Regional Forum on Cybersecurity in the Era of Emerging Technologies
&
the Second Meeting of the "Successful Administrative Practices"-2017
Cairo, Egypt 28-29 November 2017

Healthcare Security Success Story

Dr. Mohamed AbdelFattah
VP of Advisory Services, ALTERNA, IT
Business unit, 57357 Group

Healthcare Trending

1 The World Health Organization (WHO) estimates up to 40% of resources spent on healthcare are wasted, in part due to antiquated processes and systems.

2 It has been estimated that there will be approximately 50 billion devices connected to the Internet and, therefore, to each other by 2020.

3 Increased demand of healthcare due to an increased number of elderly and changed life styles leading to an increase in chronic diseases

4 Need for increased efficiency, individualization and equity of quality-oriented healthcare with limited financial resources

ITU-D 1992 2017
CELEBRATING
25 YEARS
OF ACHIEVEMENTS

Smart Hospital

The Smart can be summarized in a simple question: "How do we leverage real time information to achieve clinical excellence and enhanced patient experience?

Intelligent hospital

Intelligent hospital is one that works better and smarter

better because it's resourceful, creative, and perceptive about what patients and doctors need

smarter because it's astute and inventive when it comes to weaving together diverse technologies to enhance patient care.

4D's Framework

**The key of success**

Business first

Technology second

1 Discover

- Identify Stakeholder
- Define Project Strategy
- Discover Current state of Healthcare system
- Recommend current system enhancements

2 Design

- Get Stakeholders Consensus
- Design Organizational Integrated workflow
- Propose and approve future state of Healthcare system components & its infrastructure
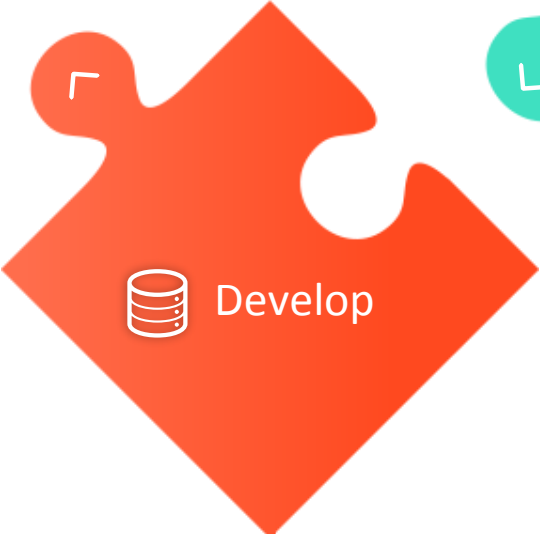
Project Life Cycle

