DIRK MAIJ, CISSP
ONYX CYBERSECURITY

ISO27000 MICRO BOOT CAMP

ONYX
CYBER SECURITY

THEORETICAL PART

- WHAT IS ISO27000
- HOW DOES AN IMPLEMENTATION PROJECT

PRACTICAL PART

- MICRO IMPLEMENTATION

AGENDA

ONYX
CYBER SECURITY

NO MOBILE PHONES OR AT LEAST SET TO QUIET

FREE TO ASK QUESTIONS, RAISE HAND

FREE TO GIVE REMARKS, KEEP IT IN CONTEXT

PRESENTATION RULES

ONYX
CYBER SECURITY

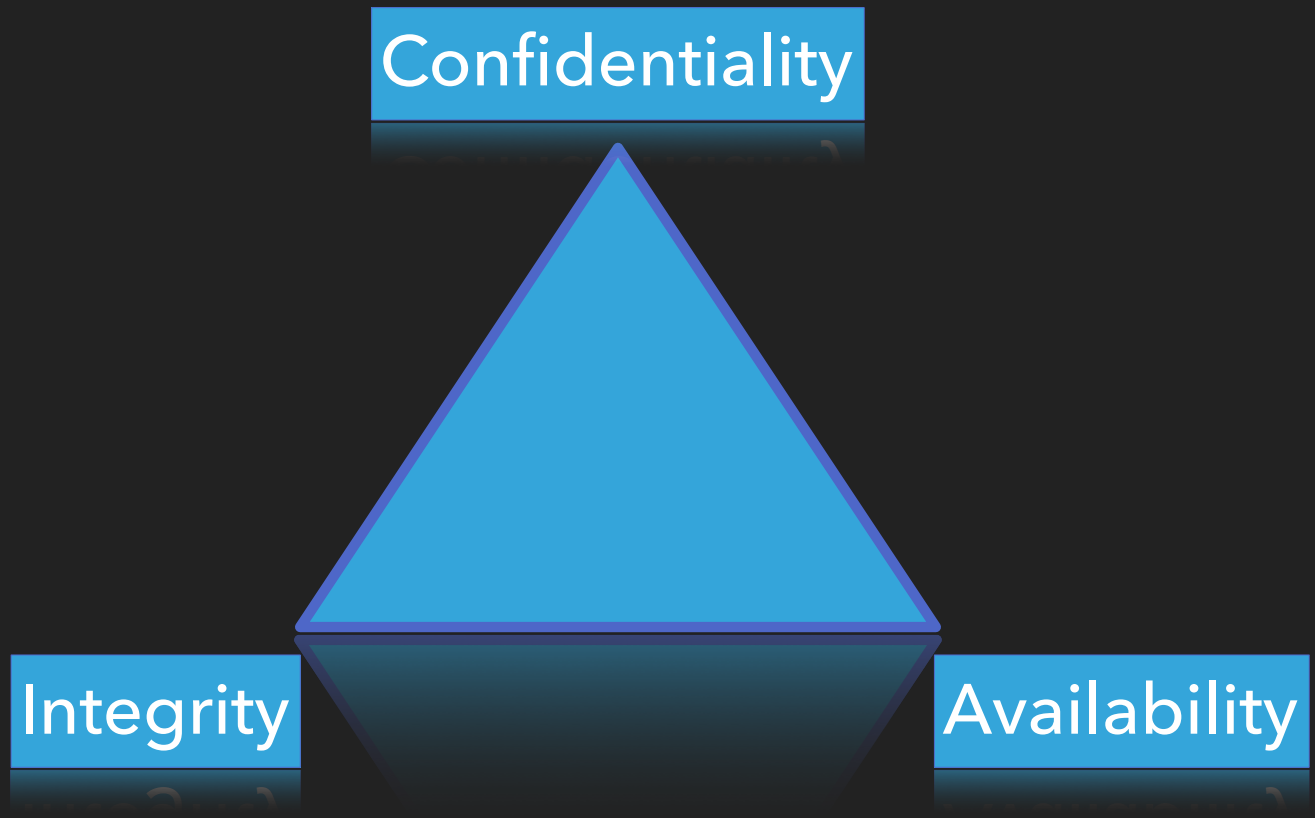
THE THEORY

ONYX
CYBER SECURITY

WHAT IS INFORMATION ANYWAY?

