ICT SYSTEMS SECURITY IN THE PUBLIC SECTOR

Ahmed Mustapha Yahuza

Computer Emergency Readiness & Response Center

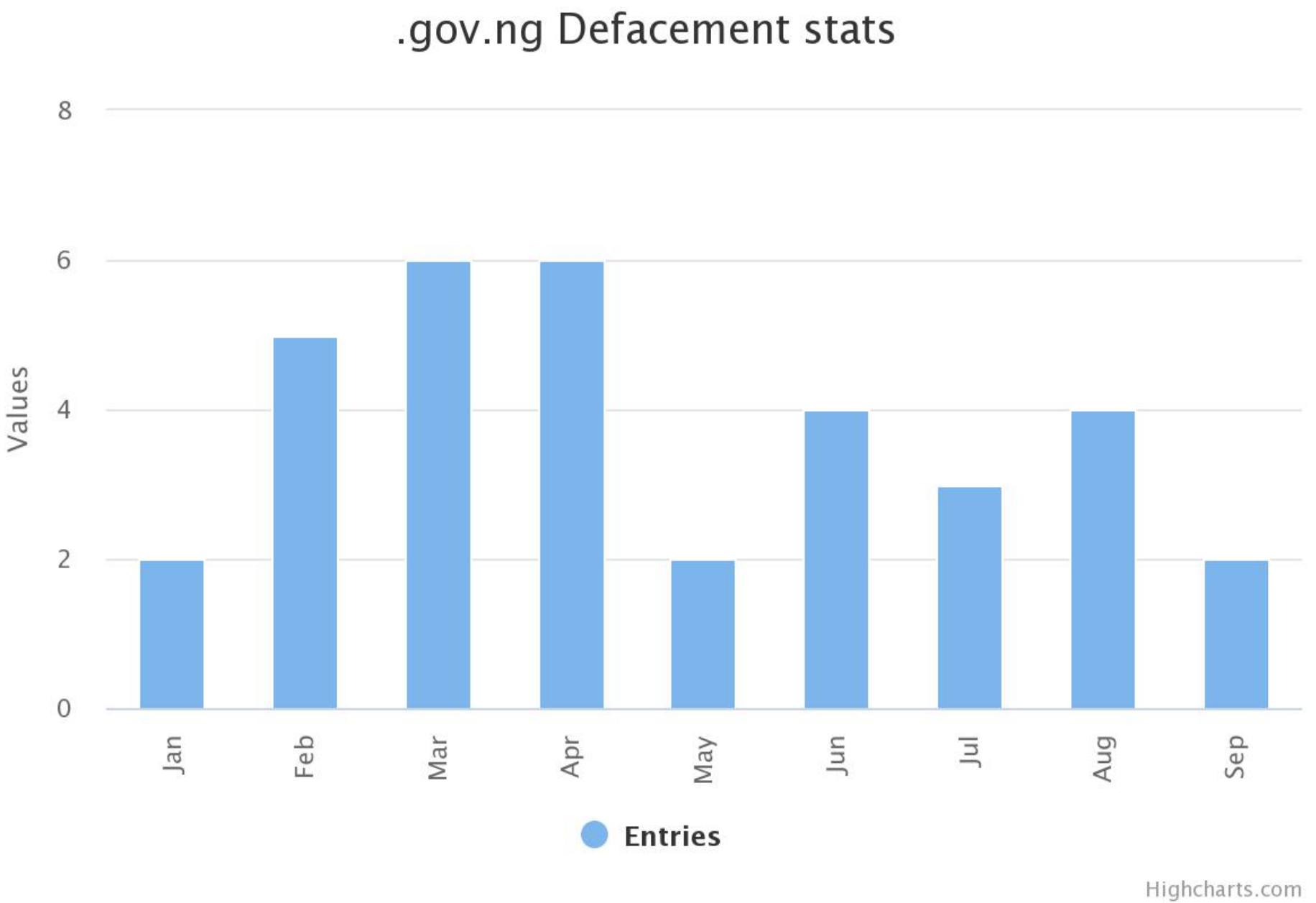
NITDA

ICT Systems in MDAs

ICT is the conduit used to deliver government services, interactions with citizens and other stakeholders and transactions with businesses.

