Standar Keamanan Informasi

Anwar Siregar

Senior Manager

Business Development

19 May 2016

Information Security - Creating trust in digital WORLD

- **Cybersecurity is a top global concern. 82% of enterprises expect to experience a cyber incident in 2015**
- **More than 35% are unable to fill open cybersecurity positions**
- **69% say certification is required for cybersecurity jobs**
- **33% say qualified candidates have hands-on experience**
- **46% say technical skills are needed**
- **There is a cybersecurity skills crisis: 1 million unfilled jobs (source: Cisco)**
- **The research is clear. Cybersecurity has evolved from critical topic into a public safety issue**

Source: ISACA

TOP PRIORITIES for INFORMATION SECURITY

EY's Global Information Security Survey 2015 – Sector highlights			
Industries	**Likely sources of cyber attacks**	**Top priorities for information security**	**Companies not changing security budget over next 12 months**
Consumer products	Employees: **61%** Criminal syndicates: **52%** External contractors: **43%**	Business continuity/disaster recovery resilience: **59%** Data leakage/data loss prevention: **50%** Incident response capabilities: **40%**	**38%**
Banking and capital markets	Cyber attacks to steal financial information: **21%** Malware: **20%** Fraud: **19%**	Data leakage/data loss prevention: **67%** Business continuity/disaster recovery: **56%** Identify and access management: **56%**	**33%**
Power and utilities	Outdated security information, careless or unaware employees, malware: **20%** each	Business continuity/disaster protection: **52%** Data leakage/data loss prevention: **44%** Security operations, such as anti-virus, patching, encryption: **43%**	**33%**

Source: EY's

Information Security – Drivers

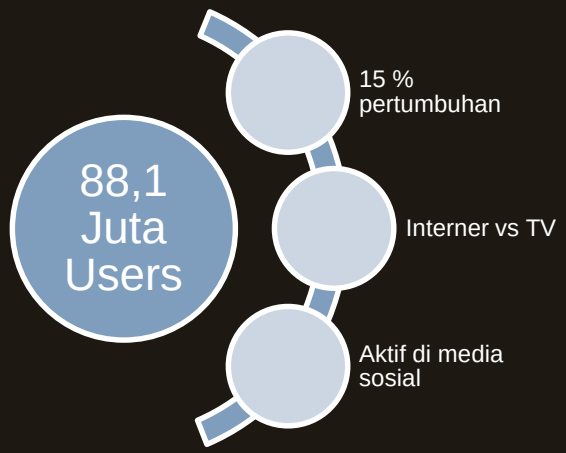
DIGITAL WORD

- Mobile devices
- Social media
- Cloud services
- Security as a service
- Community awareness
- Non Standard

Regulatory & Standard

- UU ITE No. 11 Tahun 2008
- UU HAKI No 28 Tahun 2014
- UUKependuduka No 24 Tahun 2013
- Peraturan Menteri Kominfo No 4 Tahun 2016
- ISO 27001
- Other Regulation

TOP 3 CYBER THREATS



52%
Social
Engineering

39%
Persistent
Threats

40%
Insider
Threats

Source: Liputan 6

TOP 6 Country – Internet Users

Top 25 Countries, Ranked by Internet Users, 2013-2018
millions

	2013	2014	2015	2016	2017	2018
1. China*	620.7	643.6	669.8	700.1	736.2	777.0
2. US**	246.0	252.9	259.3	264.9	269.7	274.1
3. India	167.2	215.6	252.3	283.8	313.8	346.3
4. Brazil	99.2	107.7	113.7	119.8	123.3	125.9
5. Japan	100.0	102.1	103.6	104.5	105.0	105.4
6. Indonesia	72.8	83.7	93.4	102.8	112.6	123.0
7. Russia	77.5	82.9	87.3	91.4	94.3	96.6
8. Germany	59.5	61.6	62.2	62.5	62.7	62.7
9. Mexico	53.1	59.4	65.1	70.7	75.7	80.4
10. Nigeria	51.8	57.7	63.2	69.1	76.2	84.3
11. UK**	48.8	50.1	51.3	52.4	53.4	54.3
12. France	48.8	49.7	50.5	51.2	51.9	52.5
13. Philippines	42.3	48.0	53.7	59.1	64.5	69.3
14. Turkey	36.6	41.0	44.7	47.7	50.7	53.5
15. Vietnam	36.6	40.5	44.4	48.2	52.1	55.8
16. South Korea	40.1	40.4	40.6	40.7	40.9	41.0
17. Egypt	34.1	36.0	38.3	40.9	43.9	47.4
18. Italy	34.5	35.8	36.2	37.2	37.5	37.7
19. Spain	30.5	31.6	32.3	33.0	33.5	33.9
20. Canada	27.7	28.3	28.8	29.4	29.9	30.4
21. Argentina	25.0	27.1	29.0	29.8	30.5	31.1
22. Colombia	24.2	26.5	28.6	29.4	30.5	31.3
23. Thailand	22.7	24.3	26.0	27.6	29.1	30.6
24. Poland	22.6	22.9	23.3	23.7	24.0	24.3
25. South Africa	20.1	22.7	25.0	27.2	29.2	30.9
Worldwide* **	**2,692.9**	**2,892.7**	**3,072.6**	**3,246.3**	**3,419.9**	**3,600.2**

