

Conformity Assessment Requirements and Conformity Assessment Framework for eGovernance

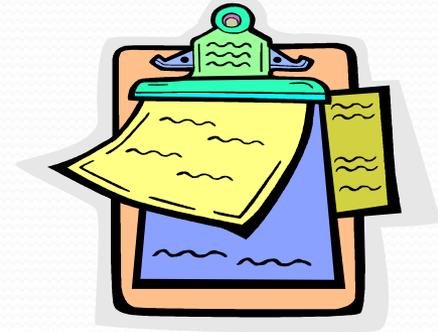
Mitali Chatterjee
Government of India
STQC, Department of Electronics and IT

**NIST-SIT Workshop with India on ICT
Gaithersburg, Maryland, USA**

September 15-19 2014

Contents

- Conformity Assessment and its Goals
- Types of Conformity Assessment
- eGovernance – the characteristics & challenges
- eGovernance – the risks and concerns
- Need for Conformity Assessment Framework (CAF) for eGovernance
- CAF for eGovernance – principles and objectives
- Positioning of CAF in eGovernance
- CAF Quality Gates (Good Governance >>>> eGovernance >>>> Secure eGovernance >>>> Quality eGovernance)
- Secure eGovernance
- eGovernance Organization Conformance – a representation



Conformity Assessment (CA)

- **Conformity Assessment (CA)** is any activity which results in determining whether a product or other object corresponds to the requirements contained in a specification.
- Officially definition of CA is the “demonstration that specified requirements relating to a product, process, system, person or body are fulfilled”.
- **Goals of Conformity Assessment**
 - The “One-one-one” principle: one standard, one test accepted everywhere, one mark where relevant
 - Safety and Security
 - Performance
 - Its effectiveness
 - Its quality
 - Its efficiency
 - Its economic use of material and energy
 - Its effect upon the environment
 - Interoperability
 - Meet the goals of 1st, 2nd and 3rd party Conformity Assessment



Conformity Assessment (CA)

The Parties

Conformity Assessment can be conducted by:

- First party – seller or manufacturer
- Second party – purchaser or user
- Third party – an independent entity that has no interest in transactions between the 1st and 2nd parties
- Government – has a unique role in regulation, but is the second party in procurement

Types of CA Activities

- Testing
- Inspection
- Certification
- Surveillance
- Accreditation



Typical Use of different types of CA

Testing (1st, 2nd or 3rd Party CA)

- Used when the critical characteristics can be evaluated via measurement under specified conditions.
- Testing can be carried out on samples that represent production for the purpose of determining conformity.
- May be an element of a suppliers' declaration or certification system.
(ex. Testing of ICT products for Conformance to Quality, Safety, Security Specifications)

Inspection (1st, 2nd or 3rd Party CA)

- Used when the critical characteristics can be evaluated via physical examination or measurement.
- May be an element of a certification system.
- May be used to ensure that all parts of a system have been properly installed
(ex. code inspection)

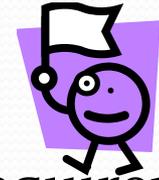
Certification (3rd Party CA)

- Used when the risks associated with non-conformity are moderate to high.
- Includes evaluation, compliance decision, attestation of conformity and some form of surveillance or follow up.
- Always conducted by a third party



Typical Use of different types of CA

Management System Certification (3rd Party CA)



- Used to provide an assurance that a process meets requirements
- Not a silver bullet for product or service quality or compliance
- Process includes initial assessment of written management system procedures and implementation followed up by actual audit
- Surveillance Audits are typically used for monitoring
- Scope of management system is key to meeting the objectives
- Useful for process critical applications, quality (ISO 9000), security (ISO 27000), service management (ISO 20000) and environmental (ISO 14000) management systems.
- Sector specific applications are generally the most effective such as ISO 13485 (medical devices), TL 9000 (Telecom) and TS 9000 (automotive).

Typical Use of different types of CA

Surveillance

- Used to ensure/enhance ongoing conformity.
- Key part of **certification** or **registration** system.
- Inspection, testing and audits are among commonly used methods
- Frequency and rigor need to be balanced with the costs (direct and indirect) and degree of assurance required
- Typically resource intensive



Accreditation

- Used to assess and ensure/enhance ongoing conformity assessment bodies and programs for competence, management and technical requirements.
- Used to attain needed confidence in laboratory **testing** operation and results.
- Used to attain needed confidence in **certification** system.