ICT Assets in MDAs

- **Information:** Websites/ Portals, Corporate Email, Social Media, Desktop Publishing
- **Software,** such as computer programs
- **Physical assets**, such as computers, Local Area Network
- **Services:** Internet access, Data Management and Queries
- **People** and their qualifications and skills
- **Intangible**, such as reputation and image,Online Meetings


.gov.ng Defacement stats
Values
8
6
4
2
0
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Entries
Highcharts.com

NITDA Computer Emergency Center

G2G (Government to Government)

- Dissemination of cyber security advisories
- Incident handling, incident coordination and response support
- Education and training programs to support National cyber security needs and capacity building.
- Create and implement cyber security awareness

Types of Cybercrime

- Phishing
- BVN Scams
- Bank Card Theft/ATM skimming
- Cyber theft/Banking fraud
- Cyber Pornography
- Software piracy

Types of Cybercrime

- Fake Promos
- Cyber stalking, harassment and blackmailing scam
- Denial of service/Distributed denial of service
- Social Hijacking/Web jacking

Types of Cybercrime

- Sales fraud and forgery
- Data/Airtime time theft from service providers
- Nigerian-Prince (Beneficiary of a Will)
- Charity Funds

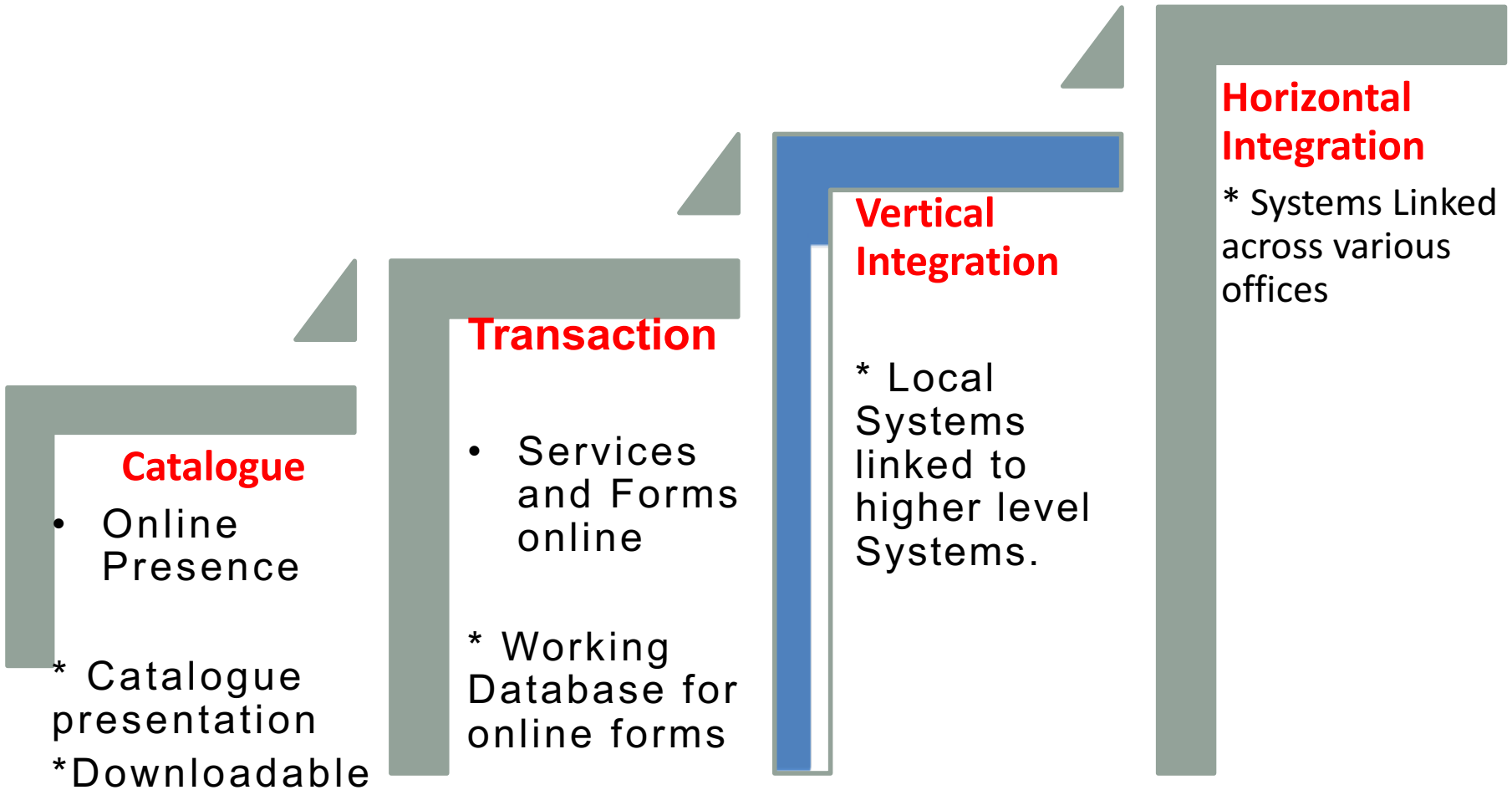
Quick assessment: Readiness for digital economy