INFORMATION SECURITY

ONYX
CYBER SECURITY



CIA TRIAD

INTERNATIONAL STANDARD FRAMEWORK
MOST POPULAR STANDARD WORLDWIDE
SET OF AROUND 30 DOCUMENTS
1 PARTICULARLY INTERESTING ISO 27001

WHAT IS ISO27K

ONYX
CYBER SECURITY

https://www.youtube.com/watch?v=Mpt5_RsLH6o

COMPLIANCE TO LAW OR REGULATION (SOX, BASEL III, PCI-DSS, ETC)
BETTER MARKET POSITION
LOWERING COST
IMPROVING COMPANY PROCESSES

WHY ISO27K?

ONYX
CYBER SECURITY

CYBERSECURITY FRAMEWORK (NIST)
STANDARD OF GOOD PRACTICE (ISF)
NIST SP 800 SERIES
RISK FRAMEWORKS LIKE COBIT, OCTAVE, COSO ETC

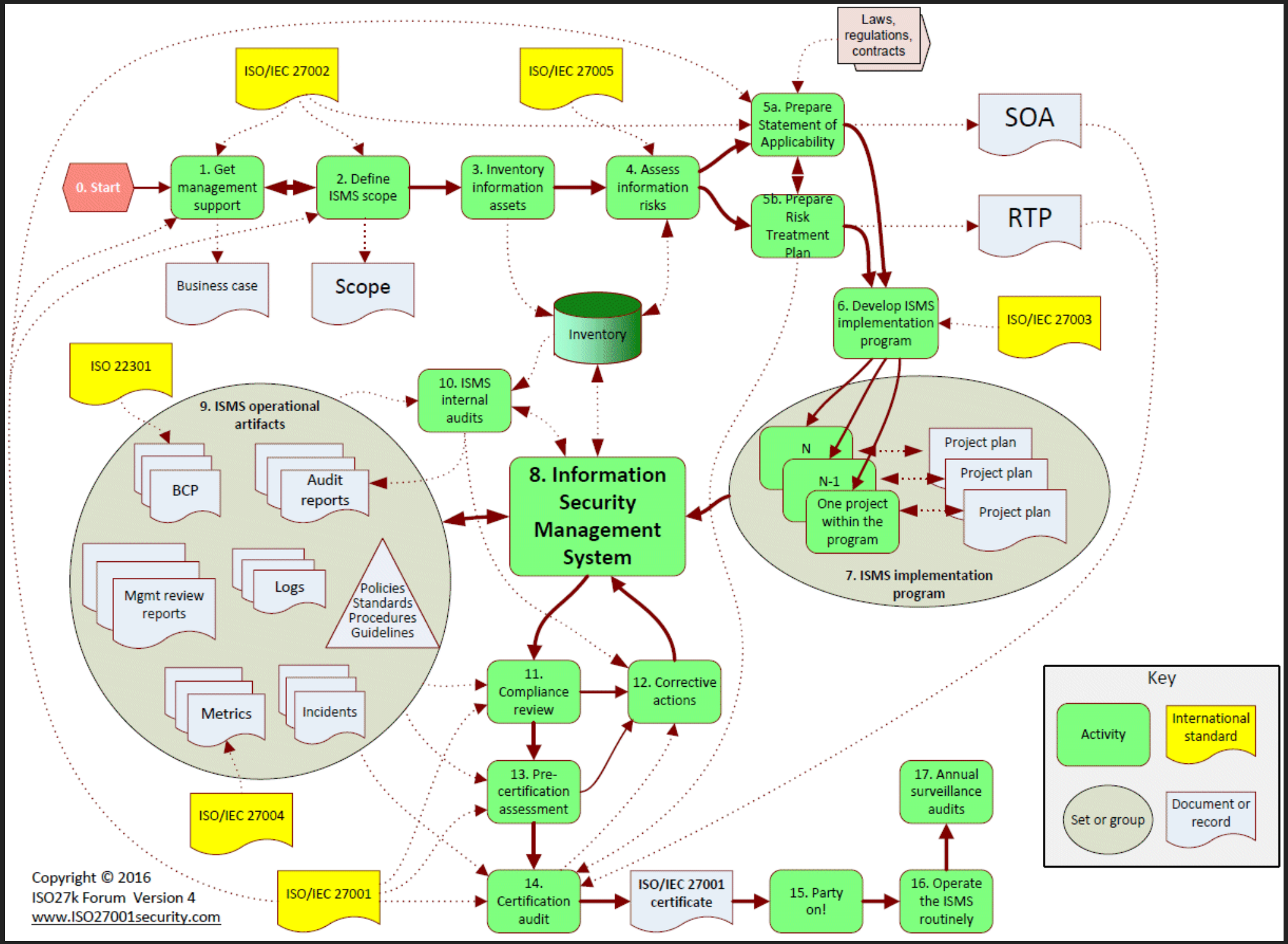
ALTERNATIVES TO ISO27K

ONYX
CYBER SECURITY

CERTIFICATION
CONTINUOUS IMPROVEMENT
INTERNATIONALLY ACCEPTED
RELATIVELY WELL KNOWN, SO MUCH INFORMATION AVAILABLE

MAIN ADVANTAGES OF ISO

ONYX
CYBER SECURITY


Laws, regulations, contracts
ISO/IEC 27002
ISO/IEC 27005
5a. Prepare Statement of Applicability
SOA
0. Start
1. Get management support
2. Define ISMS scope
3. Inventory information assets
4. Assess information risks
5b. Prepare Risk Treatment Plan
RTP
Business case
Scope
Inventory
6. Develop ISMS implementation program
ISO/IEC 27003
ISO 22301
10. ISMS internal audits
9. ISMS operational artifacts
BCP
Audit reports
Mgmt review reports
Logs