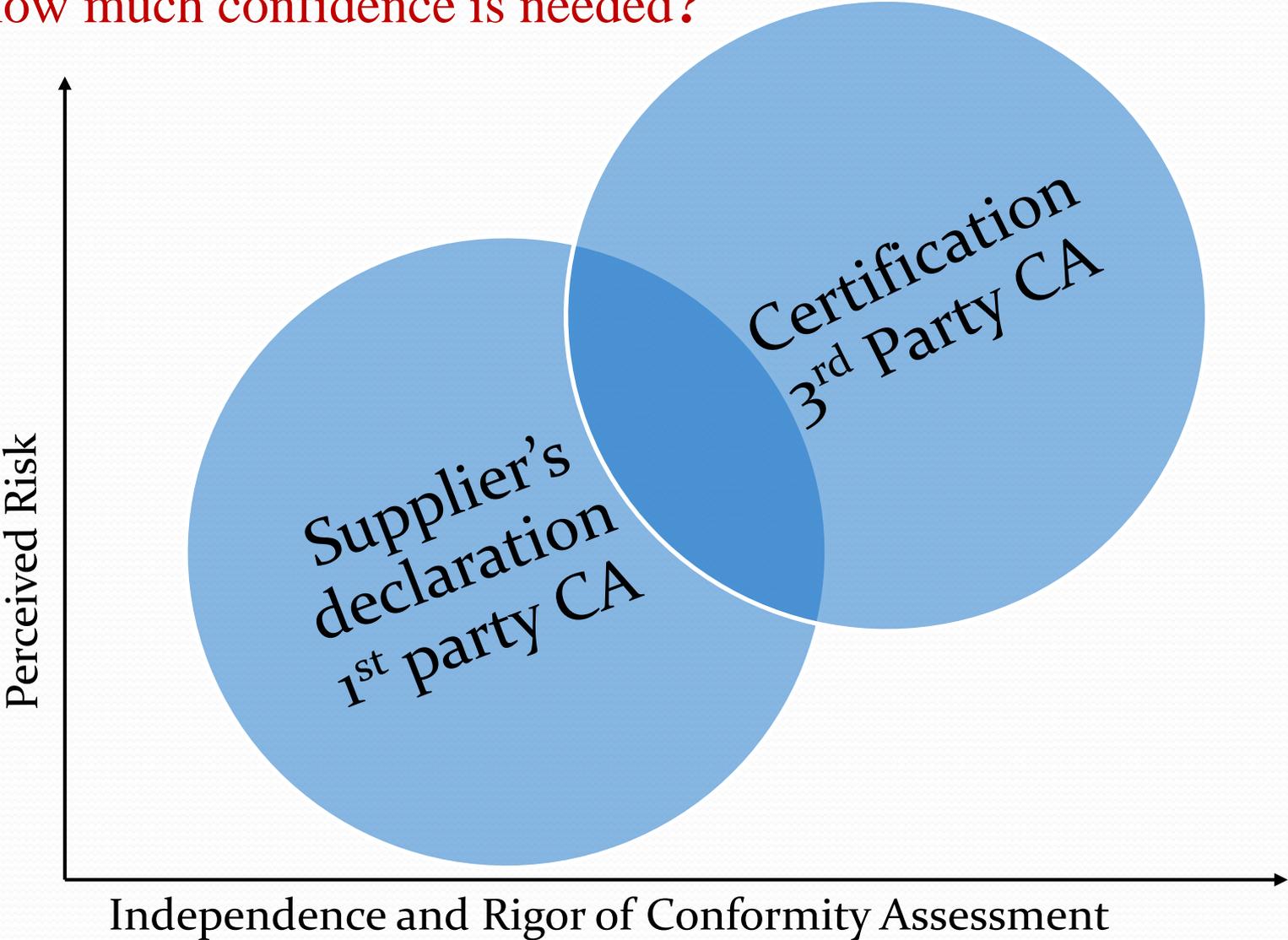
Factors in CA System Design

- The risks associated with non-compliance should be proportional to the **rigor** and **independence** of the CA system.
- System **over-design** will add too much cost.
- System **under-design** will result in too little confidence of compliance.
- **Penalties associated** with non-compliance may reduce the needed rigor and independence of the conformity assessment system.
- **Timely mechanisms** that effectively remove non-compliant products from the market may also reduce the needed rigor and independence of the system.



Risk and Conformity Assessment

How much confidence is needed?



eGovernment - The Invisible Government & its challenges

The Invisible Government - characteristics

- Virtual and always available
- Since enabled by ICT , it carries risks and concerns of ICT



© Can Stock Photo - csp1274302

Challenges

- **Policy Makers/Administrators** : Fulfillment of objectives
- **Solution Provider** : Completion of milestones
- **Users** : System is working rightly
- **The funding agencies** : Achievement of output and outcome
- **Procurement bodies** :
 - Adherence with basic principles of public procurement
 - “what was asked” versus “what is supplied”
 - Release of payment



e-Governance : Risks & Concerns



Risk

- **Economic Risk**

- Huge investment
- Cost of technology and knowledge is high

- **Technological Risk**

- High obsolescence rate
- Dependability/Reliability of technology
- Use of right technology

- **Social Risk and User acceptability Risks**

- Solutions are citizen and business centric and touch upon sensitive service oriented issues
- High expectation

Concerns

- **Users**

- Whether government services will be available in a convenient way as promised

- **Policy Makers and Administrators**

- Whether objectives of eGovernance are being achieved (Transparency, availability of service, compliance with government rules, procedures, decisions and regulations)

- **Solution/Service Provider**

- That system meets the requirements of RFP

Conformity Assessment Framework (CAF) to address the Challenges of eGovernment



CAF for eGovernance was developed with the objective to

Provide an indicator of the **degree of compliance** of the solution to the requirements as defined in RFP/contract documents by means of objective evaluation

To ensures that

- **End-to-end systems** and its **components** are conforming to the requirements of RFP/contract
- Solutions are complying with **legal** and **regulatory** requirements
- Users are **satisfied** with the services

Based on the principles of

Proportionality, Accountability, Consistency (Reproducibility and Repeatability of evaluation results) , **Transparency** and degree of **Compliance**

Conformity Assessment Framework– Business of Confidence to stakeholders

To Administrator

- Achieving his vision
- Addressing his concern
- Strategies handling of complex problems.

To Solution Providers

- A well accepted approach based on ISO standards.
- Common methodology and criteria - fair playground for all solution providers
- Independent third party.

To Users

- On usability of the solutions as a cross section of users are involved in usability test of evaluation.
- On functionality of these solutions - all functionality are tested and evaluated as a functionality and workflow (scenario).
- On security of these solutions - functional security are ensured through exhaustive testing