Complete the Assessment form

@

https://rb.gy/xkuj9a

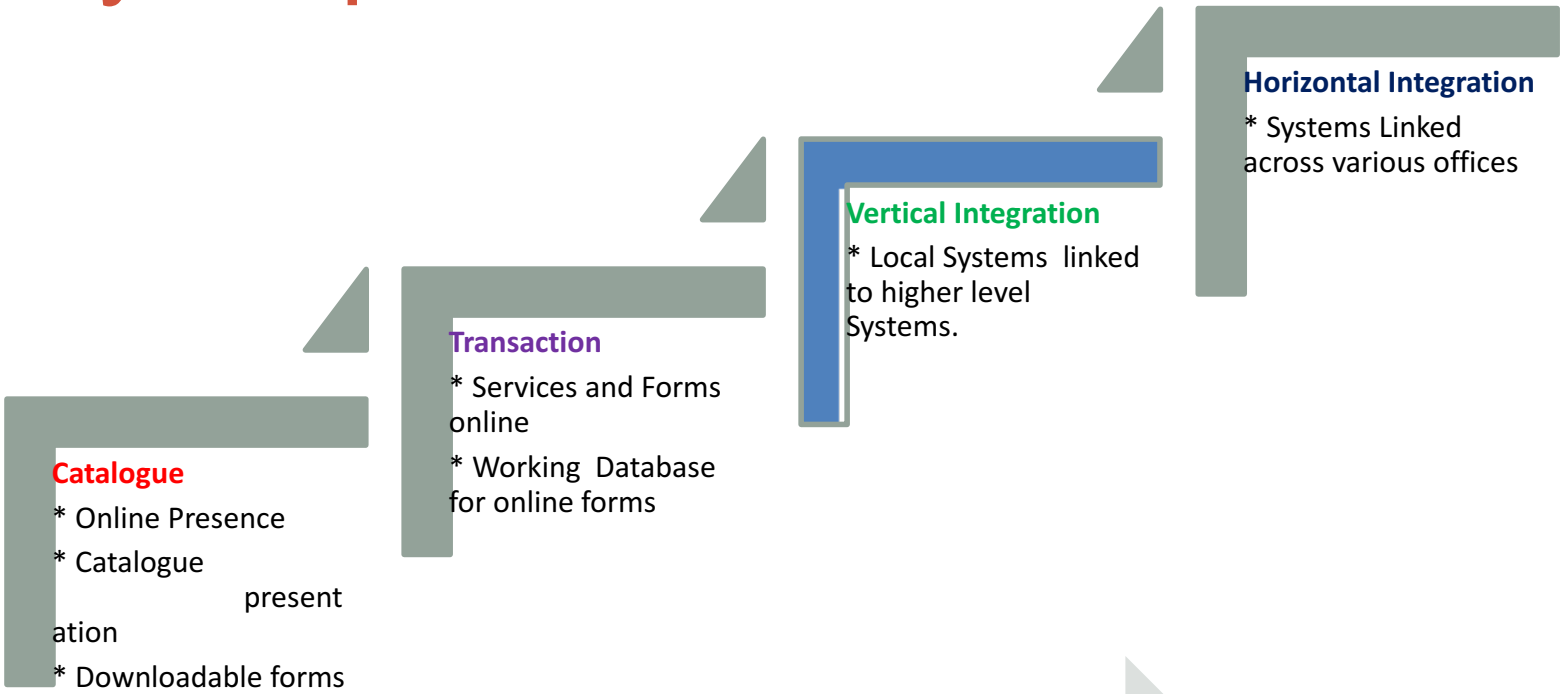
Website Maturity Model

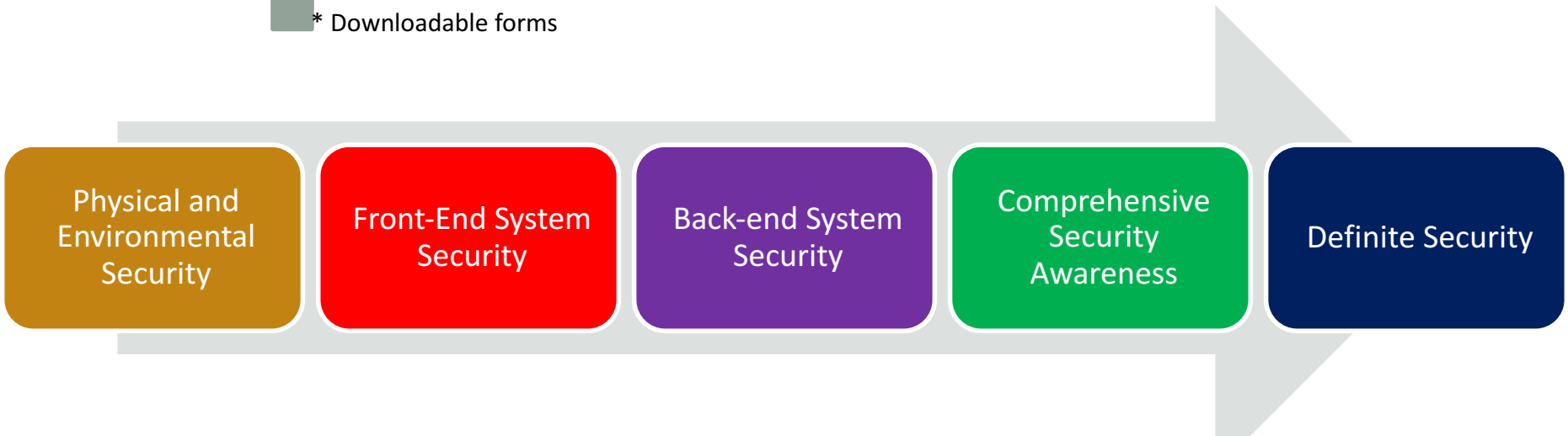