*Note: individuals of any age who use the internet from any location via any device at least once per month; *excludes Hong Kong; **forecast from Aug 2014; ***includes countries not listed*
Source: eMarketer, Nov 2014

181948 www.eMarketer.com

Source: kominfo.go.id

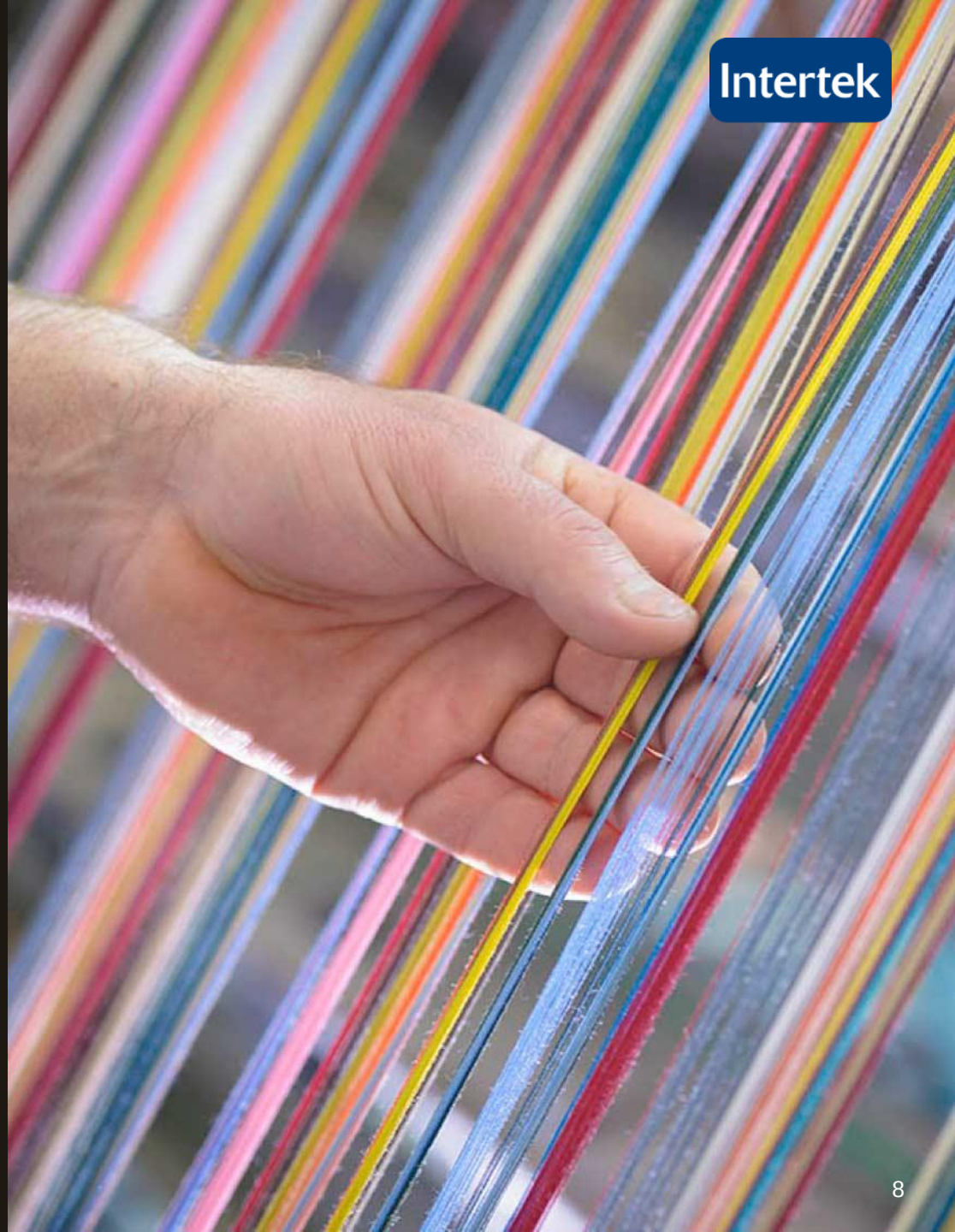
ISO 27001 – By Country

TOTAL CERTIFIED in the WORLD : 22293

ISO/IEC 27001 - East Asia and Pacific								
Year	2006	2007	2008	2009	2010	2011	2012	2013
Country	4210	5550	5807	7394	8788	9665	10422	10748
Australia	59	55	63	55	82	94	113	138
Cambodia				1	1			0
China	75	146	236	459	957	1219	1490	1710
Hong Kong, China	29	36	59	72	78	99	110	124
Macau, China	2	5	2	7	9	12	13	15
Taipei, Chinese	159	256	702	934	1028	791	855	861
Fiji								1
Indonesia	2	3	7	13	22	29	35	48
Japan	3790	4896	4425	5508	6237	6914	7199	7084
Korea, Democratic People's Republic			95		1	0	1	0
Korea, Republic of	50	77	94	174	166	191	230	252
Malaysia	18	23	34	38	60	72	100	181
Mongolia								1
Myanmar				1	1			0
New Zealand	1	1	4	5	5	5	5	12
Philippines	10	24	27	47	38	59	66	73
Singapore	7	17	36	41	43	68	65	84
Thailand	7	9	16	34	39	76	96	125
Viet Nam	1	2	7	5	21	36	44	39