Policies Standards Procedures Guidelines
Metrics
Incidents
8. Information Security Management System
N
N-1
One project within the program
Project plan
Project plan
Project plan
7. ISMS implementation program
11. Compliance review
12. Corrective actions
13. Pre-certification assessment
17. Annual surveillance audits
ISO/IEC 27004
ISO/IEC 27001
14. Certification audit
ISO/IEC 27001 certificate
15. Party on!
16. Operate the ISMS routinely
Key
Activity
International standard
Set or group
Document or record
Copyright © 2016
ISO27k Forum Version 4
www.ISO27001security.com

SET OF POLICIES, PROCEDURES, STANDARDS AND GUIDELINES
AGREED TO BY MANAGEMENT
IN PLACE TO PROTECT INFORMATION / ASSETS
ESSENTIALLY MANAGES RISK

INFORMATION SECURITY MANAGEMENT SYSTEM

ONYX
CYBER SECURITY

THE PROBABILITY OR THREAT OF QUANTIFIABLE DAMAGE, INJURY, LIABILITY, LOSS, OR ANY OTHER NEGATIVE OCCURRENCE THAT IS CAUSED BY EXTERNAL OR INTERNAL VULNERABILITIES, AND THAT MAY BE AVOIDED THROUGH PREEMPTIVE ACTION.

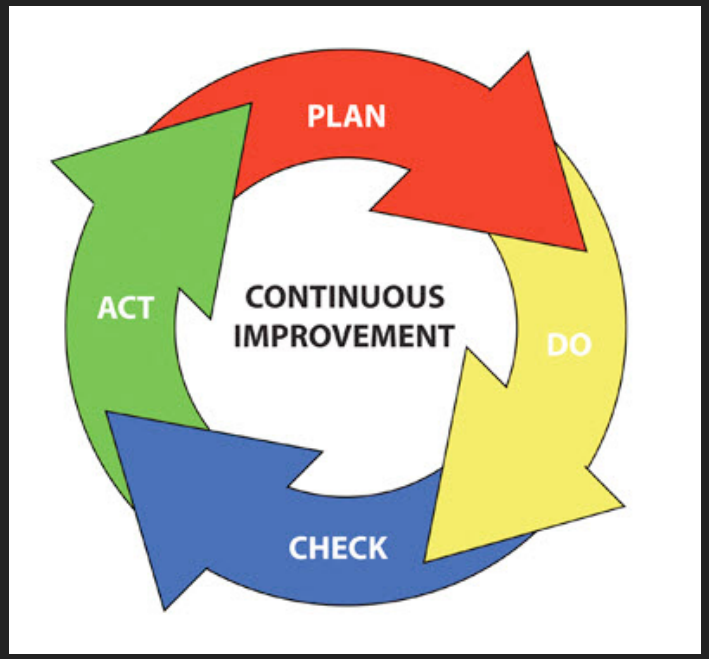
RISK

ONYX
CYBER SECURITY

ASSET BASED
ISACA RISK IT FRAMEWORK / COBIT 5
COSO
OCTAVE
CRAMM
STANDARDS OF GOOD PRACTICE
FAIR

RISK MANAGEMENT METHODS

ONYX
CYBER SECURITY



PLAN (4,5,6)
DO (7,8)
CHECK (9)
ACT (10)

