SELF ASSESSMENT FOR RISK & WEB TRUST – AN AUDITOR'S VIEW

Subhash Rao P

Digital Age Strategies Pvt Ltd

Business With Wisdom
...Growth With Assurance

Subhash Rao P B.E , MBA

Associate Director , Sr Auditor

Business With Wisdom
...Growth With Assurance

Digital Age Strategies Pvt. Ltd.

Estt. 2004

~ 30 years of industry Experience, 18 Years in IT /IS security area.

Served as Head of R&D at Sasken Communication Technologies Ltd

Domain of Expertise: HW,SW, Techno commercial Project Management, Cyber security Auditing, Consultancy.

Certification

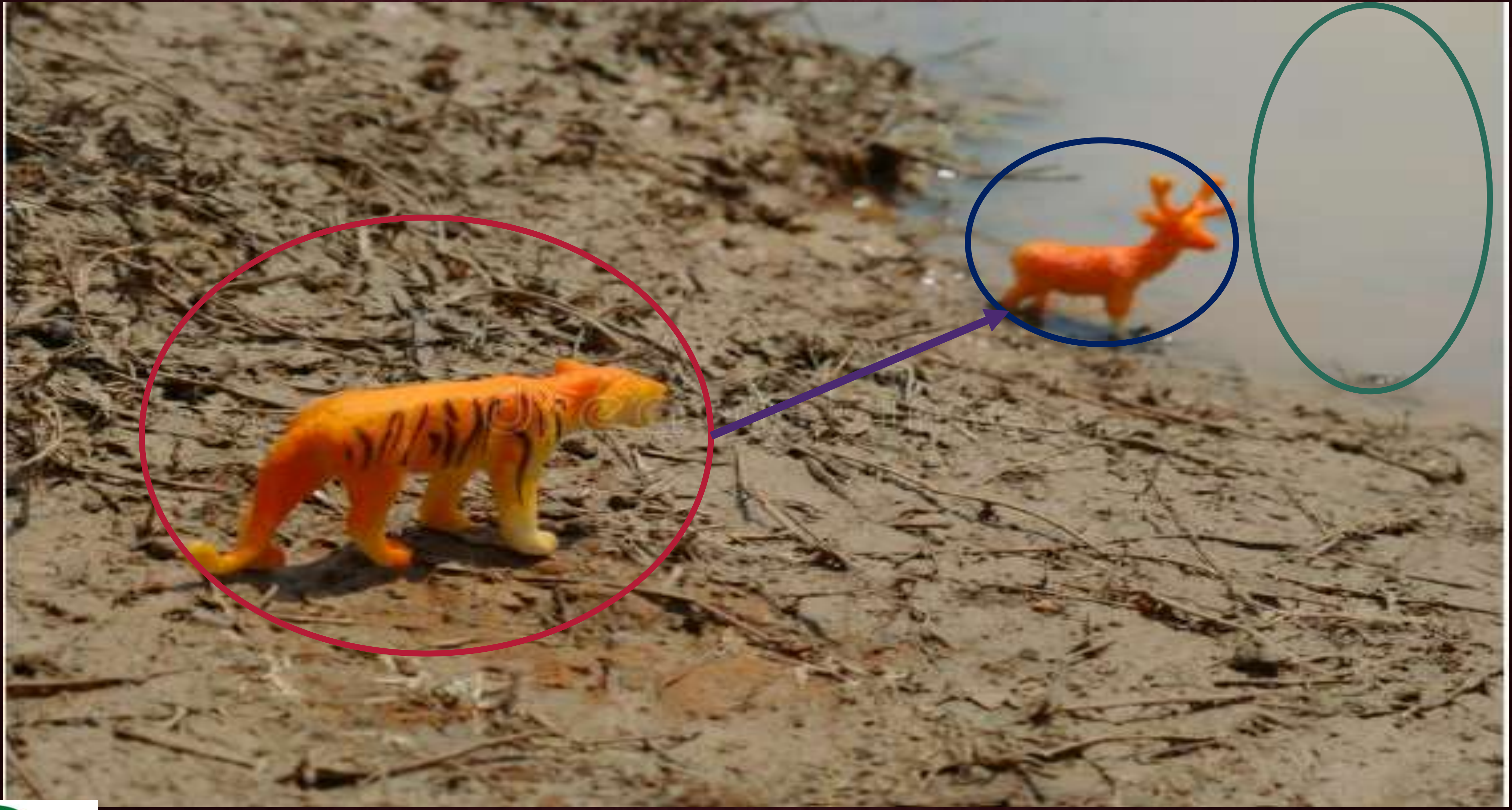
CEH CERTIFIED CHFI CERTIFIED ECIH CERTIFIED CND CERTIFIED CEI CERTIFIED CDPSE ISO 27001 Lead Auditor

