mobile business

Lecture 12

Information Security Management

Information & Communication Security
(WS 2014/15)

Prof. Dr. Kai Rannenberg

T-Mobile Chair of Mobile Business & Multilateral Security
Goethe University Frankfurt a. M.

mobile business

Agenda

- Introduction
- Laws and standards in the information security context
- Several concepts
- Comparison of the concepts
- ISMS according to ISO 27001 - Part 1
  - ISMS model
  - ISMS PDCA process model

mobile business

Agenda

- ISMS according to ISO 27001 – Part 2
  - Plan: ISMS determination and administration
  - Do: ISMS implementation and operation
  - Check: ISMS monitoring and checking
  - Act: ISMS cultivation and improvement
  - Summary
- References

Introduction

- Security of information and information processing is getting more important for the long-time success of organisations.
- Therefore there is a growing need for the employment of qualified management processes focusing on Information Security.
- Development of ISO 270nm is one answer to this need.

Introduction

- Information Security management tasks

→ Get relevant processes in place.

→ Create a responsible organizational structure.

→ Make Information Security a business objective !

Laws and standards related to information security

Germany:

- KonTraG, AktG (§91 (2)), HGB (§ 289(1)), AO (§§ 146/147), GDPdU, GoBS, Kreditwesengesetz, BDSG, …
- Produkthaftungsgesetz (ProdHaftG) bzw. BGB (§ 823), Teledienstgesetz (TDG), Teledienstdatenschutzgesetz (TDDSG)
- GG Art.10 (Brief-, Post- und Fernmeldegeheimnis), G10-Gesetz (Beschränkung von GG Art.10)
- Urheberrechtsgesetz (UrHG), Sicherheitsüberprüfungsgesetz (SüG)

International:

- Basel II, Solvency II, Sarbanes-Oxley, COSO

mobile business

Laws and ***standards*** related to information security

- ISO 270nm: Information security management
- IT Baseline Protection (BSI[1] IT-Grundschutz)
- COBIT: Control Objectives for Information and related Technology
- ISO 9000: Quality management
- ISO 14000: Environmental management
- ISO 20000: Information Technology - Service management (ITIL)
- PCI-DSS – PCI[2] Data Security Standard

[1] Bundesamt für Sicherheit in der Informationstechnik, [2] **P**ayment **C**ard **I**ndustry

Several Concepts

- Several concepts and approaches to Information Security Management are existing today
- Examples:
  - Traditional Information Security
  - IT Baseline Protection
  - **ISO 270nm: Information Security Management**

→ **This lecture is focusing on ISO270nm**

ISO 27000-series (1/2)

- ISO 27000: Information security management systems - Overview and vocabulary
- ISO 27001: Information security management systems — Requirements
- ISO 27002: Code of practice for information security controls
- ISO 27003: Information security management system implementation guidance
- ISO 27004: Information security management — Measurement
- ISO 27005: Information security risk management
- ISO 27006: Requirements for bodies providing audit and certification of information security management systems
- ISO 27007: Guidelines for information security management systems auditing
- ISO TR 27008: Guidelines for auditors on information security management systems controls
- ISO 27010: Information security management for inter-sector and inter-organisational communications
- ISO 27011: Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
- ISO 27013: Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
- ISO 27014: Governance of information security
- ISO TR 27015: Information security management guidelines for financial services
- ISO TR 27016: Information security management – Organizational economics
- ISO 27018: Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy industry

ISO 27000-series (2/2)

- ISO TR 27019: Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy industry
- ISO 27031: Guidelines for information and communications technology readiness for business continuity
- ISO 27032: Guidelines for cybersecurity
- ISO 27033-1: Network security overview and concepts
- ISO 27033-2: Guidelines for the design and implementation of network security
- ISO 27033-3: Reference networking scenarios - threats, design techniques and control issues
- ISO 27033-4: Securing communications between networks using security gateways
- ISO 27033-5: Securing communications across networks using Virtual Private Networks (VPNs)
- ISO 27034-1: Application security — Overview and concepts
- ISO 27035: Information security incident management
- ISO 27036-3: Information security for supplier relationships – Guidelines for ICT supply chain security
- ISO 27037: Guidelines for identification, collection, acquisition, and preservation of digital evidence
- ISO 27038: Specification for digital redaction
- ISO 27799: Health informatics — Information security management in health using ISO/IEC 27002

ISMS according to ISO 27001

- According to ISO 27001 an Information Security Management System (ISMS) is defined as:

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

- NOTE: The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.”