PHASES OF THE PROJECT

ONYX
CYBER SECURITY

GET MANAGEMENT SUPPORT
DETERMINE SCOPE
CREATE INVENTORY OF INFORMATION ASSETS
ANALYSE RISKS AND DETERMINE TREATMENT

PLAN

ONYX
CYBER SECURITY

EXECUTE RISK TREATMENT CONTROLS
MONITOR AND MEASURE CONTROLS

DO

ONYX
CYBER SECURITY

ANALYSE MEASUREMENTS

REVIEW ISMS

CHECK

ONYX

CYBER SECURITY

PERFORM CORRECTIVE ACTIONS
ADJUST ISMS
CONTINUAL IMPROVEMENT

ACT

ONYX
CYBER SECURITY

CERTIFICATION

ONYX
CYBER SECURITY

PHASE 1: DOCUMENTATION AUDIT
PHASE 2: MAIN AUDIT
SURVEILLANCE VISITS (YEARLY)
3 YEARS VALID, AFTER THAT RECERTIFICATION NEEDED

CERTIFICATION

ONYX
CYBER SECURITY

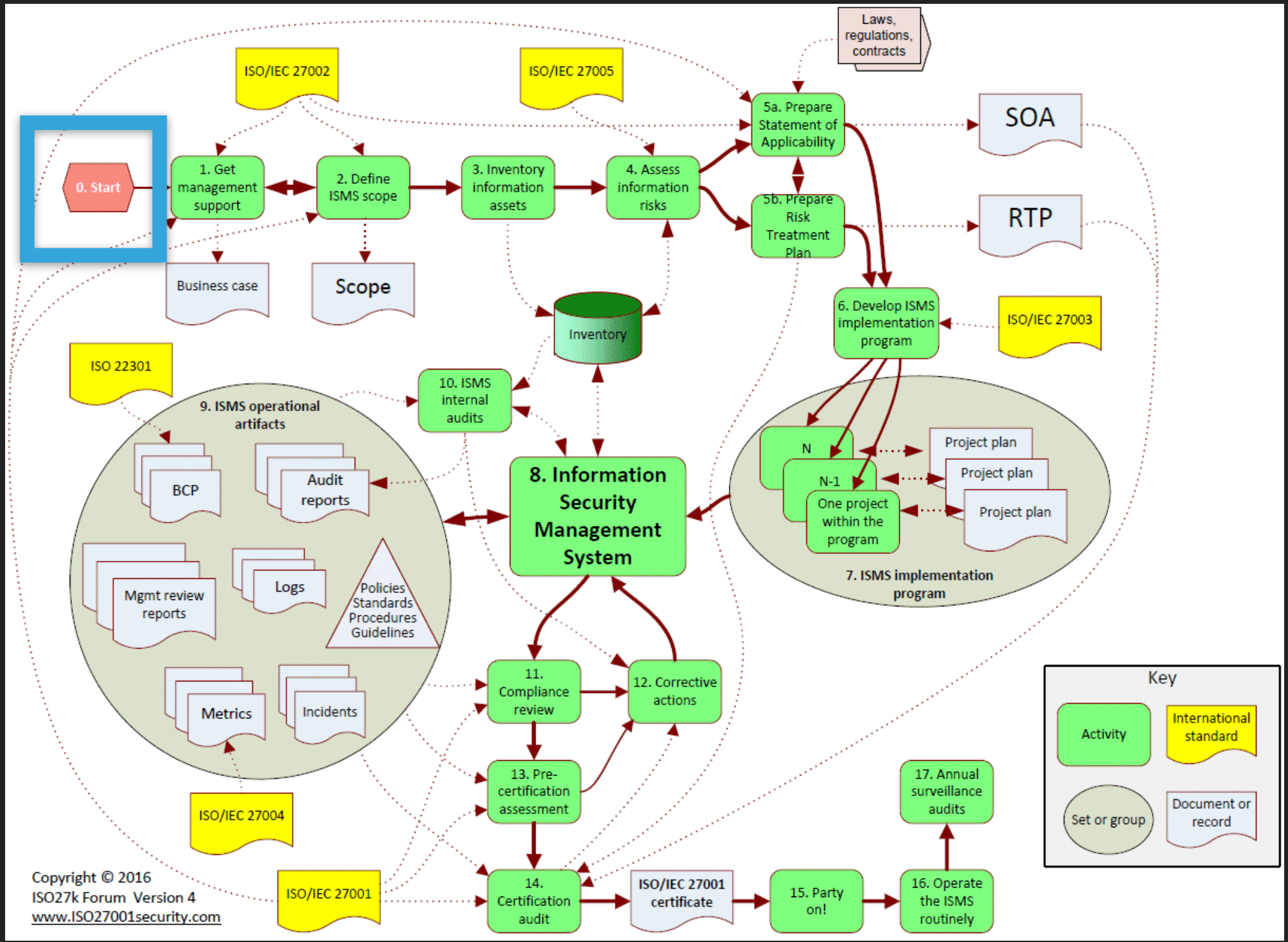
https://www.youtube.com/watch?v=AskktIDYe3A