Website Security Features

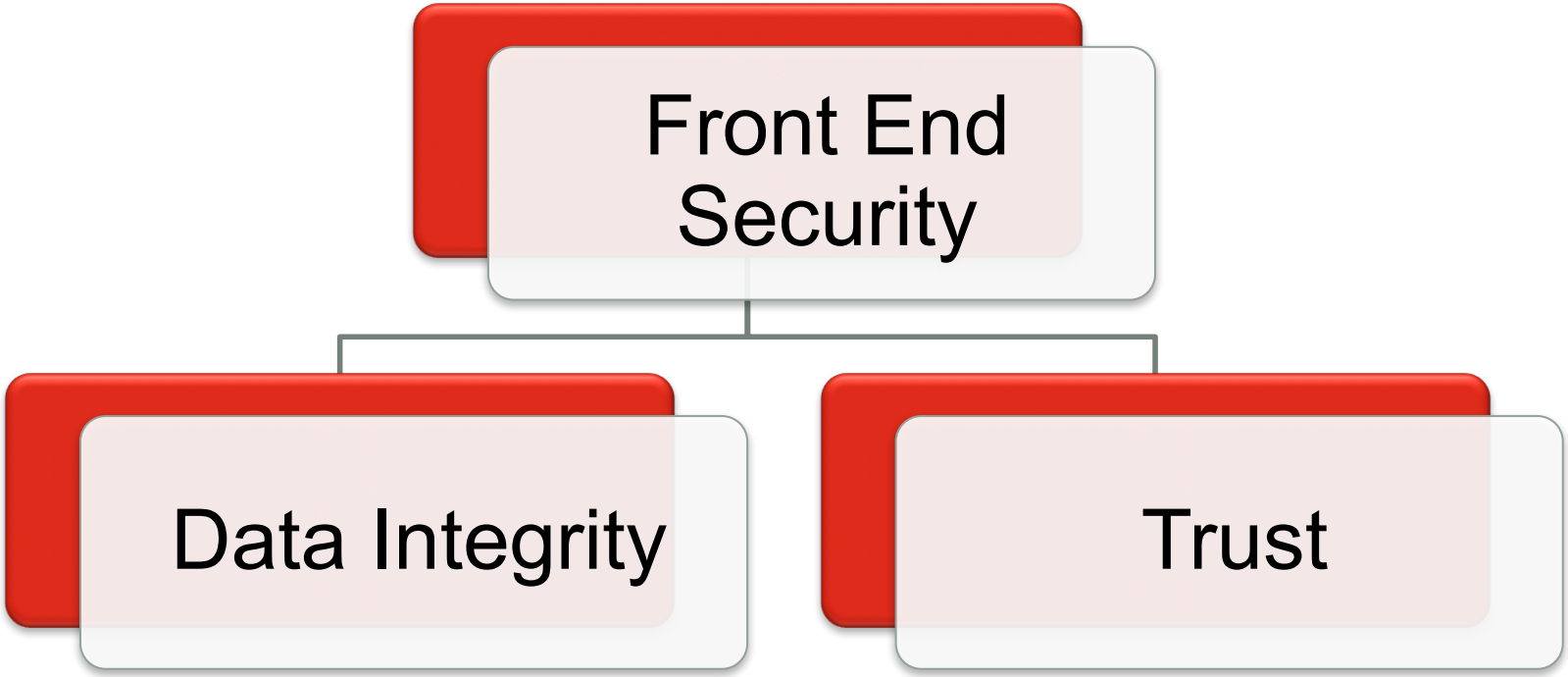
- Authentication
- Data Confidentiality
- Data Integrity
- Trust
- Non-repudiation
- User Anonymity
- Privacy
- User Location Traceability
- Auditability (Traceability)
- Security Dependencies