To Funding Agencies

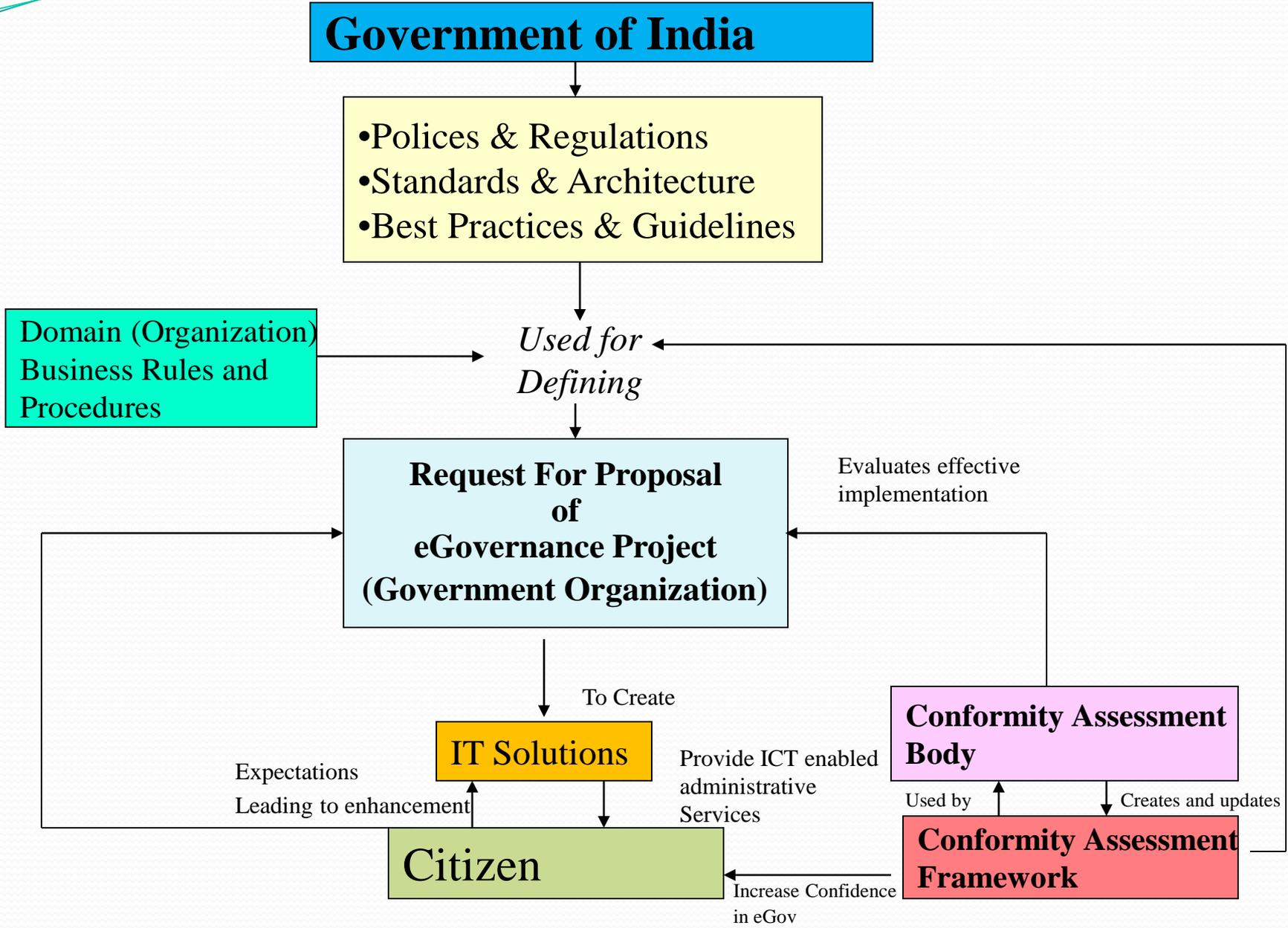
- Assurance for release of funds

To Procurement Bodies

- Confidence and assurance on products produced



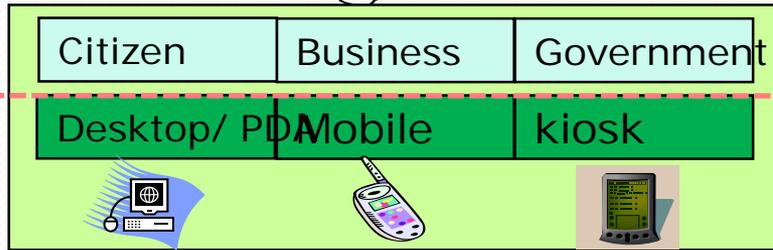
Positioning of Conformity Assessment Framework



