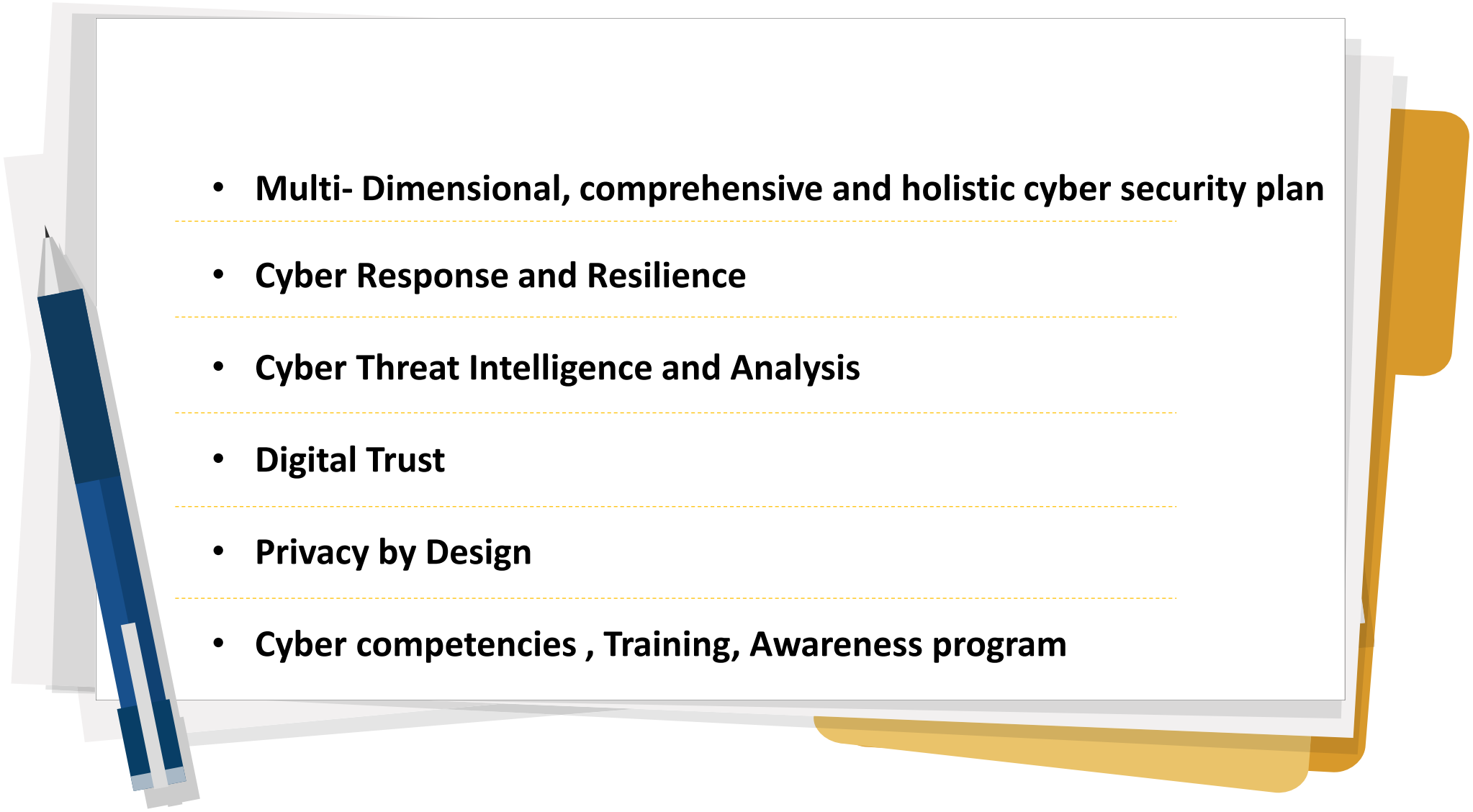