03

ISO 27001



Information asset

Knowledge or data that has value to the organisation

- Printed or written on **paper**
- Stored **electronically**
- Transmitted by post or using electronic means
- Shown on corporate **videos**
- **Verbal** - spoken in conversations
- '… Whatever form the information takes, or means by which it is shared or stored, it should always be appropriately protected.' (ISO 27002)

ISO 27001 – A Management System

Information Security Management System

Part of the overall management system, based on a business risk approach, to **establish, implement, operate, monitor, review, maintain** and **improve** information security

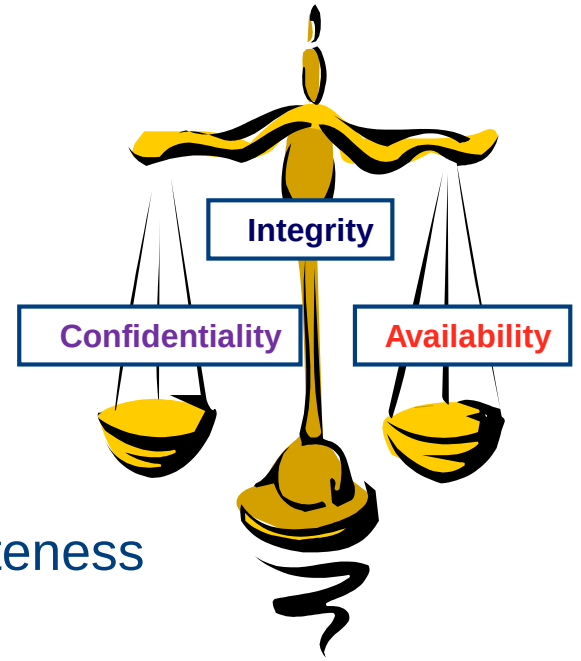
ISO 27001 – “IS ALL ABOUT **RISK”**

What is information security?

ISO 27001:2013 defines Information Security as

Preservation of

- **Confidentiality**: information is not made available or disclosed to unauthorized individuals, entities, or processes
- **Integrity**: safeguarding the accuracy and completeness of assets
- **Availability**: being accessible and usable upon demand by an authorized entity of information