PROFILE OF DIGITAL AGE

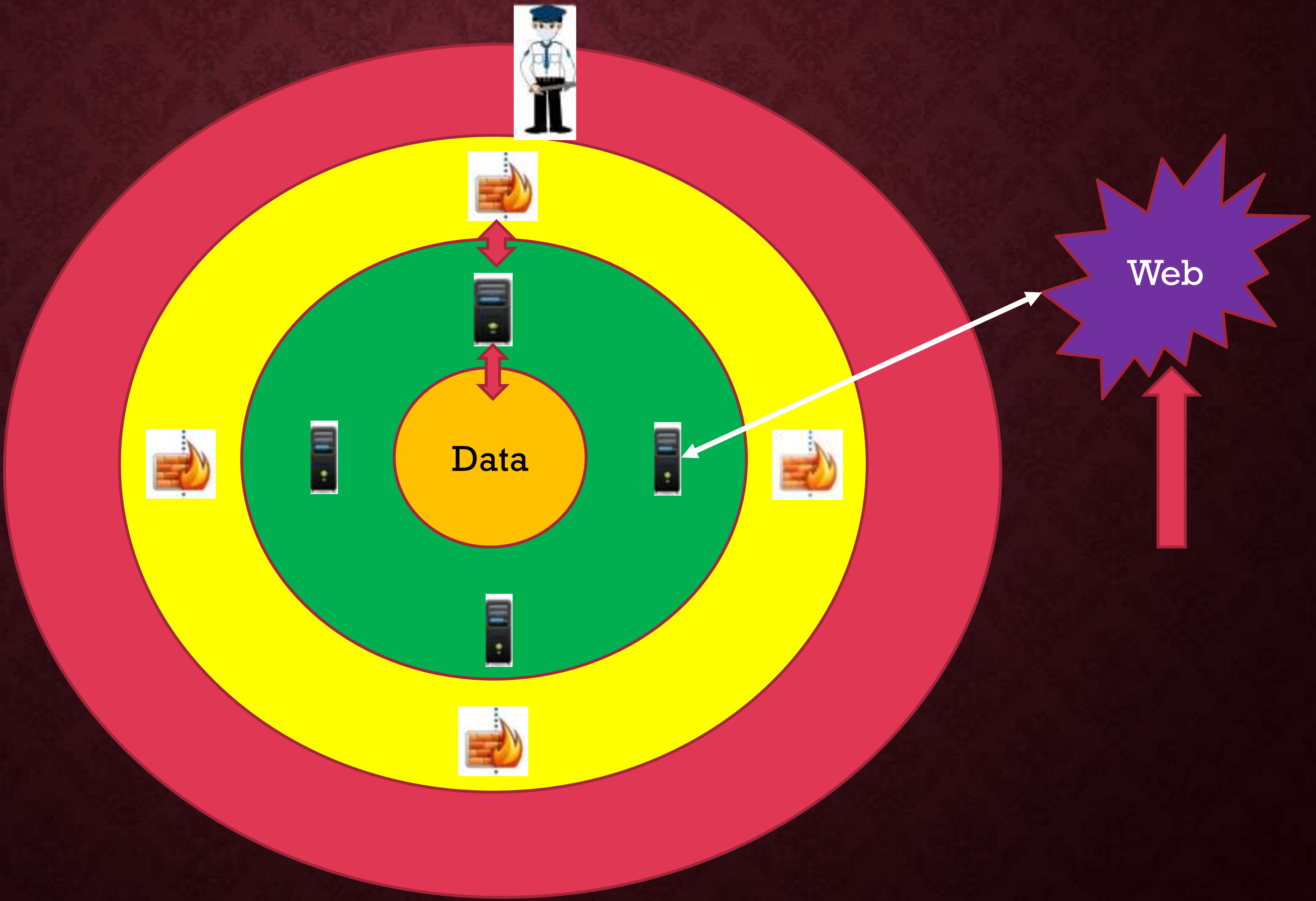
- Digital Age is more than 18 years, fast growing International Management Consulting organization in the domain of
  - Information Security Audit
  - VA & PT, Cyber Forensics, Data Migration, Code Review
  - Training
  - Audit Management
  - Business Transformation