ISMS model

- Multiple tasks
  - Shaping information security levels
  - Providing measures to support information security
  - Guidance on how to achieve information security in daily business
  - Maintain and make the information security status apparent
  - Make planned vs. actual comparison of security level comprehensible (audit/certification)
  - Building the foundation for future information security improvements

ISMS model

- ISMS includes the following parts:
  - Organizational structure
  - Responsibilities
  - Planning activities
  - Guidelines and rules
  - Procedures and practices
  - Processes
  - Proceedings
  - Resources

ISMS model

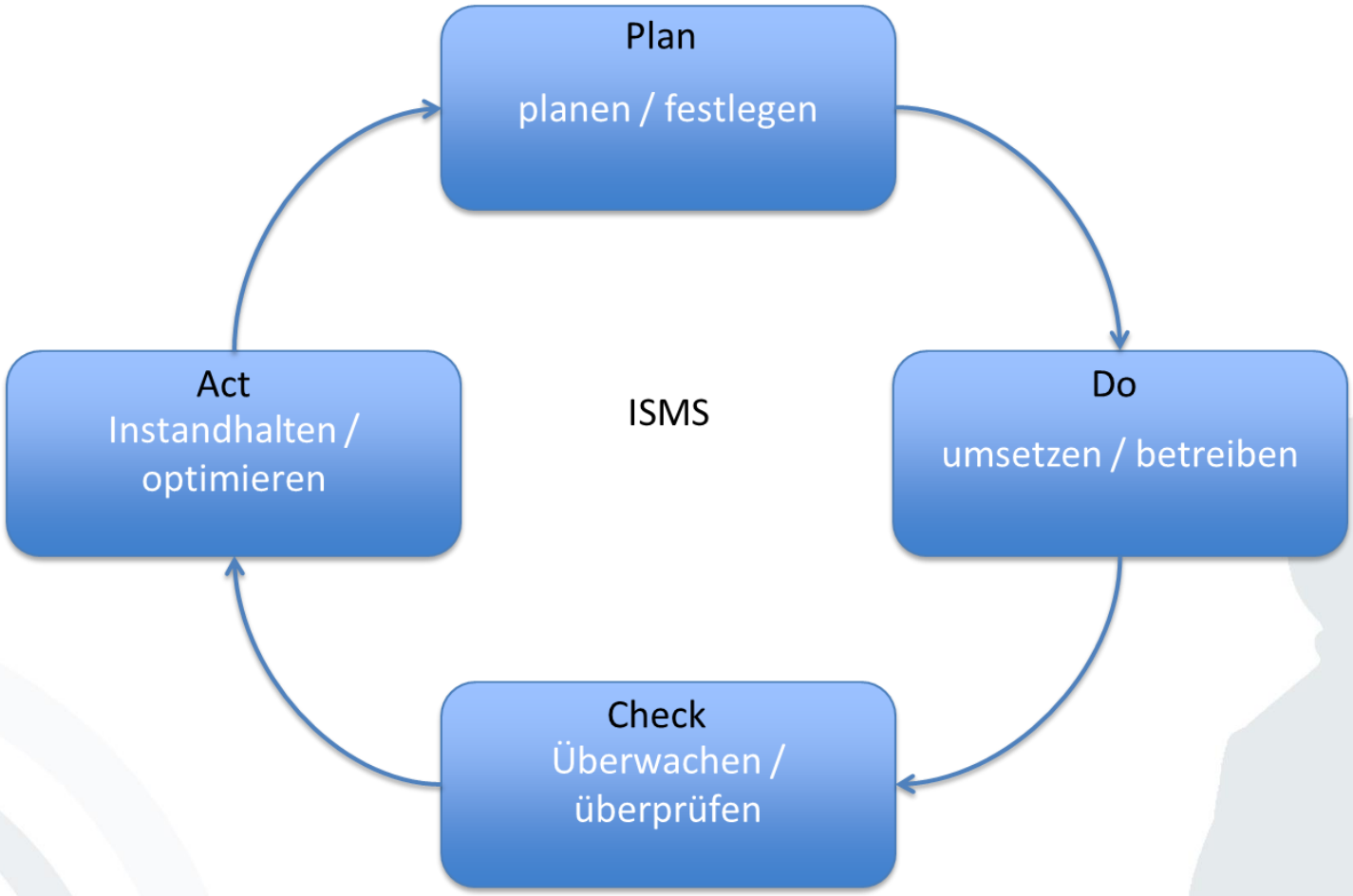
- ISMS's are based on the needs of an specific organisation.
- As organisations evolve over time ISMS's need to be dynamic and scalable:
  - Simple situations → simple solutions
  - Complex situations → advanced solutions
- The activities to introduce and to operate an ISMS are organised as a process.

