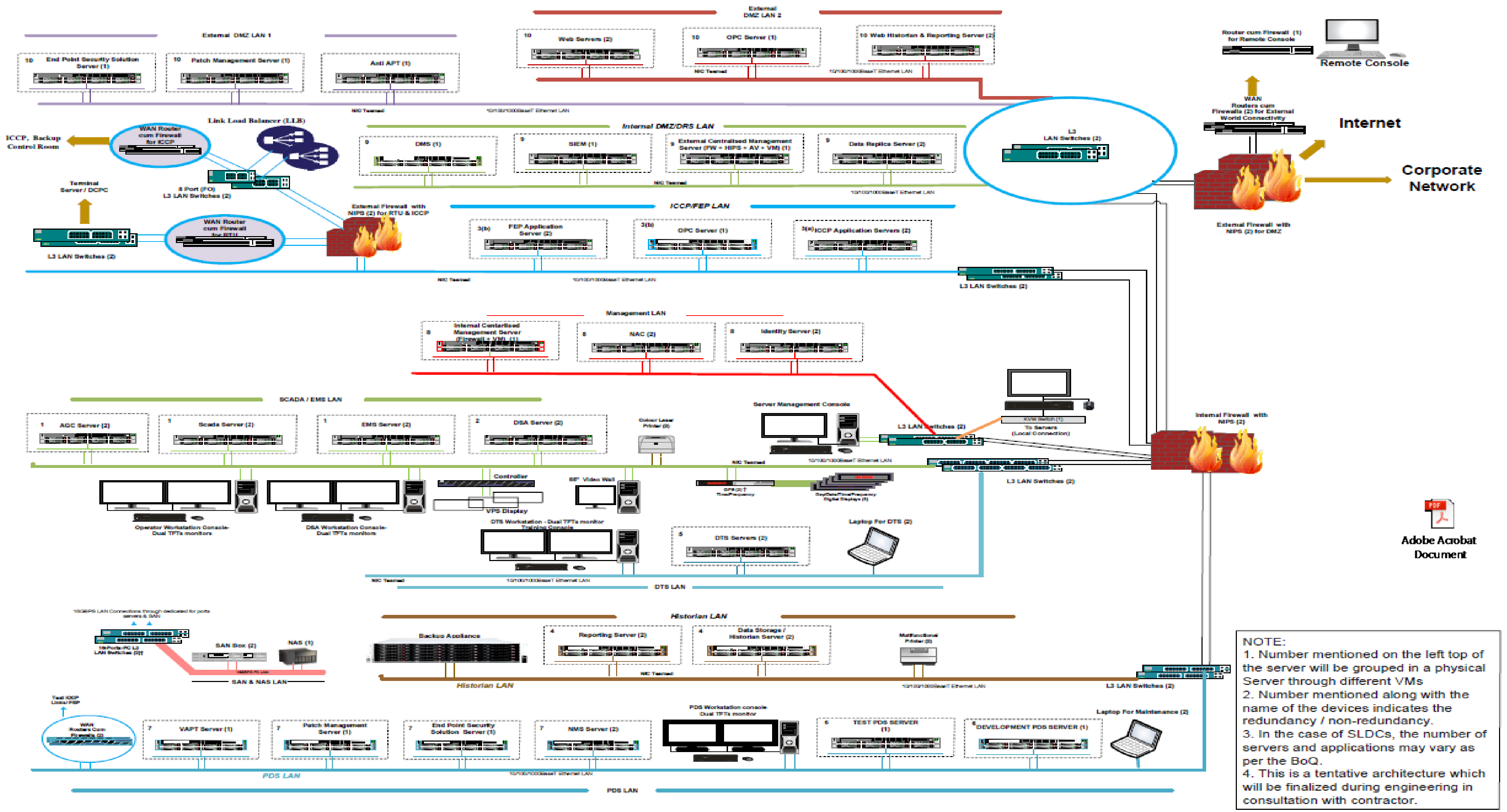
Required Files and Logs transferred unidirectionally using required protocol after establishing Air-gap between two interconnected networks

Architecture designed to establish two separate path:
-One from OT to IT
-other from IT to OT

Technical vetting under process.



