ETSI
World Class Standards

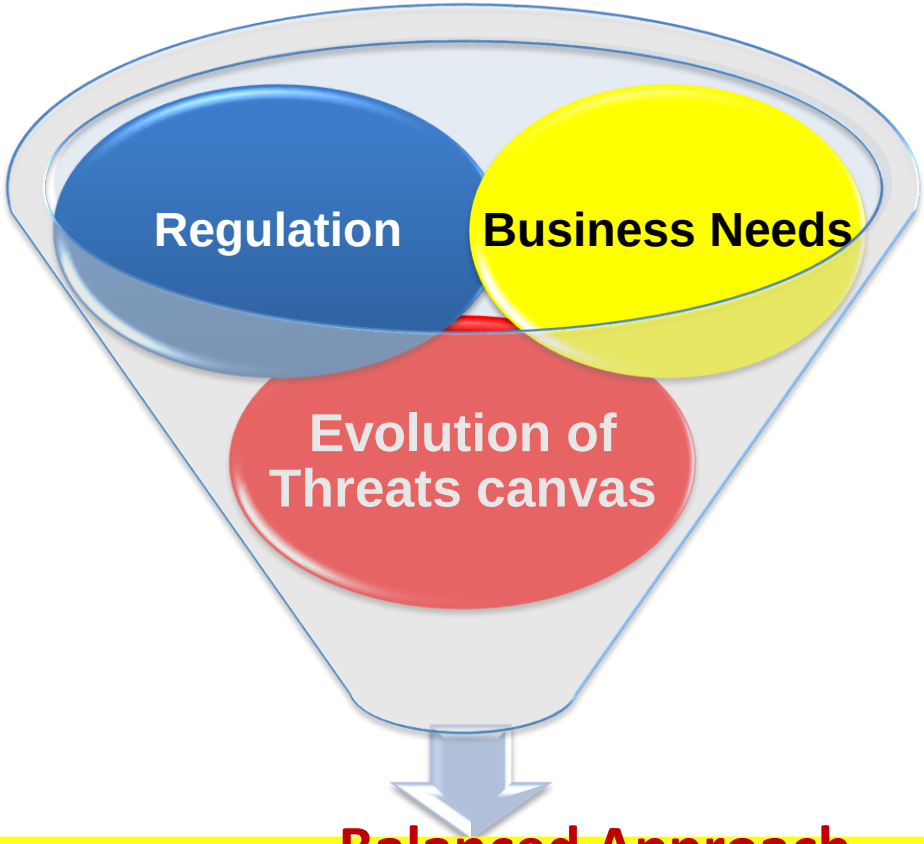
2nd Indo-European Dialogue on
ICT Standards & Emerging Technologies
4th November 2015 • Shangri-La's - Eros Hotel, New Delhi, INDIA