Discover

Design
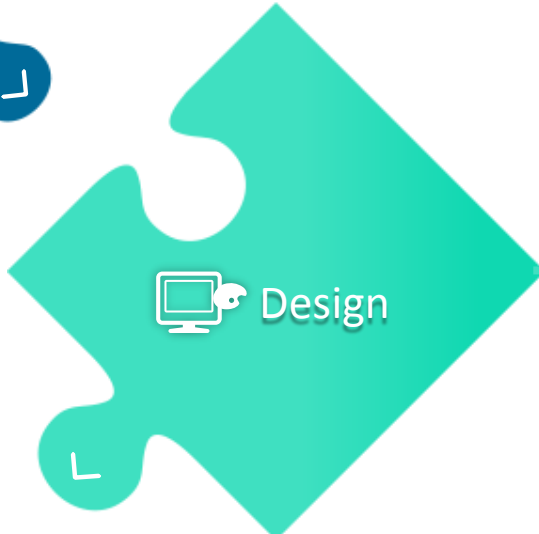
Develop

Deliver

4 Deliver

- Validate solution and measure outcomes
- Identify opportunities for improvement
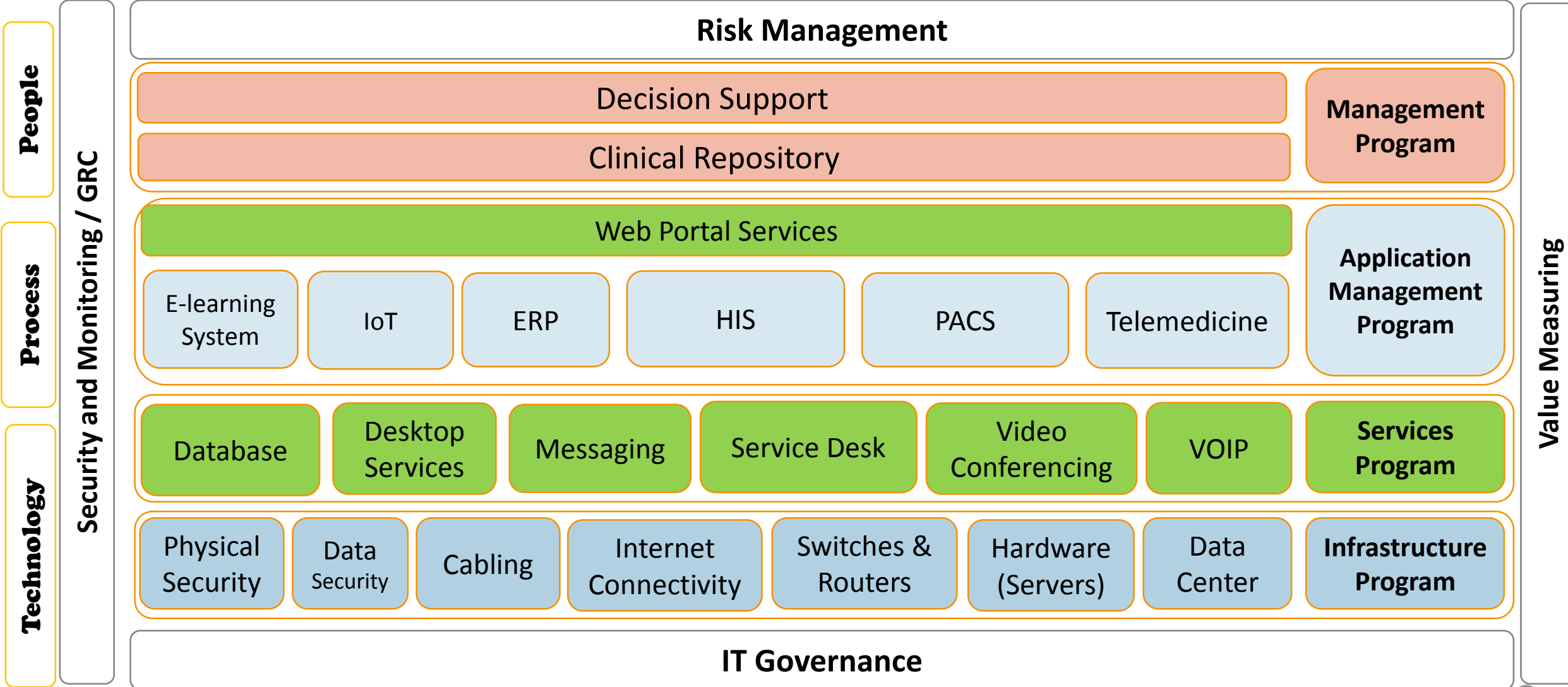- Share lessons learned
- Improve the knowledge transfer

3 Develop

- Develop and Configure approved solution
- Develop knowledge transfer plan
- Deliver training

ITU WTDC BUENOS AIRES 9-20 October

ITU-D 1992 2017 CELEBRATING 25 YEARS OF ACHIEVEMENTS

Smart Hospital Framework

Proposed Technology Services Framework

ITU WTDC
BUENOS AIRES 2017
9-20 October

Risk Management

People | **Process** | **Technology**

Security and Monitoring / GRC

Value Measuring

Decision Support

Clinical Repository

Management Program

Web Portal Services

Application Management Program

E-learning System	IoT	ERP	HIS	PACS	Telemedicine

Database	Desktop Services	Messaging	Service Desk	Video Conferencing	VOIP

Services Program

Physical Security	Data Security	Cabling	Internet Connectivity	Switches & Routers	Hardware (Servers)	Data Center