eGovernance architecture



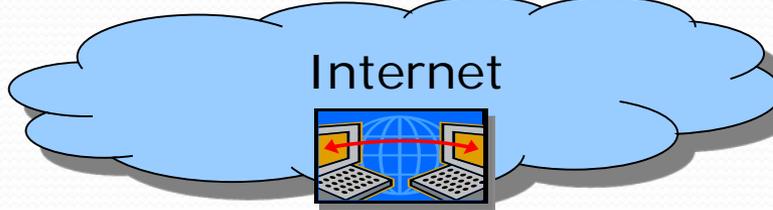
User Layer



Service /Access Layer

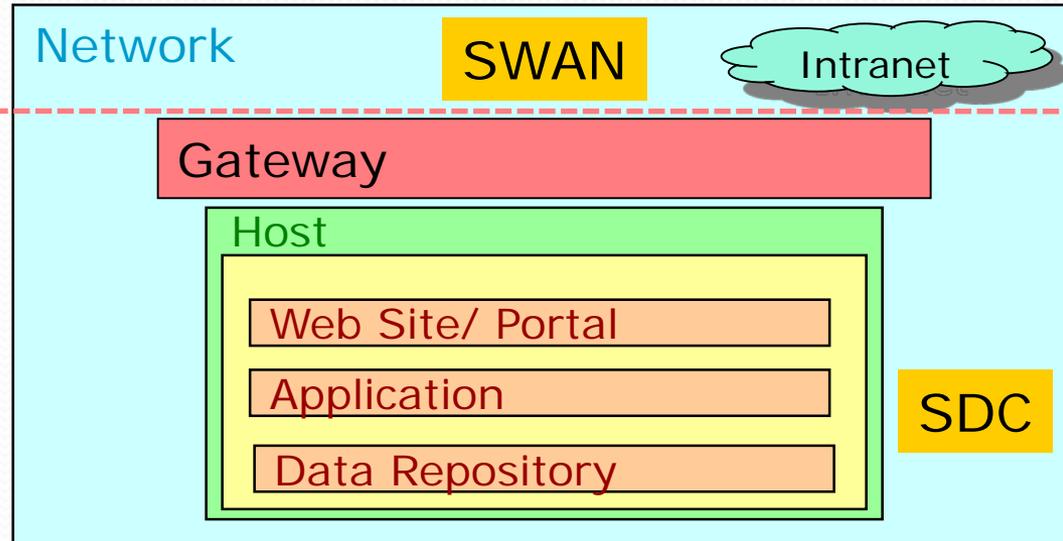
CSC

Transport Layer



Technology Layer

IT Asset Layer

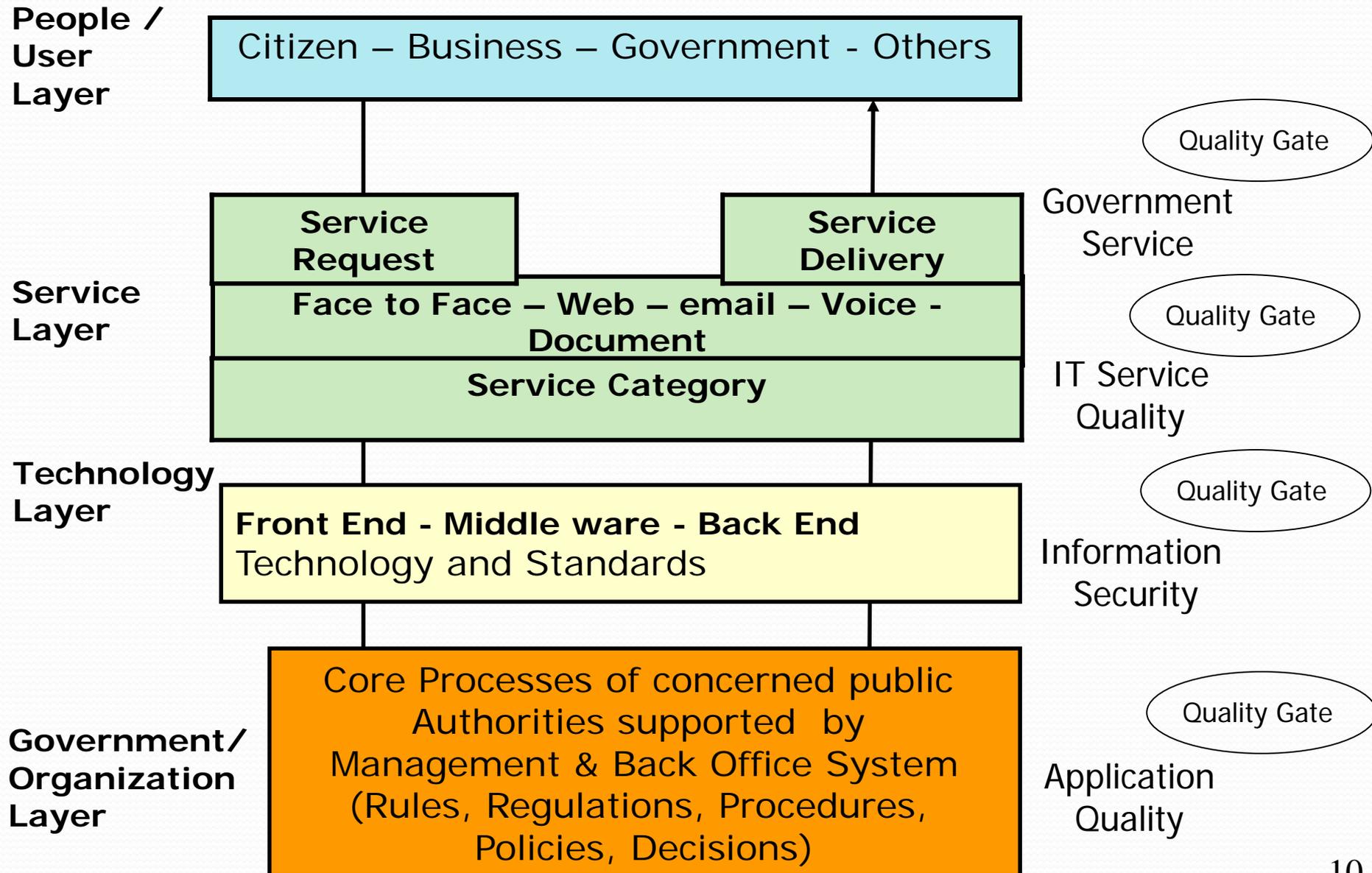


Government/ Organization Layer

Service Organization (Government)



eGovernance architecture: Gates for Conformity Assessment



Citizens/Business /Government

Requests

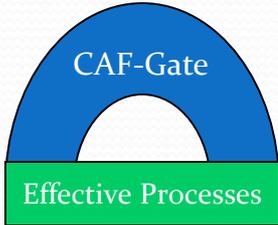


Service

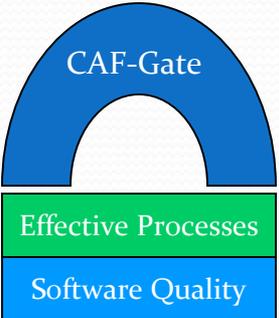


Government
Policies, procedures, decisions, legislation

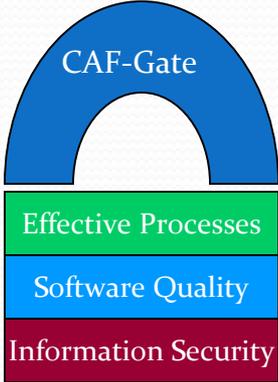
Governance



Good Governance



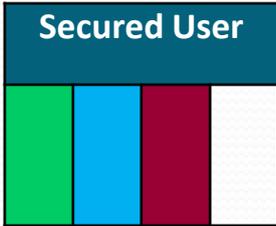
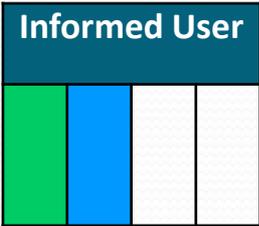
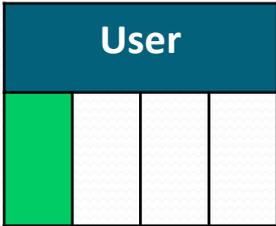
eGovernance