IN THE FRAMEWORK OF Project
SESEI
http://eustandards.in/

Security Practices - As a Mobile TSP- India

Vijay Madan - Chief Mentor, Tata Teleservices

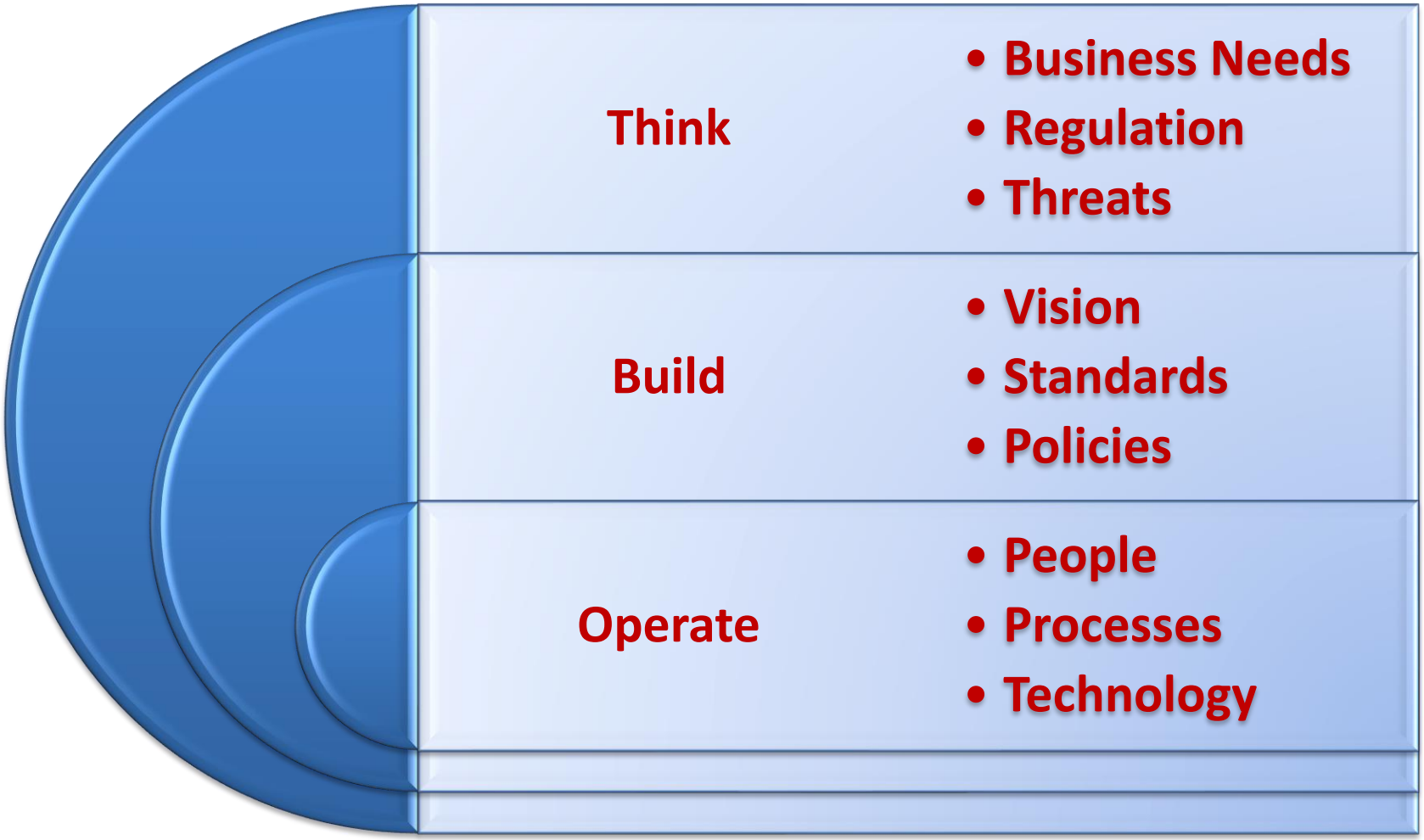
Security Approach



Balanced Approach

Complying to regulatory security guidelines, addressing business needs, to mitigate fast evolving threats canvas

Security Framework



Security Vision

Vision:

"To implement a Security Management System that protects the Confidentiality, Integrity, Availability and Privacy of the network, information of the company, our customers, business partners and other stakeholders complying with all regulatory and legal requirements".

Key Security Compliance Concerns

Securing the Business

Are **regulatory** driven security requirements adequately addressed and effectively enforced?

Is **governance** through security policies and processes adequate and working as desired?

Is **the technical infrastructure** securely designed and configured. Does it have exploitable security weaknesses?

Are the **vendor operations** secure? Are they increasing security risk?

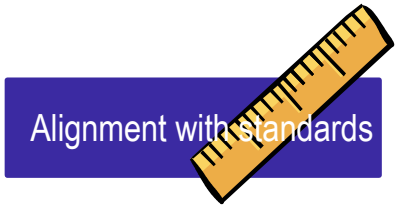
Risk Governance

Manage Risk **Achieve Compliance** **Protect**

Reputation

Security Governance Risk & Compliance

- **ISO Security /3GPP/ISO 15408/IETF/ ITU & Other Standards**



- **Information Security Policies, Procedures, Guidelines**

- **Known Risk Management Document**

- **Information Security Index**

Processes & Technology

Protect what matters!

IP, business data, privacy...