- Digital Age is empaneled by CCA and audit following Cas
-
- Digital Age is Auditor of RBI, SEBI, DRDO, Indian Navy, EIL, Indian Railways, Ports, Airport Authority of India, L&T, LIC & Several Banks/Government Organizations

Business With Wisdom
...Growth With Assurance



Business With Wisdom
...Growth With Assurance


Data
Web

RISK ASSESSMENT

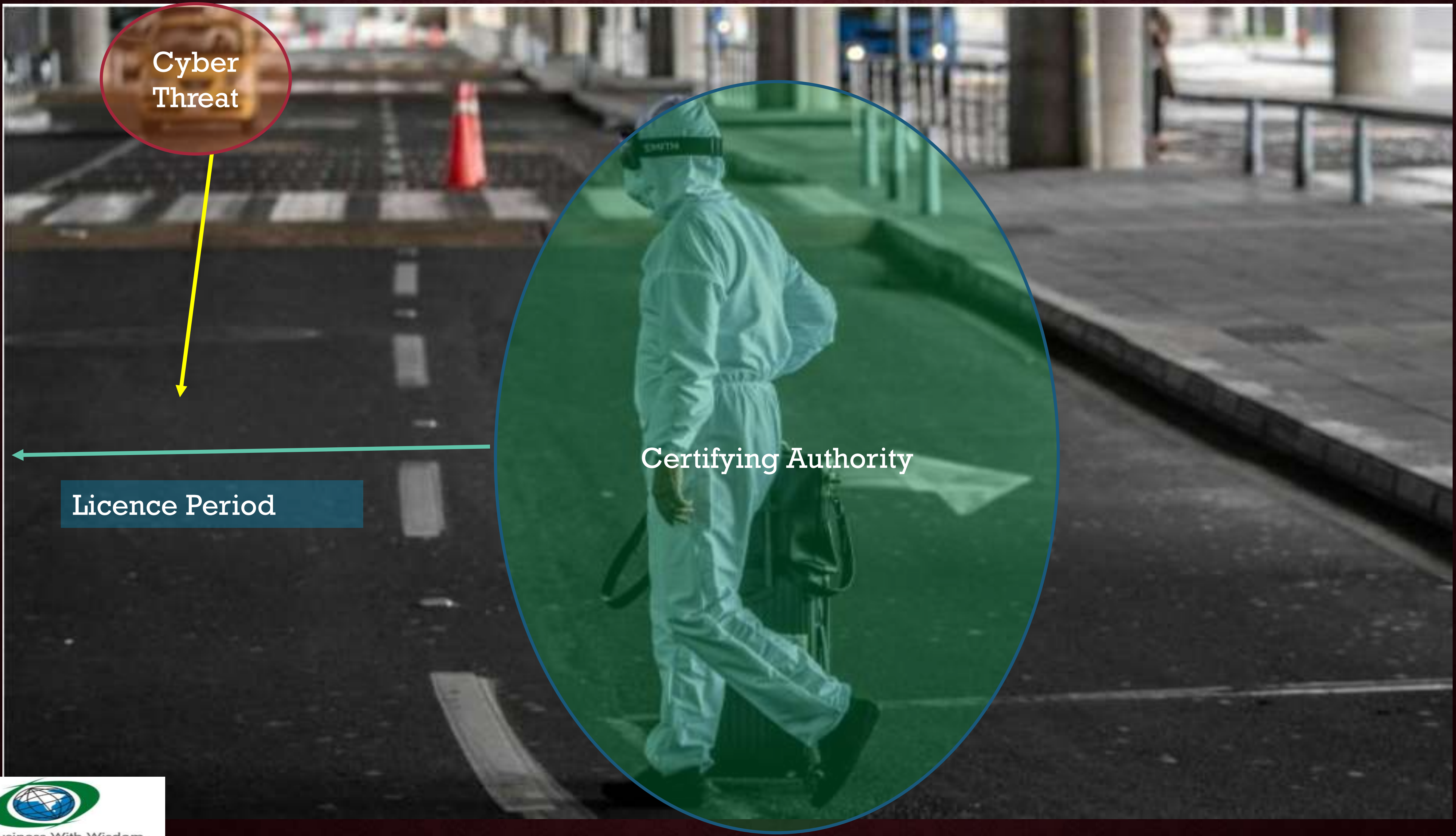
Control No	Control	Control Type	Reference
3.1.1.7	The CA's security program shall include an annual Risk Assessment	Mandatory	IT CA Rules SCHEDULE-II 17.3 CA Browser Forum 5
3.1.1.8	A list of foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any critical information shall be maintained.	Mandatory	CA Browser Forum 5
3.1.1.9	The sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter cyber threats shall be verified.	Mandatory	CA Browser Forum 5