Infrastructure Program

IT Governance

1992 2017
25 YEARS OF ACHIEVEMENT

8

Proposed Technology Services Framework, Continue

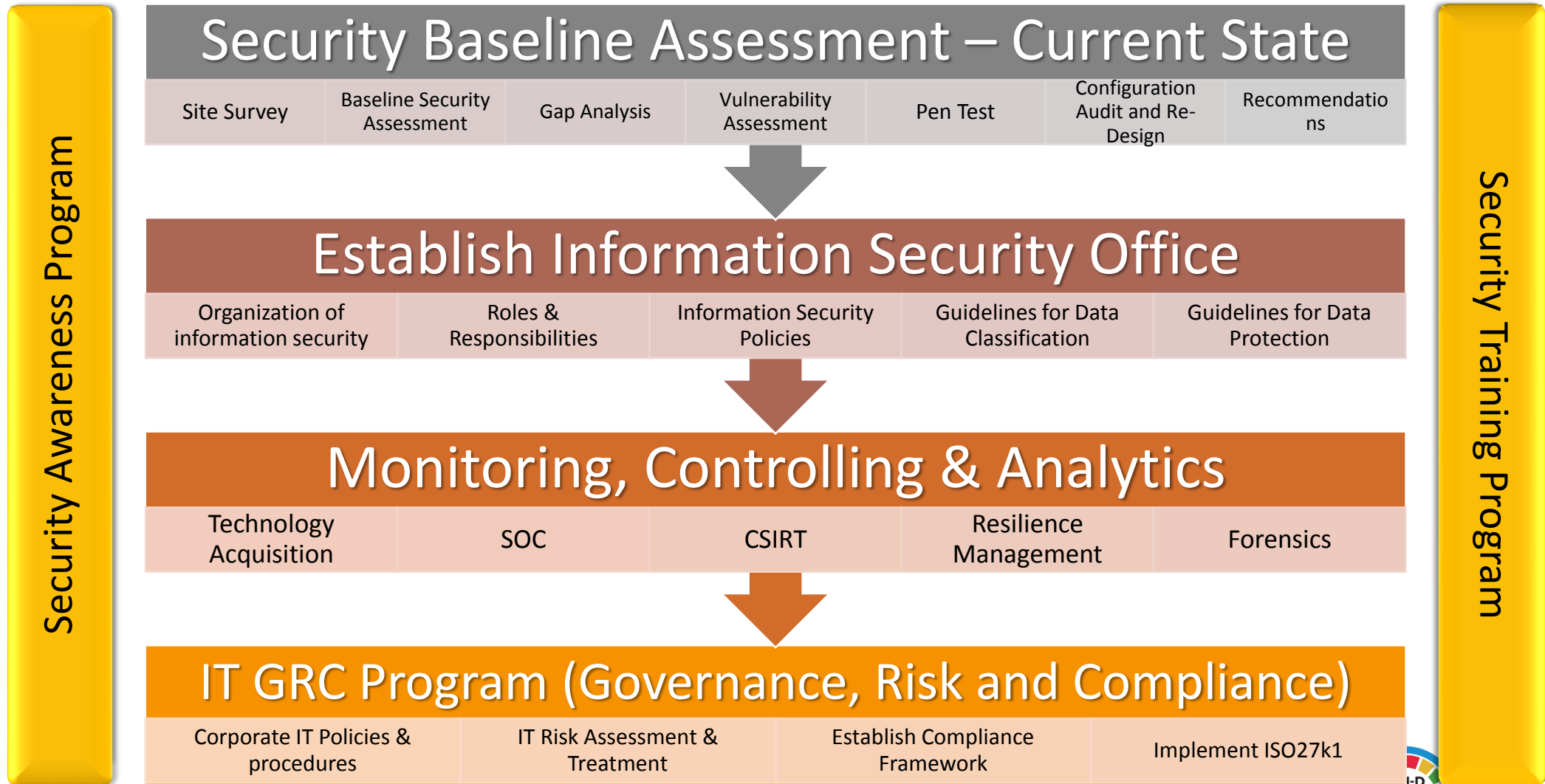| IT Governance	Governance, Risk and Compliance	Value Measuring
IT governance provides a structure for aligning IT strategy with business strategy. By following a formal framework, organizations can produce measurable results toward achieving their strategies and goals.	IT governance and GRC are practically the same thing. GRC is the parent program, what determines which framework is used is often the placement of the CISO and the scope of the security program.	Value measuring methodology (or VMM) is a tool that helps financial planners balance both tangible and intangible values when making investment decisions, and monitor benefits.