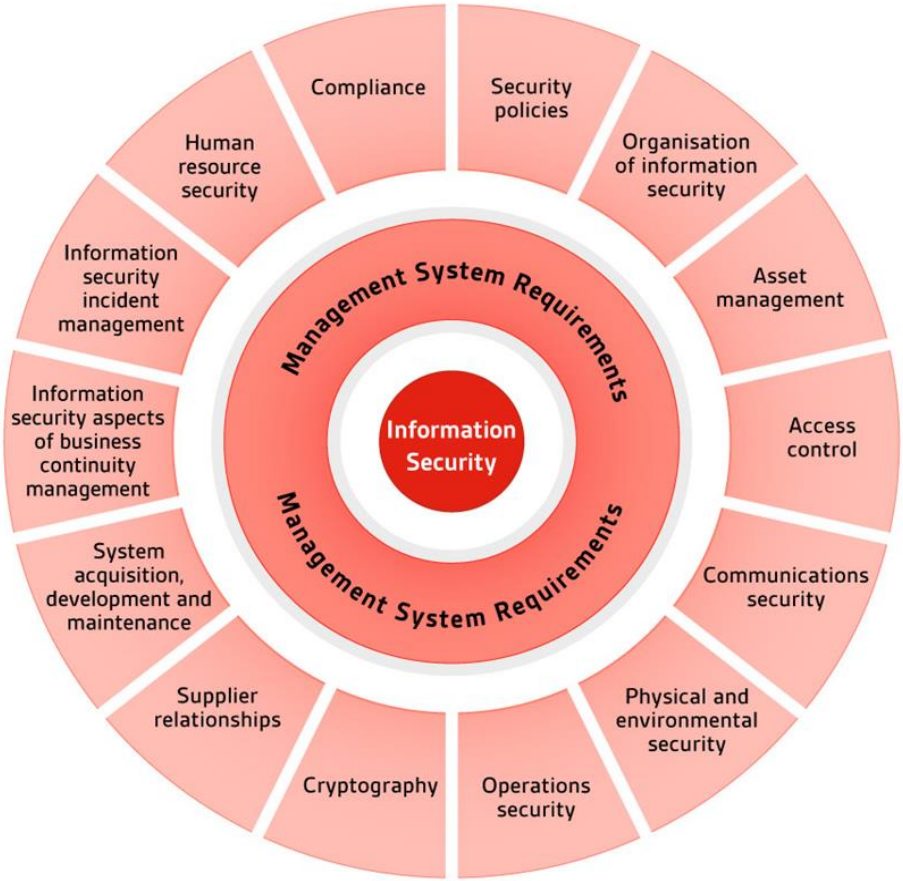
Note: In addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved

Annex A

14 security clause headings

35 security categories

114 controls



Benefits of ISO 27001 & Certification

Systemic and Holistic approach

Benefit from **best practice** as captured in the standard

Increase **confidence** of the organisation in its information security processes

Neutral internationally recognised system—helps overcome ‘not invented here’ syndrome

Eases challenges of bringing systems together—in different parts of an organisation, interoperability, etc

Helps avoid arguments about which way is best in one or another person’s opinion

Improve information security management

Reduce probability of information **security breaches**

Benefits of IMPLEMENTATION - SWOT

Strengths	Weaknesses
•Improved net security level of the organization •Demonstrated conformity with compliance requirements •External expertise & assistance brings good practices •Other……to be added by the delegates	•Requires resources: ✓-material ✓-time •Distracts personal from other important tasks •Other……to be added by the delegates
Opportunities	**Threats**
•Asset in marketing •Improved security for client's and partner's information •Opportunities for improvement identified •Other……to be added by the delegates	•Possible access to the organization's info if external assistance is not properly managed •Overconfidence in ISMS as form of total protection (it is not and is not intended to be) •Other……to be added by the delegates

The ISO 27001 family of standards

ISO 27000 – Overview and vocabulary

ISO 27001 – Audit Requirements

ISO 27002 – Code of Practice (was ISO 17799:2005)