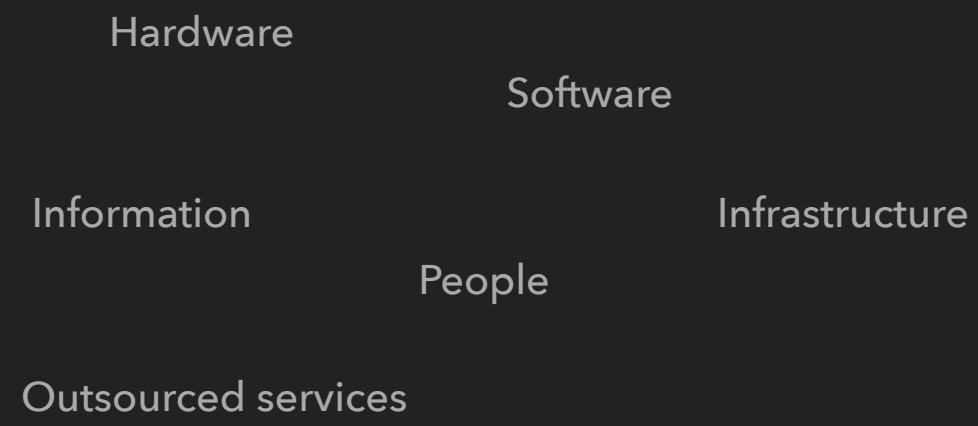
chris davenport
https://www.youtube.com/watch?

ISO27001 MICRO BOOT CAMP

IN PRACTICE

ONYX
CYBER SECURITY


Laws, regulations, contracts
ISO/IEC 27002
ISO/IEC 27005
0. Start
1. Get management support
2. Define ISMS scope
3. Inventory information assets
4. Assess information risks
5a. Prepare Statement of Applicability
5b. Prepare Risk Treatment Plan
SOA
RTP
Business case
Scope
Inventory
6. Develop ISMS implementation program
ISO/IEC 27003
ISO 22301
10. ISMS internal audits
9. ISMS operational artifacts
BCP
Audit reports
Mgmt review reports
Logs
Policies Standards Procedures Guidelines
Metrics
Incidents
8. Information Security Management System
N
N-1
One project within the program
Project plan
Project plan
Project plan
7. ISMS implementation program
11. Compliance review
12. Corrective actions
13. Pre-certification assessment
17. Annual surveillance audits
ISO/IEC 27004
ISO/IEC 27001
14. Certification audit
ISO/IEC 27001 certificate
15. Party on!
16. Operate the ISMS routinely
Key
Activity
International standard
Set or group
Document or record
Copyright © 2016
ISO27k Forum Version 4
www.ISO27001security.com



PICK 5 IMPORTANT ASSETS

ONYX
CYBER SECURITY

THREATS

Falsification of records

Fire

Flood

Fraud

User error

Loss of electricity

Software errors

Theft

Social engineering

Unauthorized use of copyright material

VULNERABILITIES

Default passwords not changed

Inadequate physical protection

Inadequate security awareness

Location vulnerable to flooding

Too much power in one person

Unmotivated employees

Uncontrolled download from the Internet

PER ASSET, PICK 2 THREATS AND VULNERABILITIES

ONYX
CYBER SECURITY

QUALITATIVE

Low

Medium

High

QUANTITATIVE

Probability %

Value $

Cost of incident $

DETERMINE LIKELIHOOD / IMPACT

ONYX
CYBER SECURITY

FILL RISK MATRIX

ONYX
CYBER SECURITY

Likelihood + Impact = Risk level

All risks get a value, determine maximum acceptance level (for instance 7)

DETERMINE RISK TREATMENT LEVEL

ONYX
CYBER SECURITY

All risks above risk level

- Mitigate
- Accept
- Transfer
- Avoid

DETERMINE RISKS TO TREAT

ONYX
CYBER SECURITY

For all mitigated risks, choose risk treatment

DETERMINE RISK TREATMENT

ONYX
CYBER SECURITY

RINSE AND REPEAT

D.MAIJ@ONYX-CYBERSECURITY.COM
+31(0) 612 930 341

DISCUSSION

ONYX
CYBER SECURITY