Security Business Approaches

Information Security Programs

Information Security Transformation Approach

Security Awareness Program

Security Training Program

Security Baseline Assessment – Current State

Site Survey	Baseline Security Assessment	Gap Analysis	Vulnerability Assessment	Pen Test	Configuration Audit and Re-Design	Recommendations

Establish Information Security Office

Organization of information security	Roles & Responsibilities	Information Security Policies	Guidelines for Data Classification	Guidelines for Data Protection

Monitoring, Controlling & Analytics

Technology Acquisition	SOC	CSIRT	Resilience Management	Forensics

IT GRC Program (Governance, Risk and Compliance)

Corporate IT Policies & procedures	IT Risk Assessment & Treatment	Establish Compliance Framework	Implement ISO27k1

Security Healthcare Solution

Information Security Programs

Security Baseline Assessment

Site Survey

Baseline Security Assessment

Gap Analysis

Vulnerability Assessment & Management

Penetration Testing

Application Security Assessment

Configuration Audit and Re-Design

Considerations & Recommendations

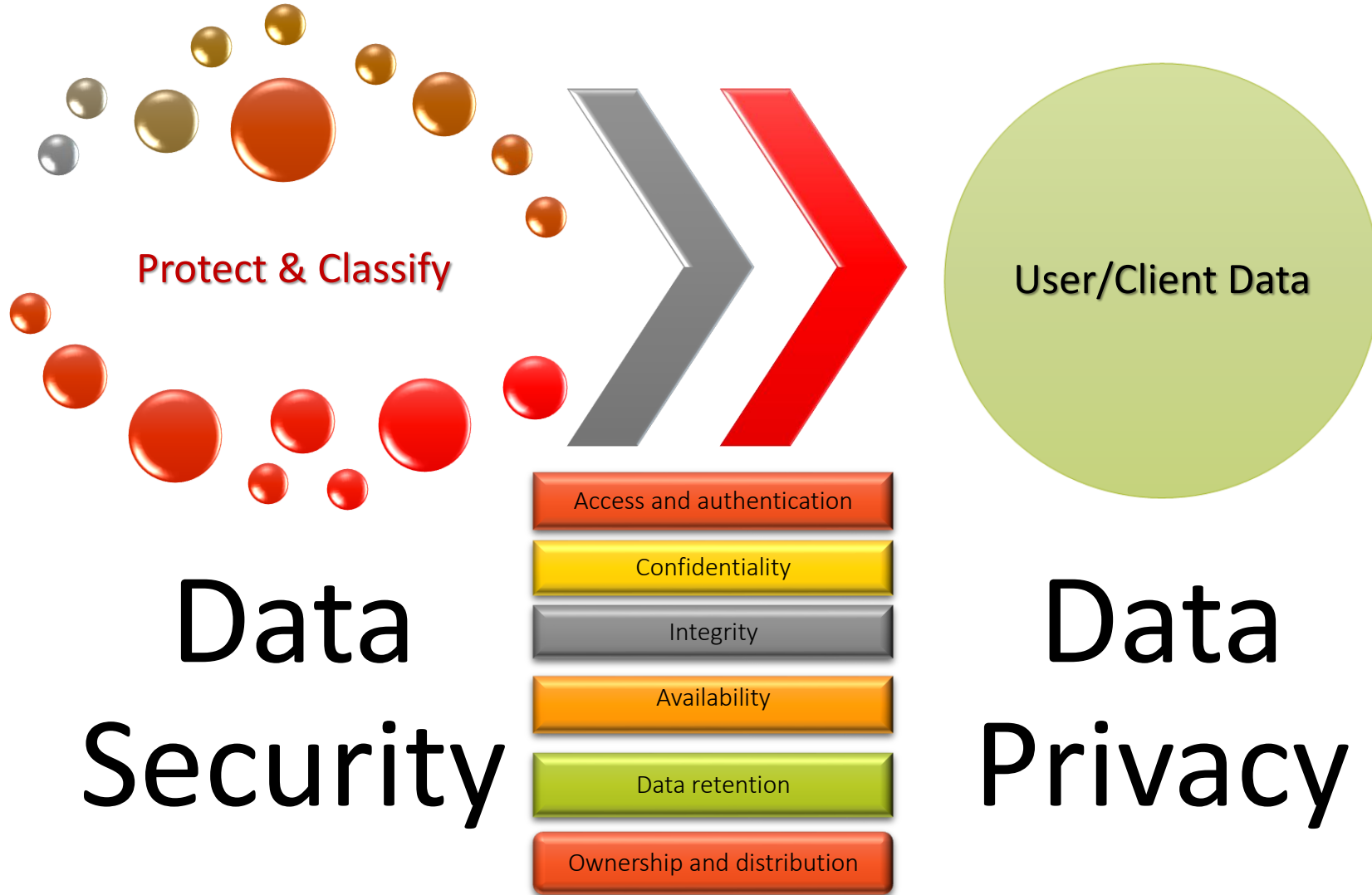# Advanced Security Programs for Enterprise