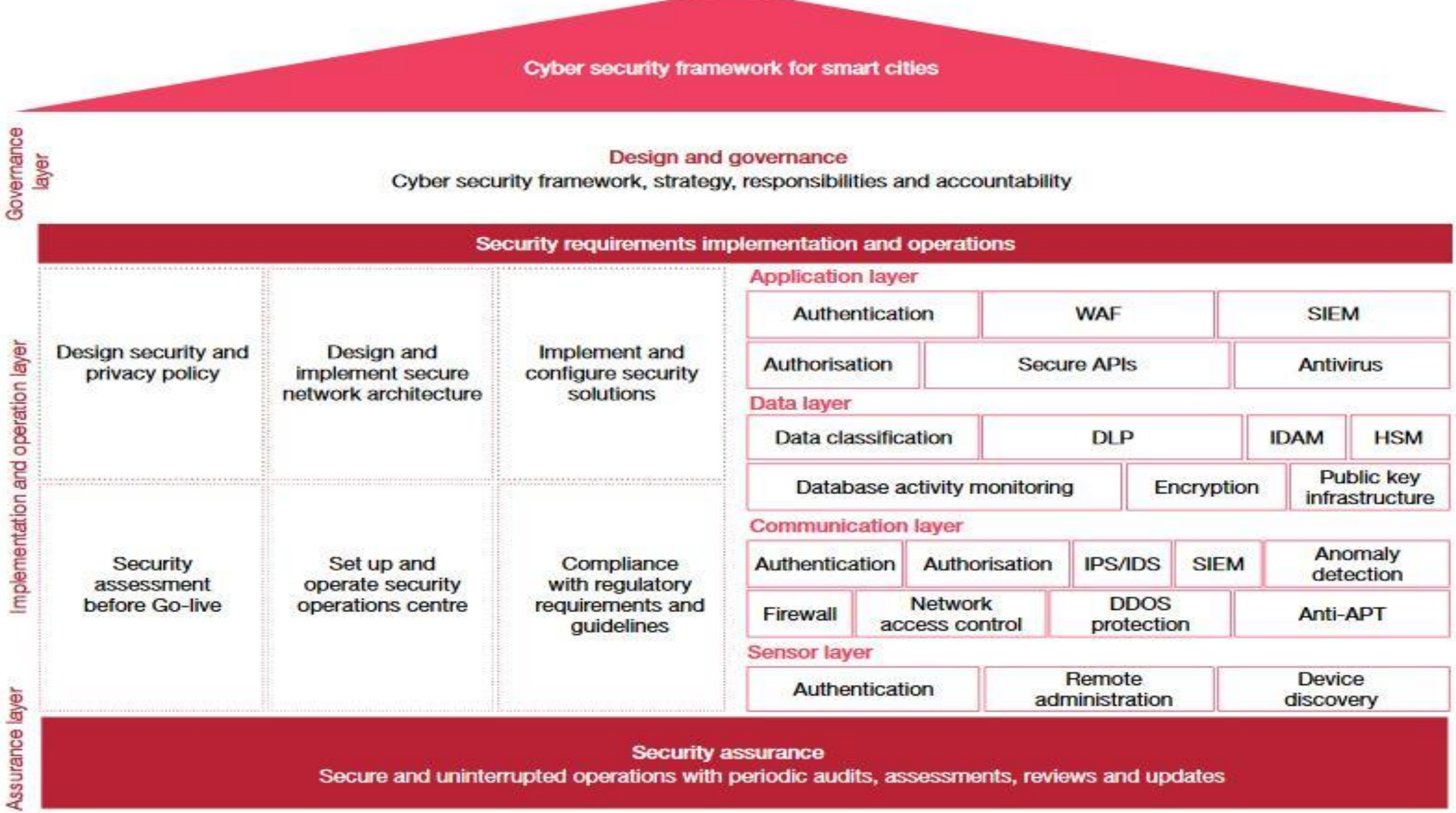
# Smart City
# Cyber Security, Privacy