Secure eGovernance

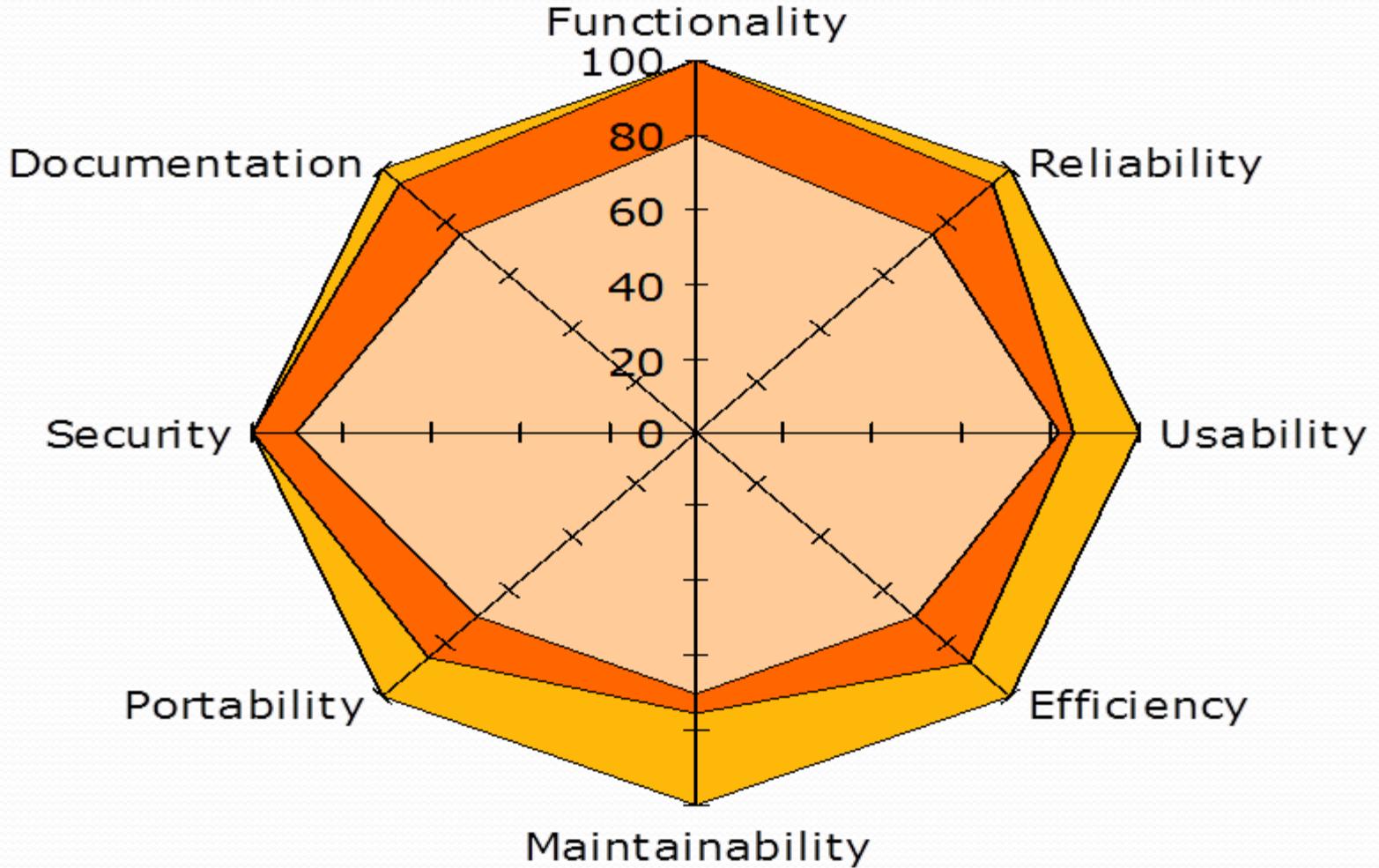


Quality eGovernance



Quality Gate : Software Quality

Illustration : Distribution of Quality Characteristics



Information Security – Why is it an issue for eGovernance?

Need for full access, an open environment where users have lots of great information and services and where one can interact electronically

Need to button the system down, close open passageways to unauthorized hackers, crackers and provide access to only authorized users

One mission two objectives !!

Specific characteristics of eGovernance applications which makes Security an important issue for eGovernance

- Dealing with highly sensitive citizen's and business data
- National Security
- Laws relating to Information Security
- Mostly remote access
- High degree of information sharing
- Consequences of security breach can be detrimental

Challenge : Struggle for balance



eGovernance Security Assurance

It has two distinct actions

- **Enabling actions** Directives / Standards & Guidelines/ Best Practices / Training & Awareness
- **Endorsing actions**

Assessments, Testing & Certification
covering **Product, Process & People**

– includes specific services such as

- Assessments and Audits
- ISMS certification
- Common Criteria (CC) Product Evaluation and Certification
- IT Security Testing
- Role Specific Manpower Training



eGovernance Security Assurance

Enabling actions

Directives : Policy directives on data security and privacy protection – Compliance, liabilities and enforcement (e.g. Information Technology Act, National Cyber Security Policy)

Standards & Guidelines :

- ISO 27001, ISO 15408 (Common Criteria)
- CERT-In Guidelines
- Information Security Assurance Framework and Guidelines for selection & implementation of security controls (E-SAFE)

Best Practices

- Information Security Best Practices (ISO 27002, OWASP Best Practices)

Awareness

- Nation wide awareness campaigns
- Awareness Programs on
 - Need for Information Security Controls Best Practices
 - Common Criteria Standards
 - Network Security Requirements
- Workshops on
 - Information Security Risk Assessments
 - Documentation Development
 - Network Security Assessments
 - Common Criteria Evaluation and Certification



eGovernance Security Assurance



Endorsing actions

Assessments and Audits

- For ascertaining compliance to defined systems

ISMS certification

- ISO 27001 Certification

Common Criteria (CC) Product Evaluation and Certification

- Establishment of CC Testing laboratories in Government, Public and Private Sectors
- Launching of the National CC Certification Scheme