Security Baseline Assessment – **SBA**

Monitoring, Controlling and Analytics - **MCA**

Identity and Access Management - **IAM**

Data Privacy, Protection and Classification - **DPPC**

Monitoring, Controlling and Analytics

Monitoring & Controlling

- NOC
- SOC
- E-Discovery

Analytics

- Incident Response Management
- CSIRT
- Forensics

Advanced Security Programs for Enterprise

Security Baseline Assessment – **SBA**

Monitoring, Controlling and Analytics - **MCA**

Identity and Access Management - **IAM**

Data Privacy, Protection and Classification - **DPPC**

Identity and Access Management

Managed Certificate Services

IAM Professional Services

PKI
Digital Certificate
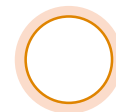
Access Management

SSO

Password Management & Self Service

Role Management

Privilege Users

Advanced Security Programs for Enterprise

Security Baseline Assessment – **SBA**

Monitoring, Controlling and Analytics - **MCA**

Identity and Access Management - **IAM**

Data Privacy, Protection and Classification - **DPPC**

Protect & Classify

User/Client Data

Data Security

Access and authentication

Confidentiality

Integrity

Availability

Data retention

Ownership and distribution

Data Privacy

Data Classification

Compliance
- Data classification can help define in-scope systems and aid with compliance efforts.

Financial Services
- Data classification can help meet compliance requirements of financial regulations and solutions

Healthcare
- Data classification can help ensuring compliance with Health Regulations as HIPAA (Health Informatics Portability and Accountability Act)

Public Corporations
- Knowing where key financial data resides and ensuring it is kept safe.

Government Organizations
- Data classification can help meet the requirements of the Government Information Systems Management Systems

Utility Organizations
- Define required data classification efforts, specifically to define what a "critical cyber asset" is and how it is protected.

IT (Governance, Risk and Compliance)

IT Governance

- IT Strategic Plan
- Process
- Policies & Controls
- Procedures
- Performance Monitoring

IT Risk Management

- Risk Identification
- Risk Assessment
- Treatment Plan
- BIA
- RCA

IT Compliance Management

- IT Standards
- Control Objectives
- Control Testing
- Internal Auditing

IT Quality Management

- Quality Control
- Quality Assurance
- Document Management System
- Business Processes