ARCHITECTURE OF PROPOSED SCADA SYSTEM FOR UPGRADATION


External DMZ LAN 1
10 End Point Security Solution Server (1)
10 Patch Management Server (1)
Anti APT (1)
NIC Teamed
10/100/1000BaseT Ethernet LAN
External DMZ LAN 2
10 Web Servers (2)
10 OPC Server (1)
10 Web Historian & Reporting Server (2)
NIC Teamed
10/100/1000BaseT Ethernet LAN
Router cum Firewall (1) for Remote Console
Remote Console
WAN Routers cum Firewalls (2) for External World Connectivity
Internet
Corporate Network
External Firewall with NIPS (2) for DMZ
Link Load Balancer (LLB)
ICCP, Backup Control Room
WAN Router cum Firewall for ICCP
8 Port (FO) L3 LAN Switches (2)
Terminal Server / DCPC
L3 LAN Switches (2)
WAN Router cum Firewall for RTU
External Firewall with NIPS (2) for RTU & ICCP
Internal DMZ/DRS LAN
9 DMS (1)
9 SIEM (1)
9 External Centralised Management Server (FW + HIPS + AV + VM) (1)
9 Data Replica Server (2)
NIC Teamed
10/100/1000BaseT Ethernet LAN
L3 LAN Switches (2)
ICCP/FEP LAN
3(b) FEP Application Server (2)
3(b) OPC Server (1)
3(a) ICCP Application Servers (2)
NIC Teamed
10/100/1000BaseT Ethernet LAN
L3 LAN Switches (2)
Management LAN
8 Internal Centarlised Management Server (Firewall + VM) (1)
8 NAC (2)
8 Identity Server (2)
SCADA / EMS LAN
1 AGC Server (2)
1 Scada Server (2)
1 EMS Server (2)
2 DSA Server (2)
Colour Laser Printer (2)
Server Management Console
KVM Switch (1)
To Servers (Local Connection)
L3 LAN Switches (2)
Internal Firewall with NIPS (2)
NIC Teamed
10/100/1000BaseT Ethernet LAN
L3 LAN Switches (2)
Controller
VPS Display
66" Video Wall
GPS (2) T Time/Frequency
Day/Date/Time/Frequency Digital Displays (5)
Operator Workstation Console- Dual TFTs monitors
DSA Workstation Console- Dual TFTs monitors
DTS Workstation - Dual TFTs monitor Training Console
5 DTS Servers (2)
Laptop For DTS (2)
NIC Teamed
10/100/1000BaseT Ethernet LAN
DTS LAN
10GBPS LAN Connections through dedicated for ports servers & SAN
16-Ports-FC L3 LAN Switches (2)
SAN Box (2)
NAS (1)
16GBPS FC LAN
SAN & NAS LAN
Historian LAN
Backup Appliance
4 Reporting Server (2)
4 Data Storage / Historian Server (2)
Multifunctional Printer (2)
NIC Teamed
10/100/1000BaseT Ethernet LAN
L3 LAN Switches (2)
Historian LAN
Test ICCP Links/ FEP
WAN Routers Cum Firewalls (2)
7 VAPT Server (1)
7 Patch Management Server (1)
7 End Point Security Solution Server (1)
7 NMS Server (2)
PDS Workstation console Dual TFTs monitor
6 TEST PDS SERVER (1)
6 DEVELOPMENT PDS SERVER (1)
Laptop For Maintenance (2)
10/100/1000BaseT Ethernet LAN
PDS LAN
PDS LAN

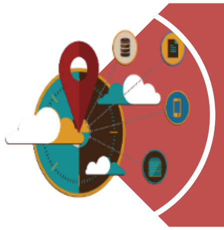
Adobe Acrobat Document

NOTE:
1. Number mentioned on the left top of the server will be grouped in a physical Server through different VMs
2. Number mentioned along with the name of the devices indicates the redundancy / non-redundancy.
3. In the case of SLDCs, the number of servers and applications may vary as per the BoQ.
4. This is a tentative architecture which will be finalized during engineering in consultation with contractor.