ISMS “life-cycle”

- Continuous Improvement: Processes can be improved easily by the adoption of an underlying improvement cycle e.g. PDCA process model (Deming-cycle)

- Basic activities:
  - P = Plan -> plan/determine ISMS
  - D = Do -> realise/operate ISMS
  - C = Check -> monitor/examine ISMS
  - A = Act -> maintain/optimise ISMS

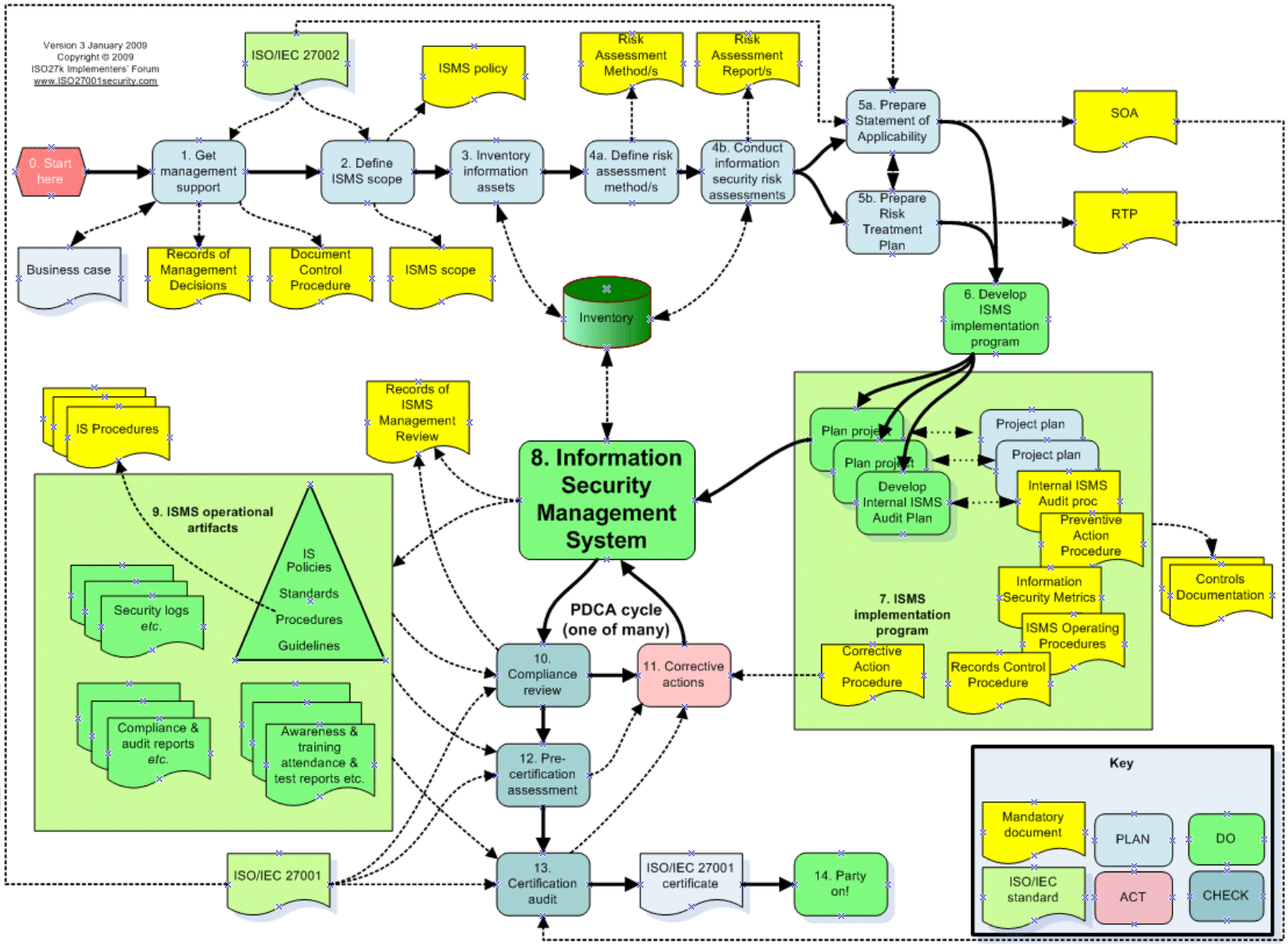
ISMS PDCA process model



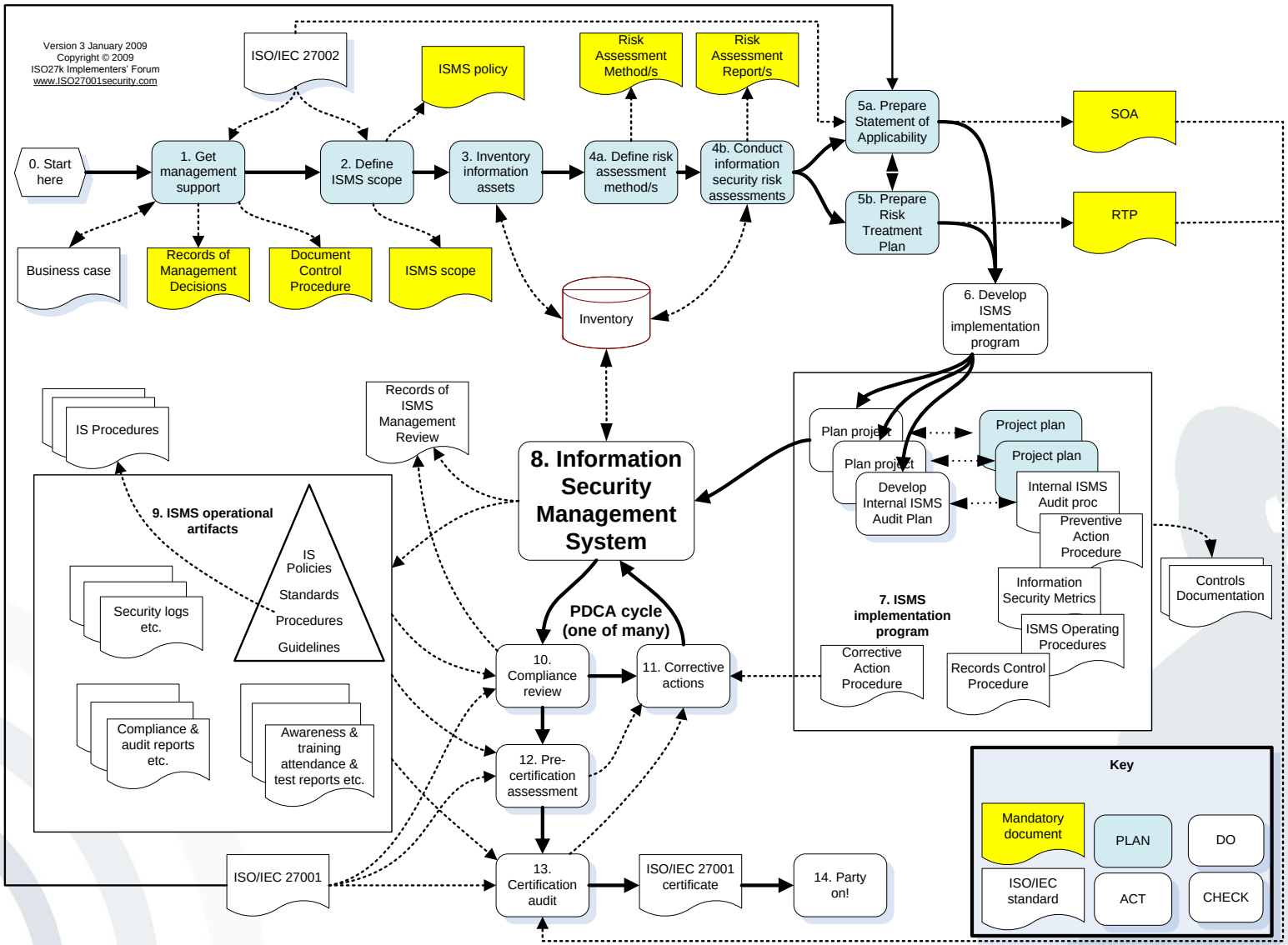
*ISMS: Information Security Management System