Professional Consulting Security Programs

IT (Governance, Risk and Compliance) - **GRC**

Managing Operational Resilience - **MOR**

Security Awareness & Simulation Program – **SAS**

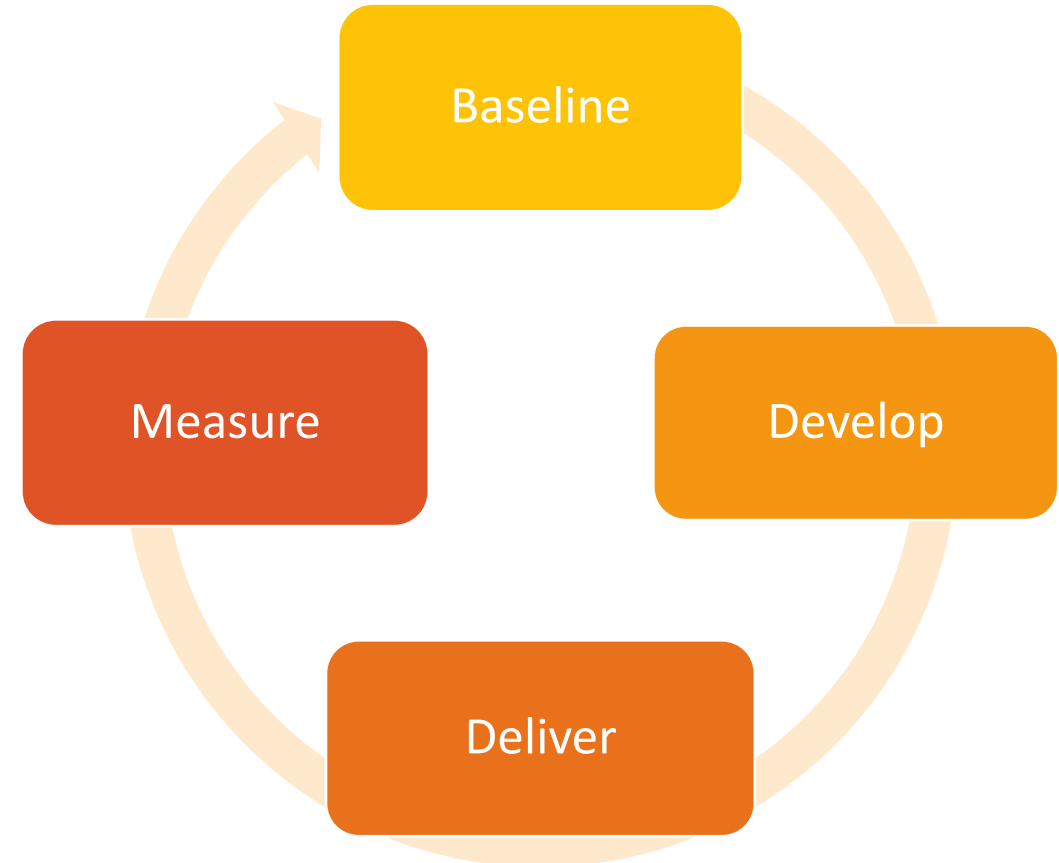Security Training Program - **STP**

Managing Operational Resilience
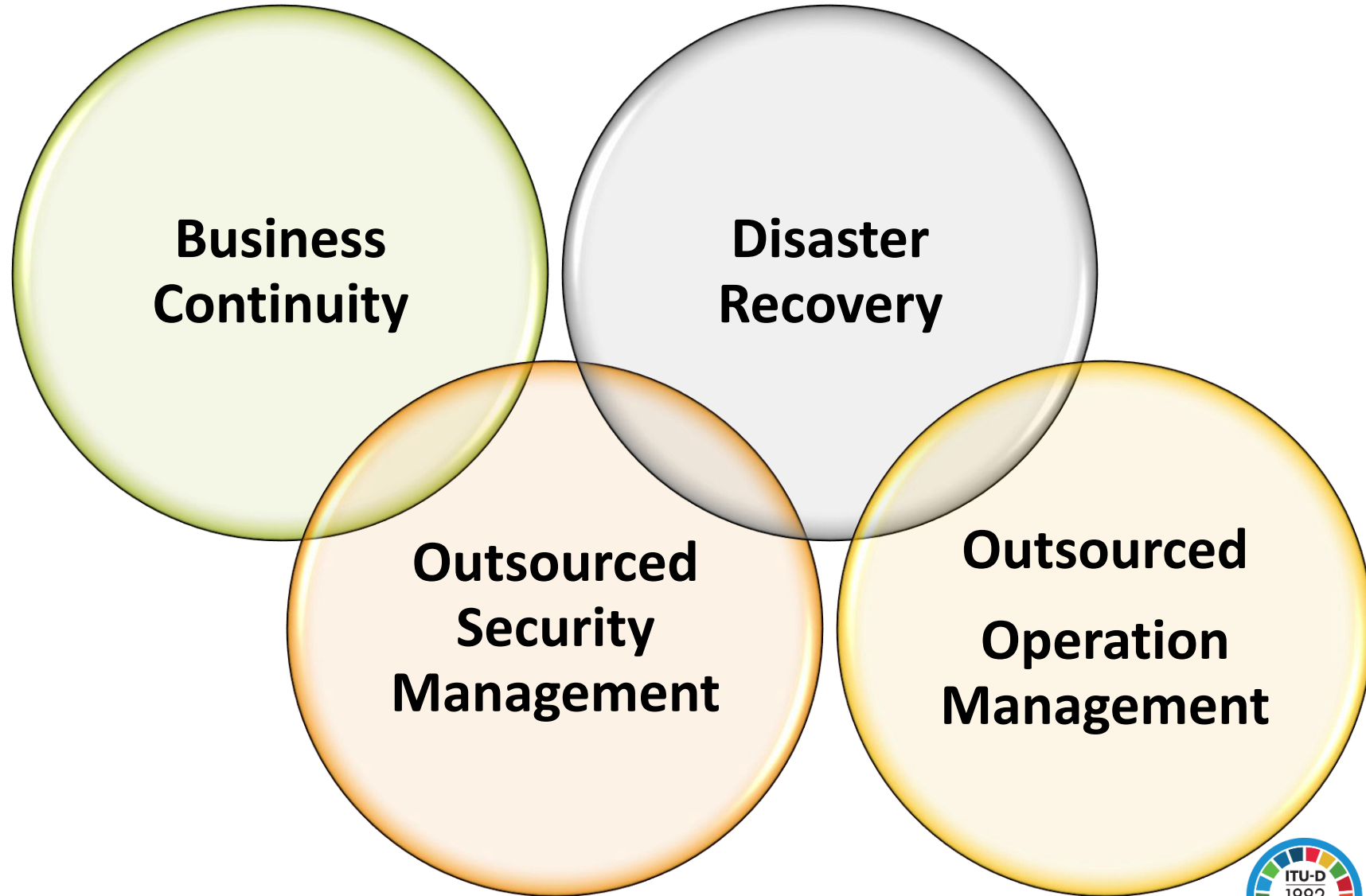
Business Continuity

Disaster Recovery

Outsourced Security Management

Outsourced Operation Management

Professional Consulting Security Programs

IT (Governance, Risk and Compliance) - **GRC**

Managing Operational Resilience - **MOR**

Security Awareness & Simulation Program – **SAS**

Security Training Program - **STP**

Security Awareness & Simulation Program

- Implement CBT Courses for Security Awareness
- Add Data Protection to the Security Awareness Program
- Include the IT security department in orientation classes
- Map acceptable use policy
- Provide Security Awareness in a new IT, existing newsletters or Digital Signage
- Provide adequate training for new technologies