IT Security Testing / Assessments / Auditing

- Establishment of Accredited Security Testing Lab : STQC's Software Testing Labs at Bangalore and Kolkata are accredited by A2LA (American Association for Laboratory Assessment) for Application Security Testing, Penetration Testing, Vulnerability Assessments, Network Assessment
- Security Testing by CERT-In and empanelled partners

Role Specific Manpower Training

- ISMS Auditors, ISMS Implementation Managers
- Network Security Managers
- Ethical Hackers

eGovernance Security Assurance Framework and Guidelines (eSAFE)



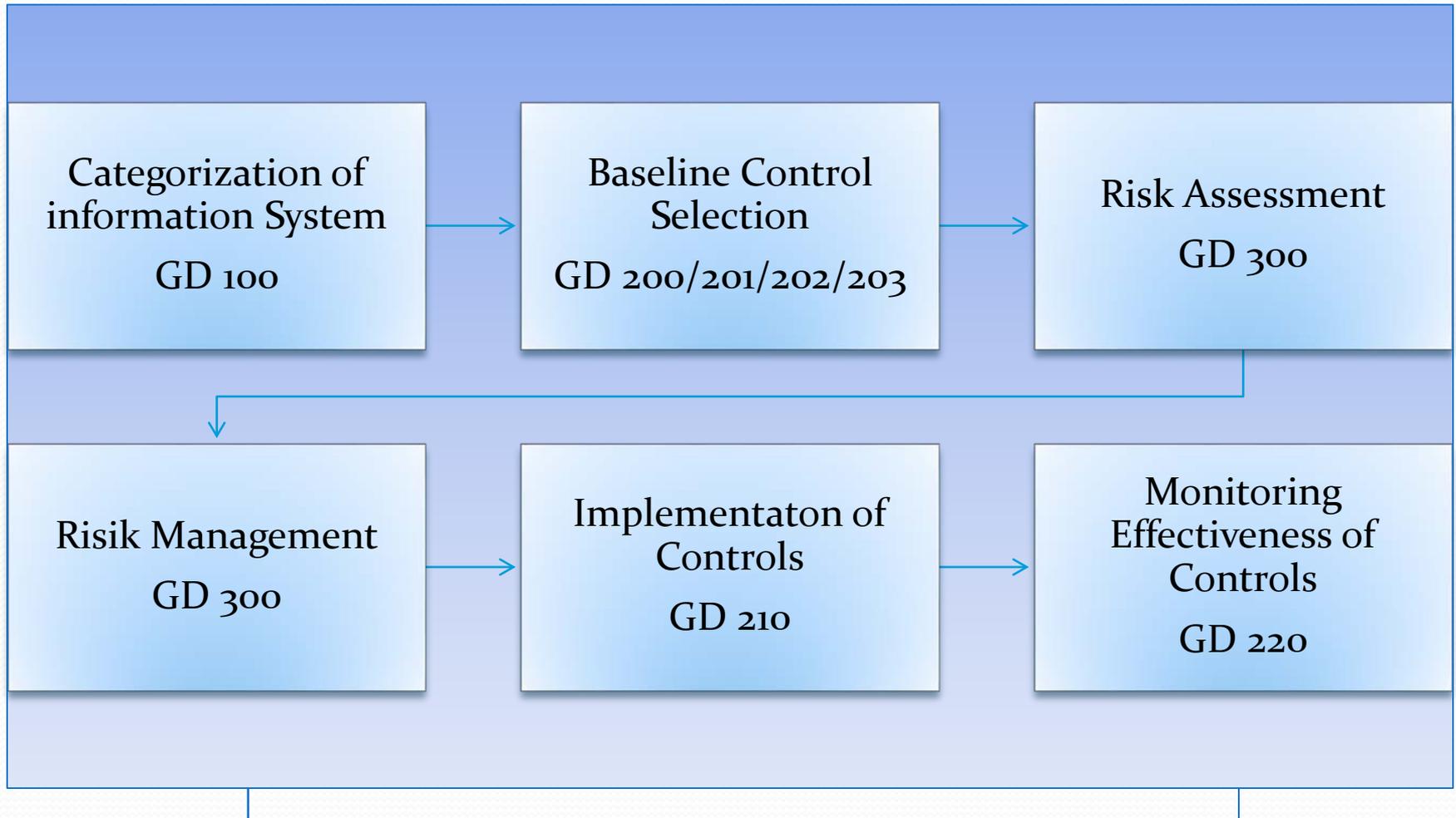
Covers three kinds environment, depending on types of **risks** & related eGovernance mission impact

- **Low risk** - In general, the environment caters to providing **information** to users
- **Medium risk** - In general, the environment caters to providing **information** to users and allowing some amount of **interaction** including non-commercial transactions
- **High risk** - In general, the environment caters to providing **sensitive information** to users, allowing **interaction** and commercial **transactions** including on-line payments

Security control **emphasis** depends on the kind of environment

- Low risk : **'Awareness'** – know your security concerns and follow best practices
- Medium risk: **'Awareness & Action'** – Proactive strategies leave you better prepared to handle security threats and incidents
- High risk: **'Awareness, Action and Assurance'** – Since security failures could be disastrous and may lead to unaffordable consequences, assurance that the security controls work when needed most is essential.

eGovernance Security Assurance Framework (eSAFE)



Security Control Focus

- Perimeter defense
- Authentication
- Management & Monitoring
- Configuration
- Interconnection through cables
- Interconnection through wireless LAN

Infrastructure Security

- Security Policy
- Outsourcing Management
- Operational Procedures
- Protection from malware
- Back-up and recovery
- Patch and update Management
- Physical & Environmental Security
- Training & Awareness