SALIENT FEATURES IN SCADA UPGRADATION

- 3 firewalls i.e. (External Firewall, Internal Firewall and firewall for RTU & ICCP) has been considered.
- External firewall shall have the features of Next Generation Firewall to secure the system more effectively.
- Dual authentication i.e. credential and OTP based authentication is added in firewall
- Application awareness and control for identifying application in network
- Identity awareness for giving accessing rights to user ,user groups
- Firewall shall have the Protection from Advanced Persistent Threats (APT).
- Easy integration with SIEM

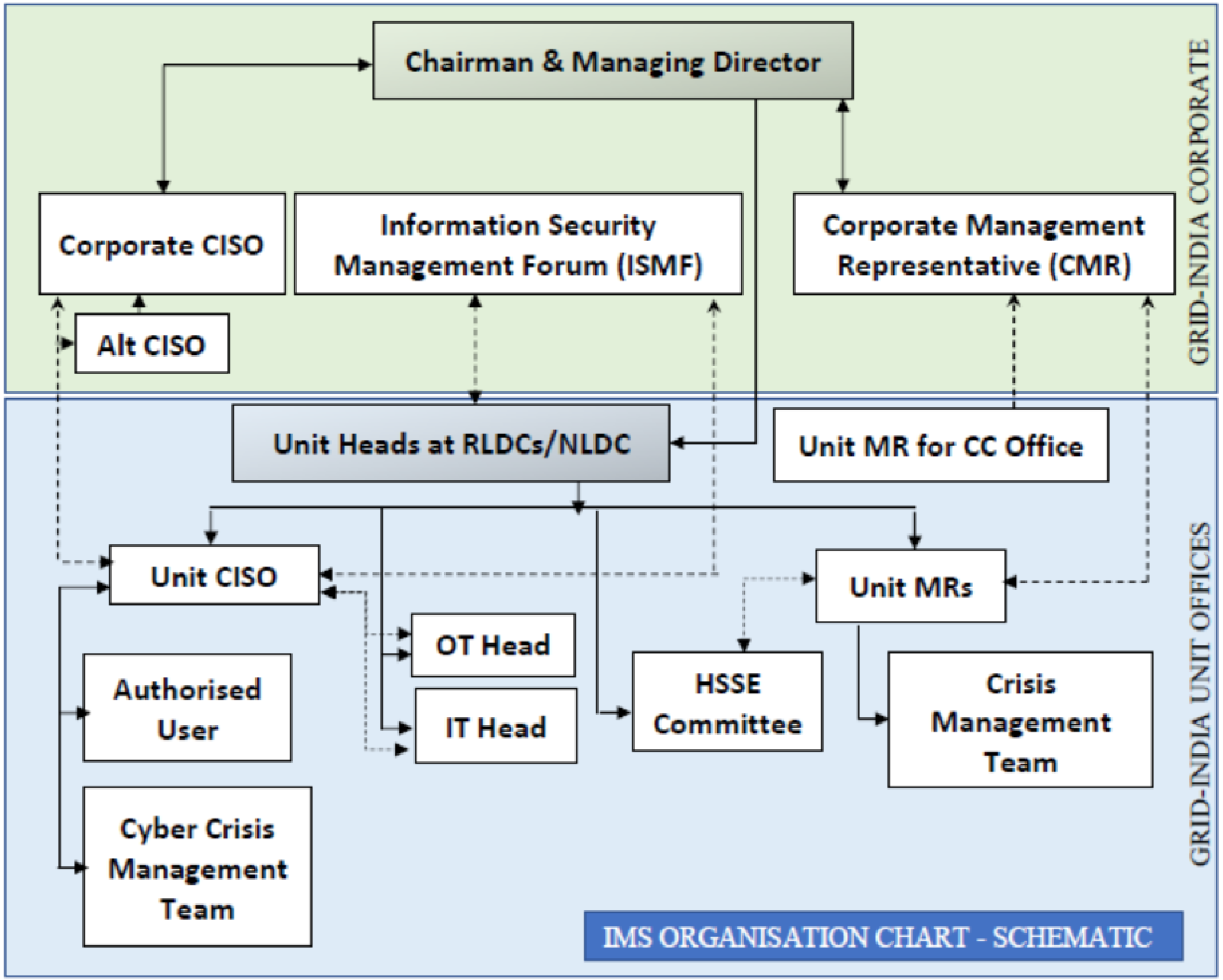
Security Information and Event management (SIEM)



centralize log management (for 3 years)