Business With Wisdom
...Growth With Assurance

RISK ASSESSMENT

Control No	Control	Control Type	Reference
3.1.1.10	A security plan shall be developed covering the following: • Security procedures to manage the risks • administrative, organizational, technical, and physical safeguards • cost of implementing the specific measures • security breach plan in case of any incidents	Mandatory	CA Browser Forum 5
3.1.1.11	Hypervisors, operating system, database, and network device patches and updates shall be applied in a timely manner when deemed necessary based on a risk assessment and follow formal change management procedures	Mandatory	WebTrust 3.6.18

Business With Wisdom
...Growth With Assurance



Cyber Threat

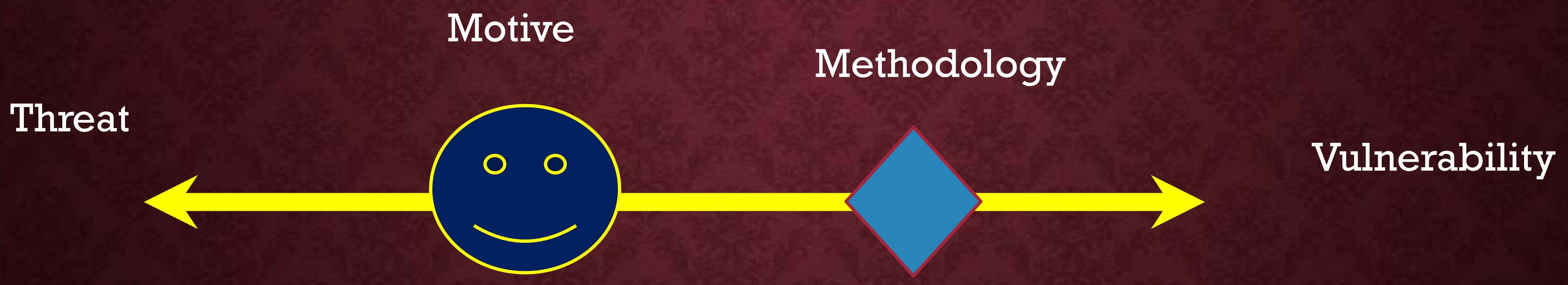
Certifying Authority

Licence Period

RISK

- Probability of you escaping from Incident / threat
- Your capability Vs Threat

THREAT



- Threat = Motive * Methodology * Vulnerabilities

RISK ASSESSMENT

Control No	Control	Control Type	Reference
3.1.1.12	A documented security self-assessment plan shall be prepared by the CA	Mandatory	IT CA Rules 2.e
3.1.1.13	Self-Assessment shall be performed on a periodic basis and the findings shall be reported to management and discussed for closure	Mandatory	IT CA Rules 2.e