ISO 27003 – Implementation Guidance

ISO 27004 – Measurement

ISO 27005 – Risk Management

ISO 27006 – Requirements for Bodies providing Audit and Certification of ISMSs

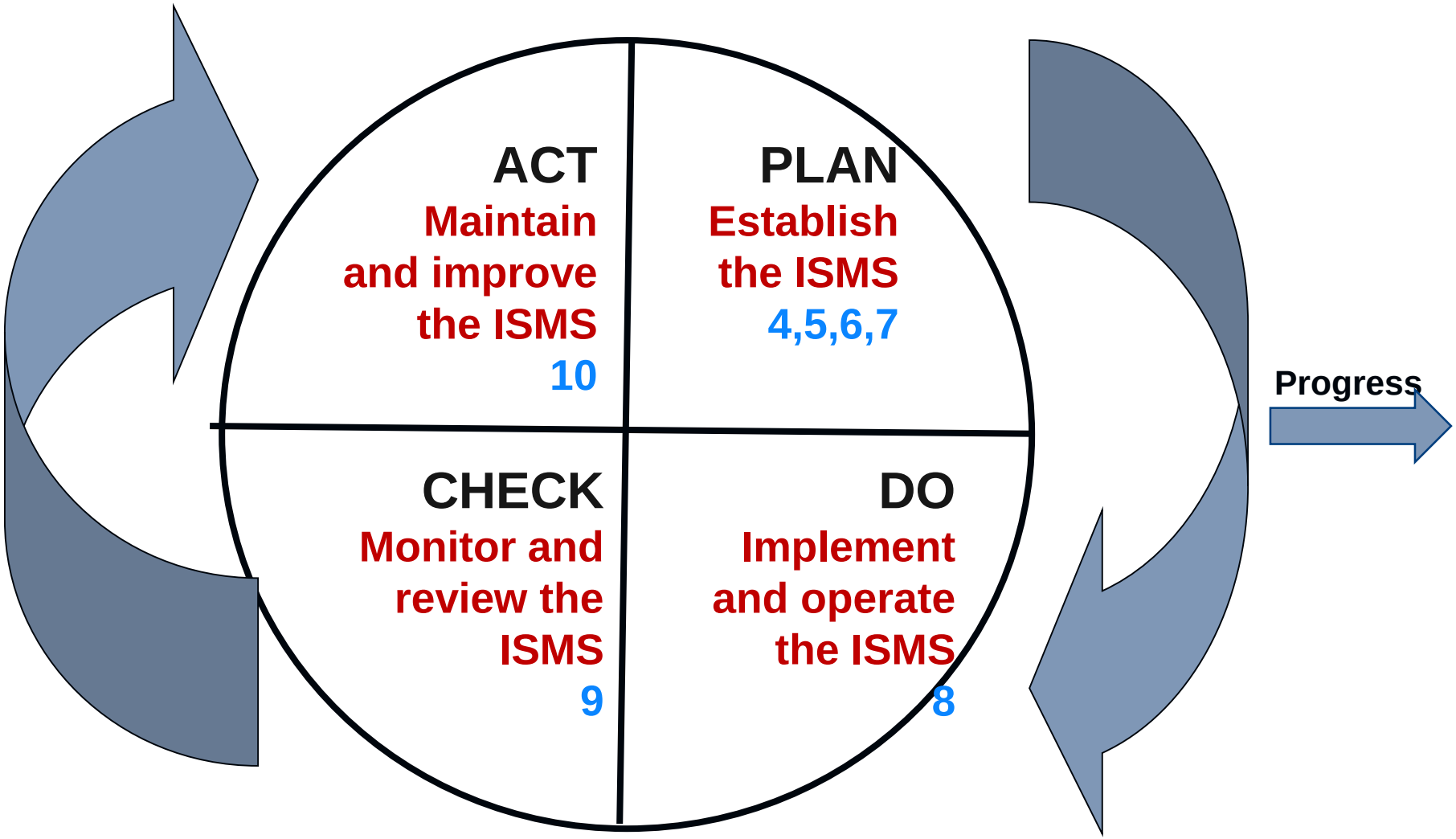
Also relevant:

BS 7799-3:2006 – Risk Management

BS 31100:2011 – Risk Management Code of Practice

ISO TR 18044:2004 Information Security Incident Management

ISO 27001:2013



ISO 27001 Components Overview

PLAN

4 Context of the organization

- Understanding of context.
- Expectations of interested parties.
- Scope and ISMS.

5 Leadership

- Management commitment.
- IS policy.
- Roles, responsibilities and authorities.

6 Planning

- Actions to address risk and opportunity.
- IS objectives.

7 Support

- Resources.
- Competence.
- Awareness.
- Communication.
- Documented Information.

DO

8 Operation

- Operational planning and control.
- Risk assessment.
- Risk treatment.

CHECK

9 Performance and Evaluation

- Monitoring, measurement, analysis and evaluation.
- Internal audit.
- Management review.

ACT

10 Improvement

- Nonconformity and corrective action.
- Continual improvement.

Auditor - Behaviour

- **ethical**, i.e. fair, truthful, sincere, honest and discreet;
- **open-minded**, i.e. willing to consider alternative ideas or points of view;
- **diplomatic**, i.e. tactful in dealing with people;
- **observant,** i.e. actively observing physical surroundings and activities;
- **perceptive**, i.e. aware of and able to understand situations;
- **versatile**, i.e. able to readily adapt to different situations;
- **tenacious**, i.e. persistent and focused on achieving objectives;
- **decisive**, i.e. able to reach timely conclusions based on logical reasoning and analysis;
- **self-reliant**, i.e. able to act and function independently whilst interacting effectively with others;

Auditor - Behaviour

- **acting with fortitude**, i.e. able to act responsibly and ethically, even though these actions may not always be popular and may sometimes result in disagreement or confrontation;
- **open to improvement**, i.e. willing to learn from situations, and striving for better audit results;
- **culturally sensitive**, i.e. observant and respectful to the culture of the auditee;
- **collaborative**, i.e. effectively interacting with others, including audit team members and the auditee’s personnel.

END