Operations & Management

- Deployment & use
- Application Design
- Data Storage & Communication

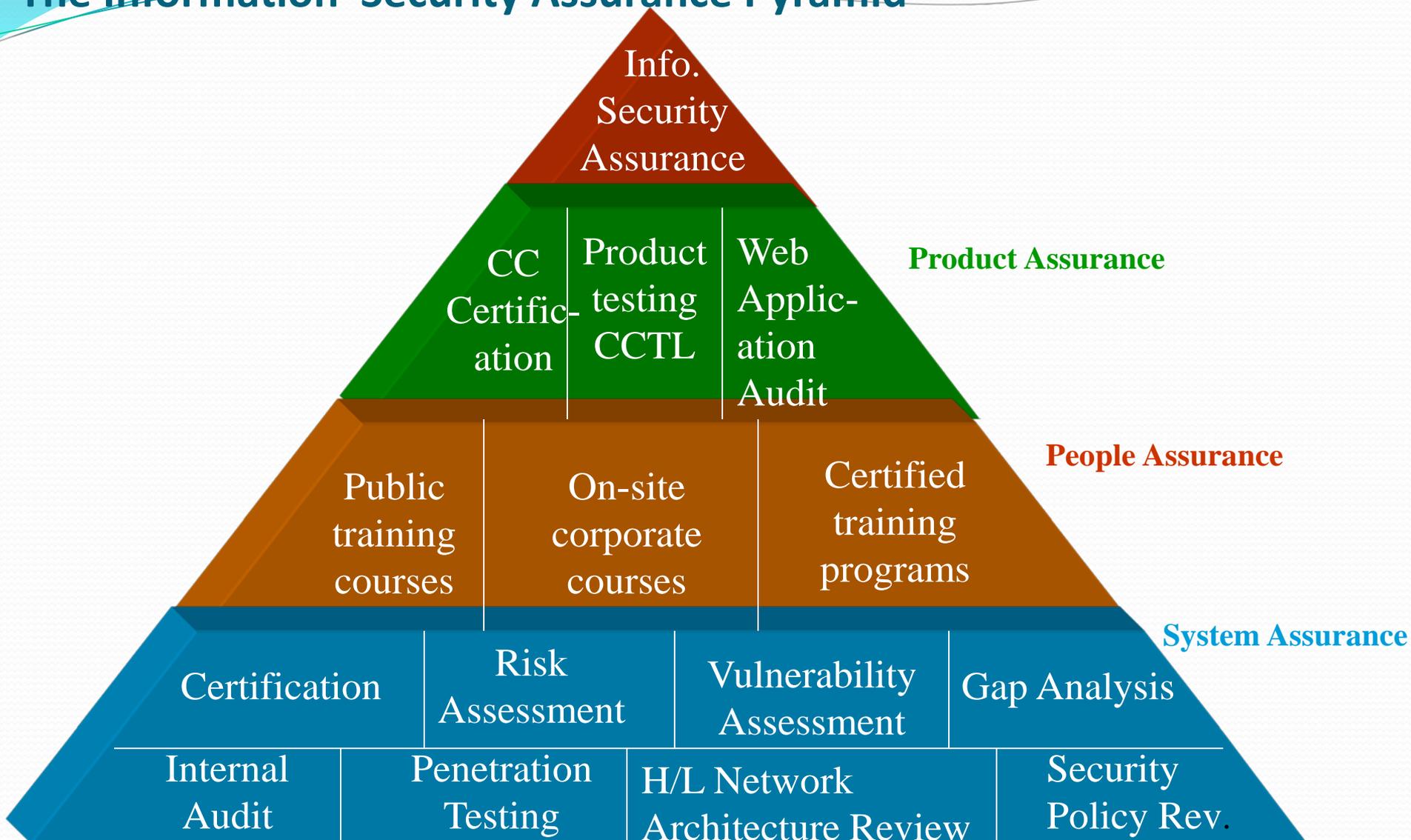
Application Security

Information Asset

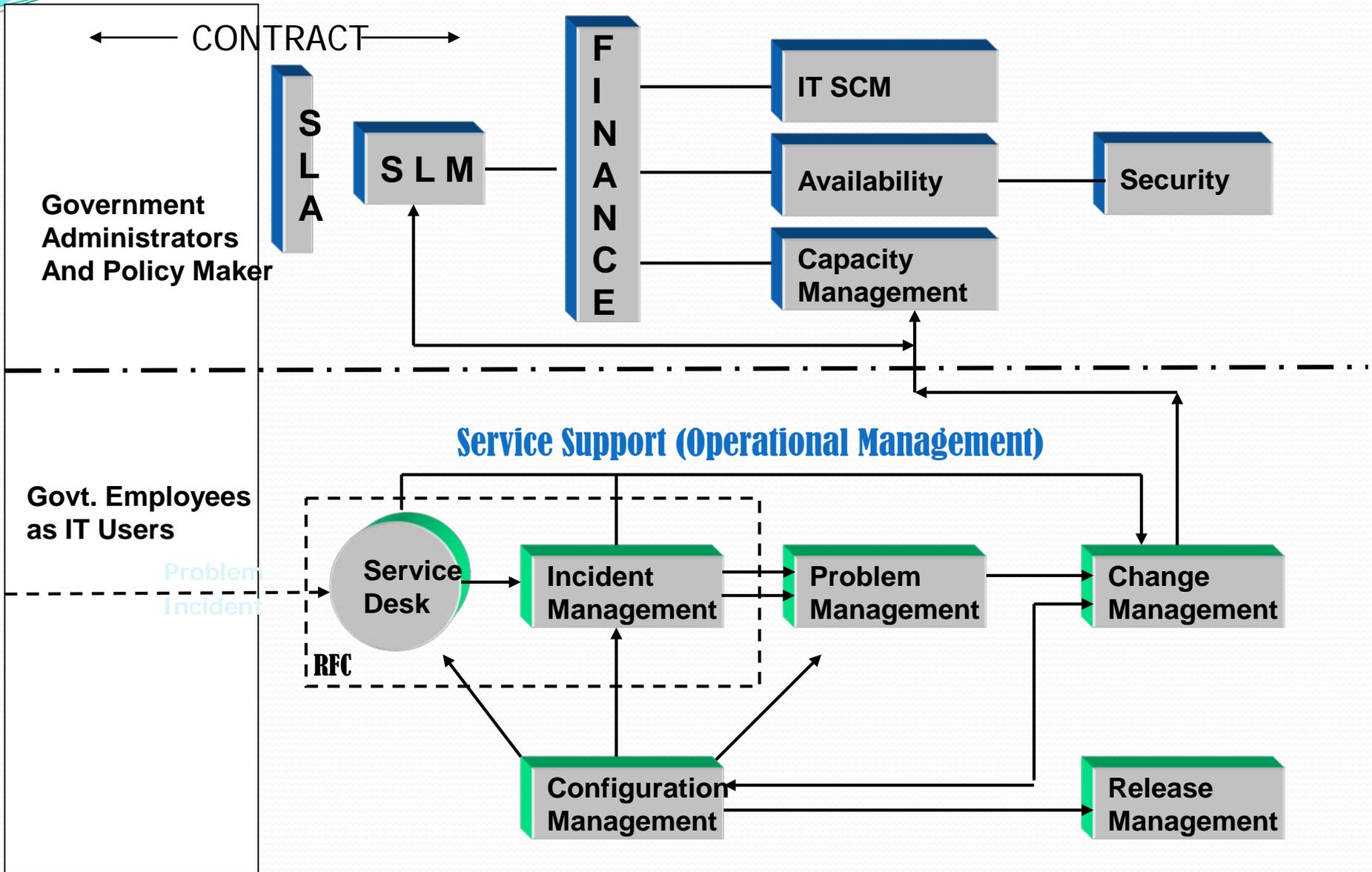
IMPACT ANALYSIS & RISK ASSESSMENT



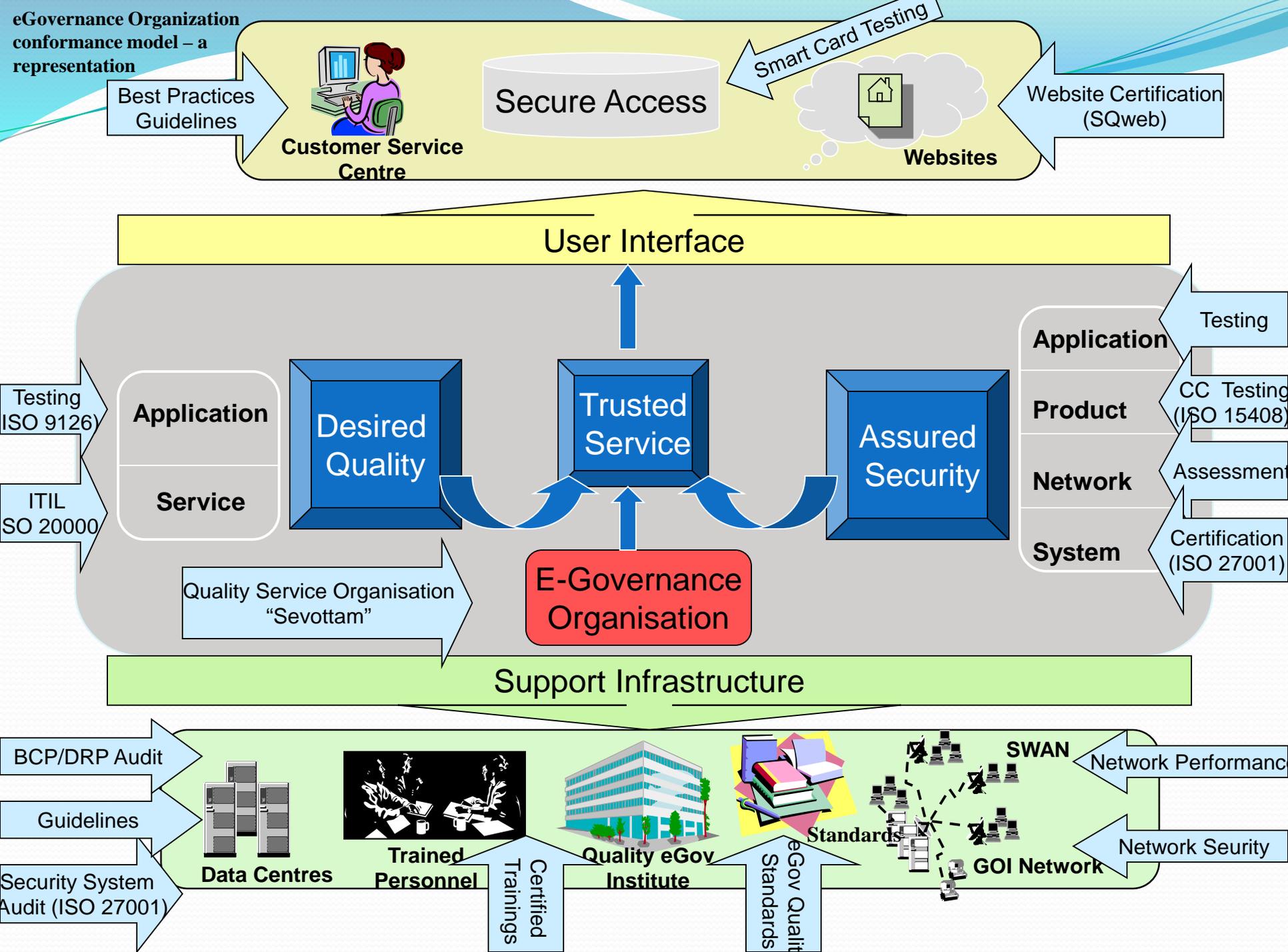
Quality Gate : Information Security -Illustration of Activities involved The Information Security Assurance Pyramid



Quality Gate : IT Service Management



eGovernance Organization conformance model – a representation



e-Governance Projects – Experience and Validation

- MCA 21Passport Seva Project
- Passport Seva Project
- Municipality Applications
- Land Record Information System, National Informatics Center
- Treasuries Software of Madhya Pradesh Government
- ENVISION, Ministry of Environment & Forest
- Property Registration
- Community Information Services of North East
- India Portal
- NSDG
- e-Seva for Security Evaluation
- eDistricts



Thank you