Operations Security

Enable Secured Setup

Network Security
(Firewall, VPN, Access Control, IPS/IDS, Websense, SOC, Watch Dog)

Applications Security
(Hardening Checklist, VA / PT, IDM)

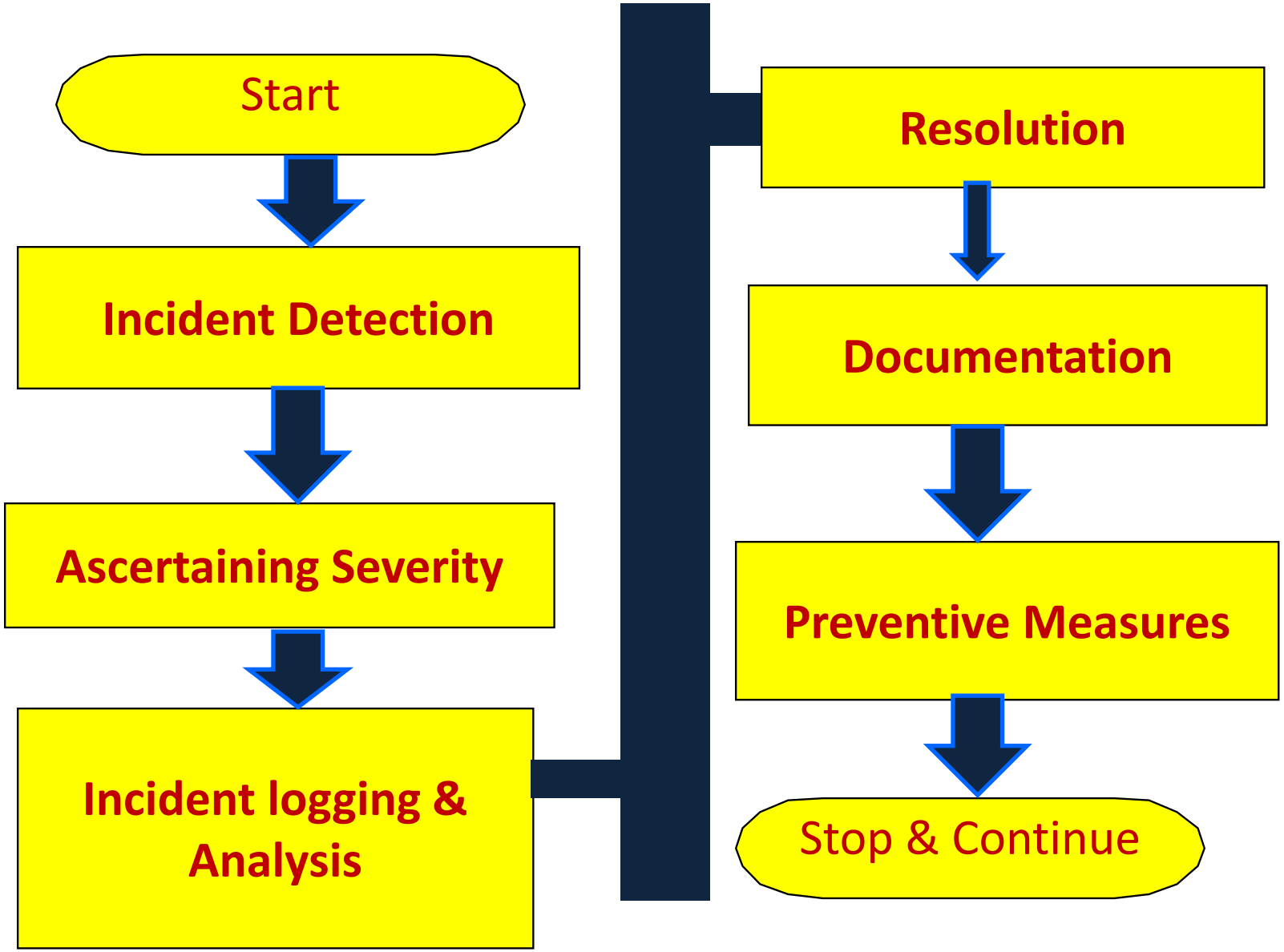
End Point Security
(Antivirus, Antimalware, Network Threat Protection, User authentications, subscriber management, SNAC)

Regulatory Compliance

Security Governance, Risk & Regulatory Compliance

7

Security Incident Management Process



Continual Improvement & Way Forward

- Compliance reporting to Senior Management
- Compliance to policies, processes , practices, procedures, guidelines & checklists
- Self compliance reporting & auto repository, efforts to integrate NW into IT SOC
- Security compliance audits
- Strengthening internal & Stakeholders awareness and placing Formal Security Organization Structure