Baseline

Develop

Deliver

Measure

e- Learning Platform

Professional Consulting Security Programs

IT (Governance, Risk and Compliance) - **GRC**
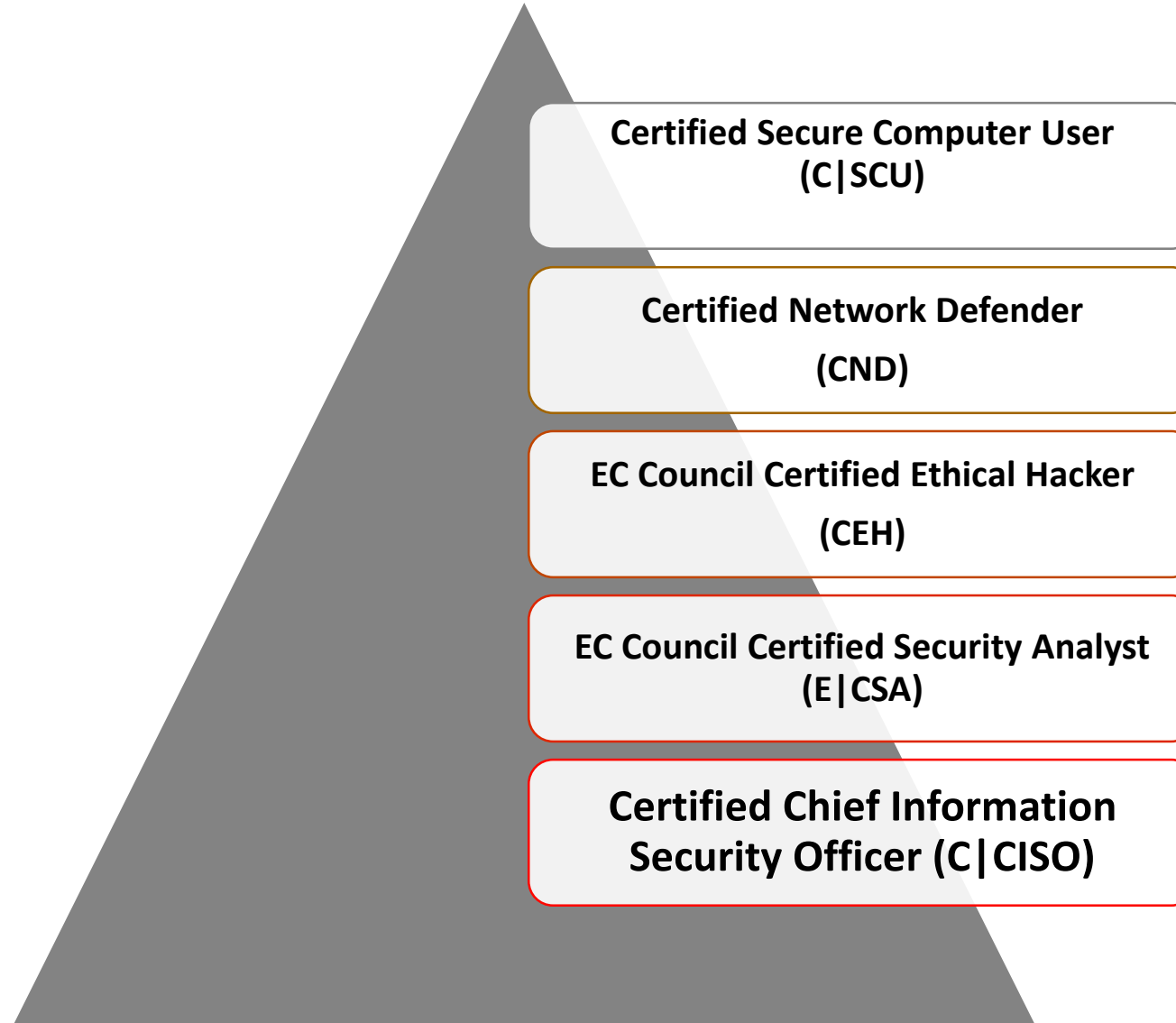
Managing Operational Resilience - **MOR**

Security Awareness & Simulation Program – **SAS**

Security Training Program - **STP**

Security Training Program – EC-Council Certified

Certified Secure Computer User (C|SCU)

Certified Network Defender (CND)

EC Council Certified Ethical Hacker (CEH)

EC Council Certified Security Analyst (E|CSA)

Certified Chief Information Security Officer (C|CISO)

Hire CISO

1 — Direct and approve the design of security systems

2 — Review and approve security policies, controls and incident response planning

3 — Schedule periodic security audits

4 — Manage all teams, employees, contractors and vendors involved in IT security, which may include hiring

VISION

We believe in talents to provide innovative-alternative ways to change the world.

Mission

Our mission is to inspire and transform businesses into the new digital era through smart minds, research and alternative solutions.