Assessment of Network

User and Entity Behavior Analytics (UEBA)



Policy Level:

Corporate MR
Unit MR
ISMF

Monitoring Level:

HSSE Team
Corporate CISO
Unit CISO

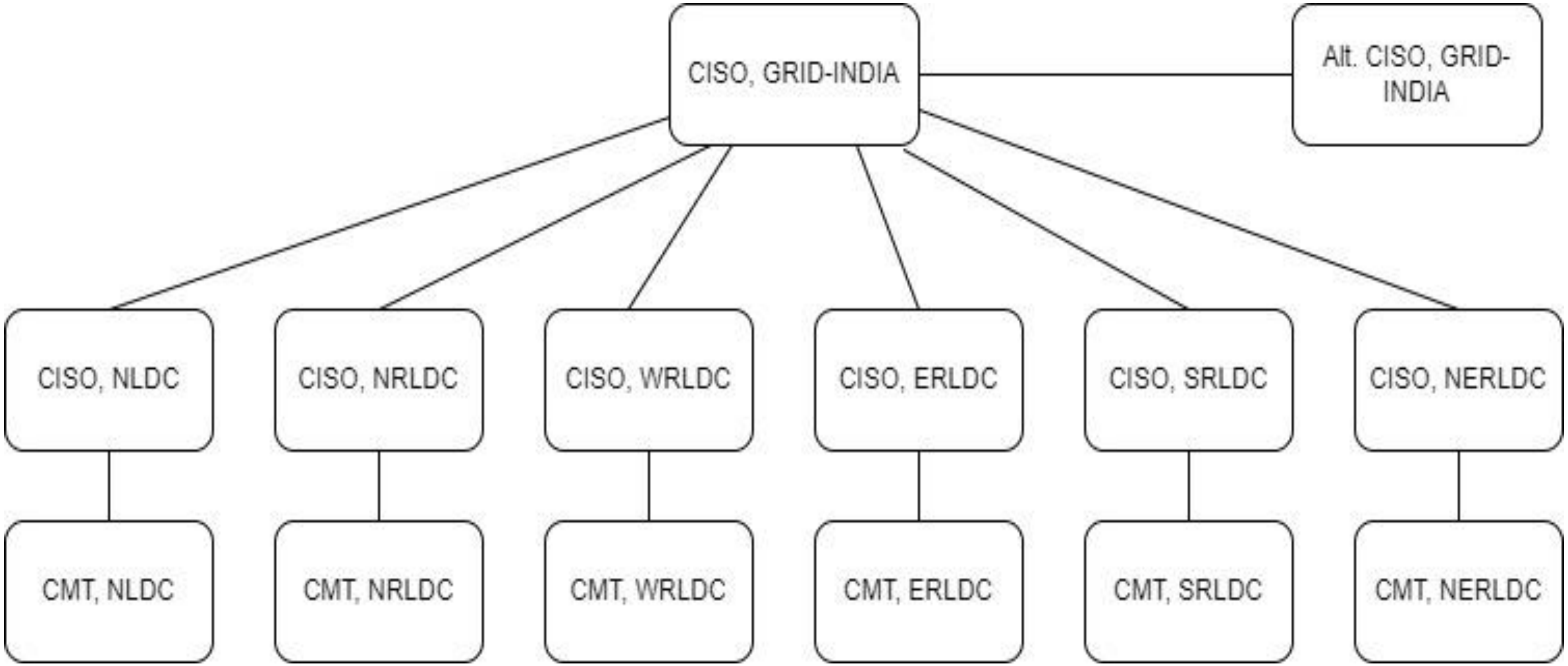
Crisis Management

CMT
CCMT

Audit:

Internal Auditor
External Auditor

Cyber Crisis Governance in GRID-INDIA


CISO, GRID-INDIA
Alt. CISO, GRID-INDIA
CISO, NLDC
CISO, NRLDC
CISO, WRLDC
CISO, ERLDC
CISO, SRLDC
CISO, NERLDC
CMT, NLDC
CMT, NRLDC
CMT, WRLDC
CMT, ERLDC
CMT, SRLDC
CMT, NERLDC