Security Requirements for Websites



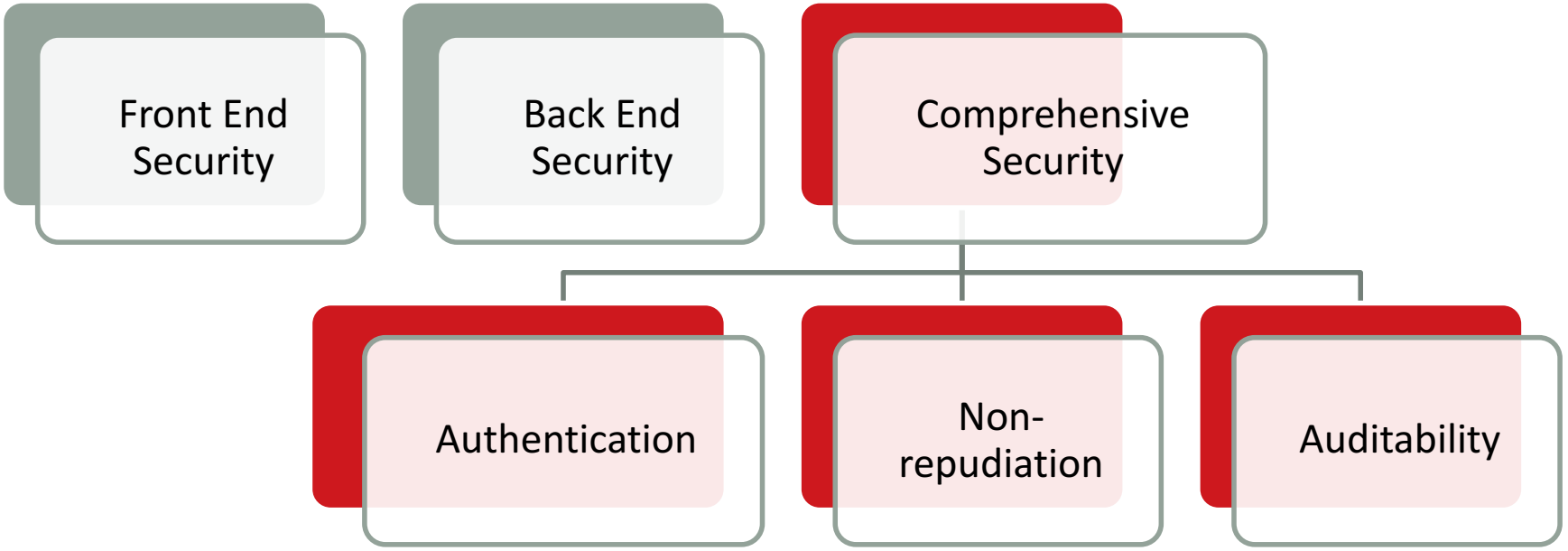


Low Security Requirements



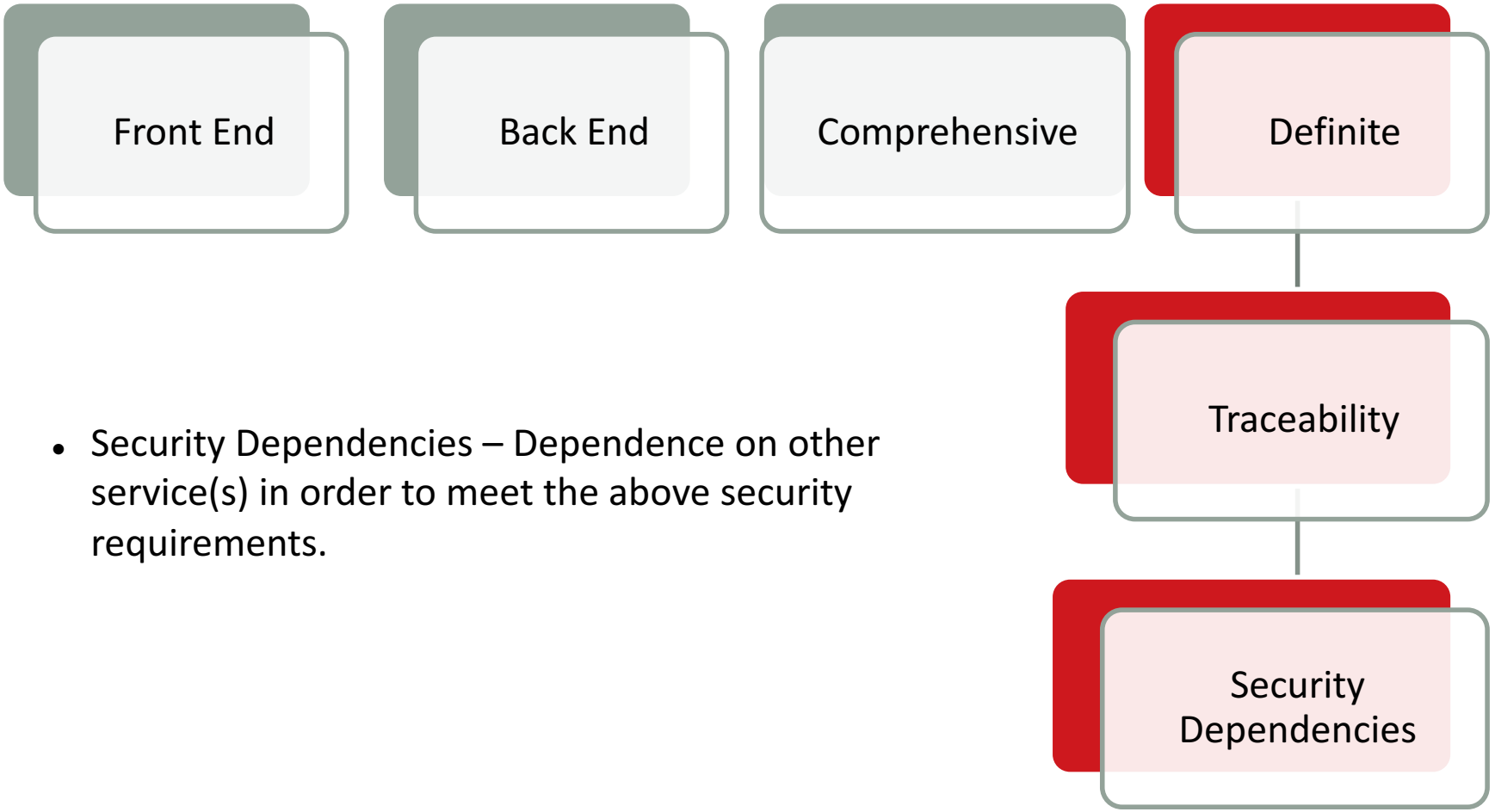
- Data Integrity - The assurance that data has not been altered in an unauthorized manner
- Trust – Confidence in the reliability and validity of an identity.

Medium Security Requirements



- Authentication – The process of verifying an identity claimed by or for an entity using credentials.
- Non-repudiation – Provision of undeniable proof of an action by an entity.
- Auditability (Traceability) - The level to which transactions can be traced and audited through a system

High Security Requirements



- Security Dependencies – Dependence on other service(s) in order to meet the above security requirements.

Quick Recap

- ICT Systems in MDAs
- NITDA Computer Emergency Center
- Website Maturity Model
- Security Requirements for Websites

Next Line of Action??

1. Risk Assessment

- Risk management enables critical information and communications technology (ICT) risks to be effectively identified, managed and governed.
- Clarify objectives for how ICT supports business outcomes
- Make sure critical ICT risks to service delivery are identified and effectively managed, avoiding operational surprises
- Prioritise the allocation of resources to areas of greatest risk
- Be more responsive to new and emerging ICT risks.

Know your online presence

- site:*xyz.gov.ng
  - Expired sub domains
  - No content (unused) pages
  - Internal documents.

2. Leadership and commitment

- Leadership and commitment

Top management shall demonstrate leadership and commitment with respect to the information security management system by: a) ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization;

Policy

- Policy Top management shall establish an information security policy that:
- is appropriate to the purpose of the organization;
- be available as documented information;

3. Organizational roles, responsibilities and authorities

- Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated.

4. Support

- Resources: Determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system.
- Competence: Determine the requirement competency and ensure that these persons are competent on the basis of appropriate education, training, or experience.
- Awareness: Persons doing work under the organization's control shall be aware of the information security policy.

Questions!!

THANK YOU

AND

GOD BLESS