Implementation Challenges

- Techno-economic feasibility
- Enhanced awareness amongst all stakeholders
- Structured information on applicable security standards
- Availability of tools, Testing facilities of Devices under test and Context aware Testing
- Multiple Government agencies issuing policies , Guidelines, Advisory bodies and related confusion and overlap at times
- Thin line between privacy, legal interception and related operating processes and procedures
- Huge funding requirements
- Local expertise on Cyber Security
- Indigenous research and develop programs on security
- Global Cooperation

Network Security Processes

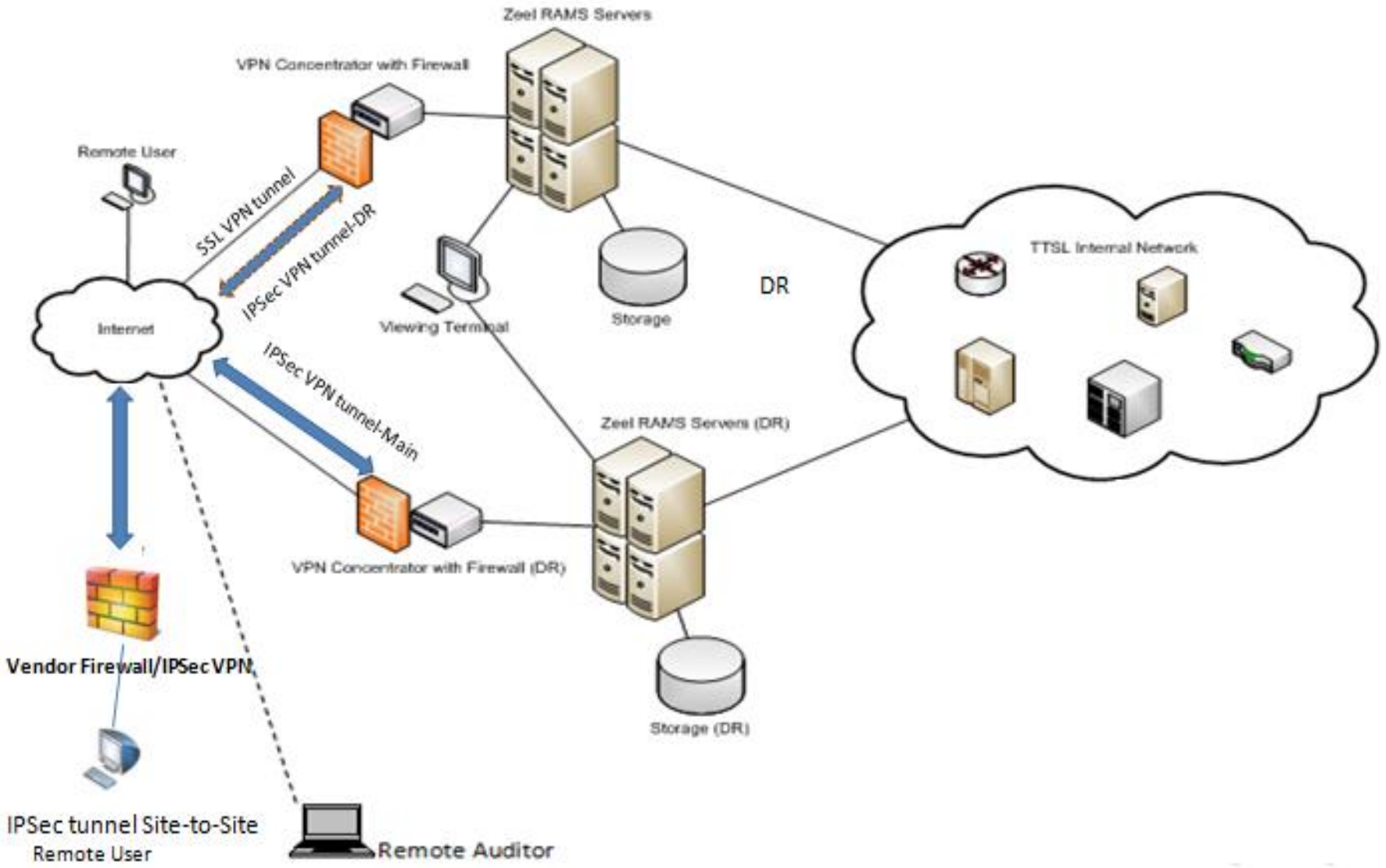
.