Rama Vedashree
CEO, DSCI

# LEVERS OF SMART CITY CYBER SECURITY FRAMEWORK



- Multi- Dimensional, comprehensive and holistic cyber security plan
- Cyber Response and Resilience
- Cyber Threat Intelligence and Analysis
- Digital Trust
- Privacy by Design
- Cyber competencies , Training, Awareness program




Source: DSCI- PWC Report " Creating Cyber Secure Smart Cities"

# Cyber Security Requirements of a Smart City – Products and Services

Based on MoUHA Guidelines

| ICT Layers in Smart City Architecture | *Products* | *Services* | Architectural Objectives |
|---|---|---|---|
| Application | Authentication, API Management, WAF<br>Authorization, Identity & Access Management<br>Security Incident and Event Management, SSO | Intra App Encryption, Hosting<br>RBAC, Zoned Architecture, DMZ<br>Incident Monitoring & Response, VAPT | Software Analysis, Federated Access<br>API Service Orchestration<br>Web Server Protection<br>Citizen Security |
| Data | Data Leak Prevention, Data Classification<br>Privacy Enhanced Threats, Data Layer as Gateway | Defining Data Flows, Zoned Architecture<br>Data Encryption, Binding Data Flows to Apps | Data Visualization, Data Privacy<br>Data Segmentation<br>Secure Binding, Secure Analytics |
| Communication | Authentication, Authorization, Firewall<br>IDS / IPS, DDoS protection, Anomaly Detection<br>SIEM, Advanced Persistent Threat Solution | RBAC, Network Segmentation<br>Network Zoning, Gateway Encryption | Data Diodes, Industrial Firewalls<br>Deep Packet Inspection<br>Unidirectional Gateways, Pattern Recognition |
| Sensing | Authentication, Authorization, Device Discovery<br>Dynamic Provisioning, Remote Administration | Network Segmentation, Network Binding<br>Hardening, Encryption, SSL | IIoT/OT Discovery, Baseline Monitoring<br>Device Centric Authentication<br>Monitor Signals, Securing PLCs |

**ISO27001 | ISO22301 | ISO37120 | ISO27017 | ISO27018 | BSI PAS 180,181,182 | 3GPP | PEAP**

Reference URL: Cyber Security Model Framework for Smart Cities

# Minimum Cyber Security Requirements of a Smart City – Products and Services

Based on MoUHA Guidelines

| ICT Layers in Smart City Architecture | *Products* | *Services* | Architectural Objectives |
|---|---|---|---|
| Application | Authentication, API Management, WAF<br>Authorization, Identity & Access Management<br>Security Incident and Event Management, SSO | Intra App Encryption, Hosting in India<br>RBAC, Zoned Architecture, DMZ<br>Incident Monitoring & Response, VAPT | Software Analysis, Federated Access<br>API Service Orchestration<br>Web Server Protection<br>Citizen Security |
| Data | Data Leak Prevention, Data Classification<br>Privacy Enhanced Threats, Data Layer as Gateway | Defining Data Flows, Zoned Architecture<br>Data Encryption, Binding Data Flows to Apps | Data Visualization, Data Privacy<br>Data Segmentation<br>Secure Binding, Secure Analytics |
| Communication | Authentication, Authorization, Firewall<br>IDS / IPS, DDoS protection, Anomaly Detection<br>SIEM, Advanced Persistent Threat Solution | RBAC, Network Segmentation<br>Network Zoning, Gateway Encryption | Data Diodes, Industrial Firewalls<br>Deep Packet Inspection<br>Unidirectional Gateways, Pattern Recognition |
| Sensing | Authentication, Authorization, Device Discovery<br>Dynamic Provisioning, Remote Administration | Network Segmentation, Network Binding<br>Hardening, Encryption, SSL | IIoT/OT Discovery, Baseline Monitoring<br>Device Centric Authentication<br>Monitor Signals, Securing PLCs |

**ISO27001 | ISO22301 | ISO37120 | ISO27017 | ISO27018 | BSI PAS 180,181,182 | 3GPP | PEAP**

Reference URL: Cyber Security Model Framework for Smart Cities

# Key features  of the Smart City Cyber Security Policy

**1**.Protect sensitive information stored with city, state government departments and agencies

**2.**Protect the critical infrastructure

**3.**Create risk assessment structure to manage risks in alignment with criticality of the information resource

**4**.Continuously improve the cyber response capability

**5.**Capacity building in cyber security of city administration, state government departments, agencies, commissions and Law Enforcement Agencies

**6.**Facilitate cyber risk awareness to its operations and citizens on online safety and security

# Highlights of the Smart City Cyber Security Policy

## City Organization Structure

- The city shall appoint a **City Chief Information Security Officer**
- **Each city organisation** to have a cyber security management team that would be responsible for Identification of city's organisation security goals and integrate them into the appropriate processes

## Security Implementation

- The Information Security Officer of each City Organisation to establish **standard operating procedures (SOPs**) as per industry standards and best practices.
- Every city organisation to establish **a cyber security response team** operating in conjunction with state IT Department Security Team and CERT-In

## Governance

- **Annual audit** to measure the security posture in-line with the **city policies, procedures, cyber security framework and other regulatory requirements** and readiness assessment to be conducted
- Policy recommends that all **SMBs** operating in city to adopt fundamental Internet security practices,