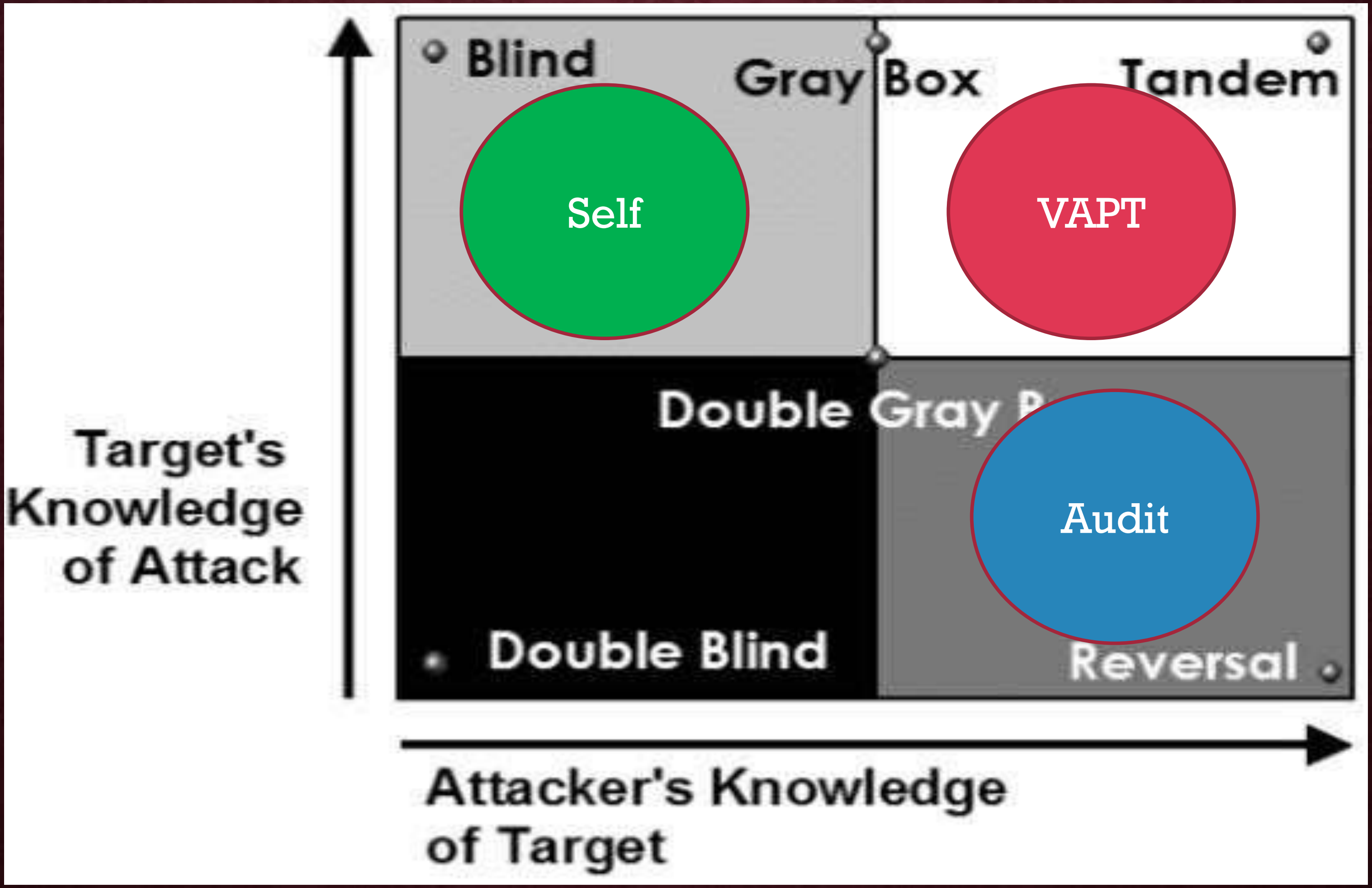
Business With Wisdom
...Growth With Assurance

- WebTrust Principles and Criteria for Certification Authorities and Verified Mark Certificates (“Criteria”)VMC
    - To set out principles and criteria that would be used by a practitioner to conduct a Verified Mark Certificate assurance.
    - The primary goal of these requirements is to describe an integrated set of technologies, protocols, and identity and mark proofing requirements that are necessary for the issuance and management of Verified Mark Certificates (VMCs) – certificates that are trusted by Consuming Entities and Relying Parties.
    - VMCs assert a cryptographically verifiable and auditable binding between an identity, a logo, and a domain.

- Verification of domain control
  - CA obtains confirmation in accordance with one of the allowed methods in the VMCR related to the Fully-Qualified Domain Name(s) (including wildcard domains).
  - The CA maintains records of which validation method, including the relevant VMCR version number, used to validate every domain.