- **Network Access (Logical) Management Process**
  - Management of user and access control of network elements, access related logs.
  - Best Practices based Identity and Access management solution as a centralized security solution - CNOC and Network Security teams
- **Remote Access Management Process**
  - Management of remote access user using VPN Virtual Private Network, management of access logs.
- **Password Management Process**
  - Tool based management of passwords and privileges across the Nodes

Log Management

- Keeping records of Operation and Maintenance command Logs of Network Elements at Centralized Server for a period of 12 months.
- For next 24 months, Logs available in Archive mode in external Tape Drive.
- Regular backups taken

Remote Access Network Architecture



The Multi-Layered Approach
New technologies

- Getting the IP network design right
- Protecting the IP traffic in transit
- Enforcing controls in the Gateway
- Ensuring UE and HeNBs are secure
- Monitoring and Response
- Testing

Unified/Consolidated Gateway

- The “Gateway” enforcing some very important controls:
- Anti-spoofing
- Encapsulation protection
- Device to device Routing
- Billing and charging of users

IP Routing

- Architecture design and routing in the core is complex
- Getting it right is critical to security
- We see issues with this
- Needs extensive testing before production deployment

IPSec - the battle between Essential and Optional

- Difficult choice (encryptions / PKIs / DPIs) latency
- If correctly implemented will provide Confidentiality and Integrity protection
- Can also provide authentication between components
- Keeping the keys secure is not trivial and not tested
- Embedded, centralized & security servers, firewalls positioning, amongst e/h nodeBs, to / from MMEs and Gateways
- Issues of UEs, VoLTEs, Other Devices

Testing for Security

- Captive facilities
- Key protective controls for test within LTE and HetNets environment as also fail safe fallbacks
- Safe to connect and Safe to transact
- Policies and rules in the Unified/Consolidated Gateway , Protocol tests
- The implementation of IPSec or mixed others between all back-end components
- A back-end IP network as also non-IP , with well-designed routing and filtering

We sincerely believe

- Despite fears from the use of IP in 4G and beyond (security by design) , will improve security if implemented correctly
- Key controls must be correctly implemented
- Testing must be completed for validation
- Continued scrutiny is required
- Legacy systems may still be the weakest links

Looking ahead

- More air interface extensive testing is needed
- Will need co-operation from vendors/operators
- Global Cooperation. Cyber Issues.
- Private Sector the first line of defence. Enterprise and National Interests both
- Context Aware testing Vs Device testing
- “Open” testing tools will need further significant development effort
- Still lower hanging fruit, if support for legacy wireless standards remain

Some known Standards to us so far

3GPP Security Specifications 4G+ Security

- 33.401: System Architecture Evolution (SAE); Security architecture
- 33.402: System Architecture Evolution (SAE); Security aspects of non-3GPP ++

Lawful Interception

- 33.106: Lawful interception requirements
- 33.107: Lawful interception architecture and functions
- 33.108: Handover interface for Lawful Interception

Key Derivation Function

- 33.220: GAA: Generic Bootstrapping Architecture (GBA)

CONTD

Some known Standards to us so far

Backhaul Security

- 33.310: Network Domain Security (NDS); Authentication Framework (AF)

Relay Node Security

- 33.816: Feasibility study on LTE relay node security (also 33.401)

Home (e) Node B Security

- 33.320: Home (evolved) Node B Security

Areas of Submission to Regulator and Audit

Network & IT security policy implementation

Internal and external NW & IT audit reports

NW and IT hardening reports

Security authentication reports

VA & PT security tests, logs

Security Certificates reports vendors tests

Vendor agreement & Vendor Inspection

Data retention, O&M logs , software updates, change management

RAS, C-RAS – Status and compliance

LBS status

CDRs

Audit reports

Regulator may visit and inspect & for further engagement

Tools used, used, methodology, PoCs

Thank You for all your kind patience and consideration

Have a Wonderful Time Ahead – Stay connected and Guide us

2nd Indo-European Dialogue on
ICT Standards & Emerging Technologies

4th November 2015 • Shangri-La's - Eros Hotel, New Delhi, INDIA