- Registered mark verification
  - CA confirms that the Mark Representation submitted by the Subject organization matches the Registered Mark in accordance VMCR
  - CA confirms that the Registered Mark identified in the official database of the applicable Trademark Office or the WIPO Global Brand Database is the same Subject organization verified by the Verified Mark vetting process

- Audit and legal
  - The CA performs ongoing self-assessments on at least a quarterly basis against a randomly selected sample of at least three percent (3%) of the VMC issued during the period commencing immediately after the previous self-assessment samples were taken

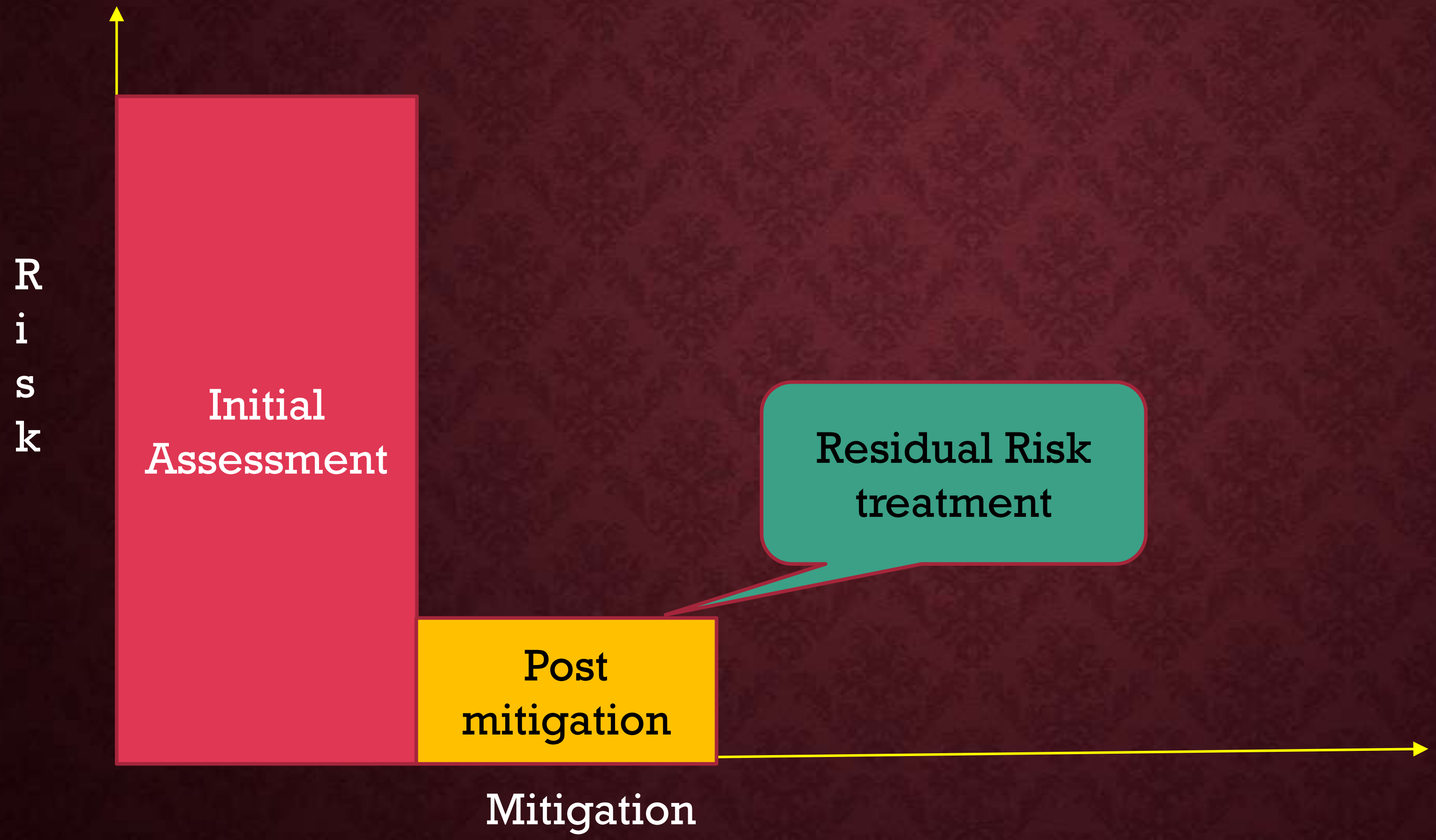


Business With Wisdom
...Growth With Assurance

SELF ASSESSMENT

- Location of CA setup
- Assets used in CA activity
- Process followed
- EKYC process
- People involved
- Protection to Root certificate

- Preparedness to
- Physical security threat
- Environmental security threat
- Network security threat
- Application security threat
- Phishing attack
- Periodic review
- Backup and restoration
- Preparedness to face incidents
- Quickness in response



Risk

Initial Assessment

Post mitigation

Residual Risk treatment

Mitigation

Thank You