mobile business

ISMS PDCA process model



Plan: ISMS **determination** and administration



Plan: ISMS **determination** and administration

- Purposes of the “Plan” phase:
  Based on a management decision to introduce an ISMS a committee for the development of the ISMS is set in place to fulfil the tasks of:
  - Planning a new ISMS
    - One-time task
    - 10 steps a – j
  - Adoption of an existing ISMS to changing/evolving conditions
    - Continuous (usually annual or biannual) task
    - Same but modified 10 steps a* - j*

Plan-a: ISMS **determination** and administration

- ISMS - Field of application/boundaries:
  - Field of application:
    - Freedom of definition e.g. whole/part of the organisation, sites, subset of business processes, set of special information values, …
    - Only enclosed subsections, cross-divisional functions are not excludable
  - Boundaries:
    - Need to be defined/documented
    - Impact on the selection of measures

Plan-b: ISMS **determination** and administration

- Define ISMS / information security policy:
  High level of abstraction without technical details
  - Information security policy
    - Describes business, legal, contractual, and other regulative requirements as well as the duties for the personnel to fulfil these requirements
  - ISMS policy
    - Describes in addition: the prevailing conditions to reach information security, the principles applied, criteria to evaluate risks*
- Policies need to be signed and released by management -> (audit/certification)

* In cooperation with strategic risk management

Plan-c: ISMS **determination** and administration

- Risk assessment modalities:
  - Definition of risk analysis and valuation methods
  - Risk acceptance criteria
  - Classification of risks, e.g. low, medium, high
  - No concrete method given by ISO 270nm, but the need for comparability and comprehensibility

  -> see ISO 27005 for more info

Plan-d: ISMS **determination** and administration

- Identification of risks:
  - Risks are related to information values: therefore information values need to be identified first.
  - Values need to be identified by their owner.
  - Identification of threats (based on values)
  - Identification of vulnerabilities of values, systems, and measures that are exploitable by threats
  - Determining the violation consequences of a value's security goals

  - **Keep in mind: Unidentified risks still remain !!**

Plan-e: ISMS **determination** and administration

- Risk estimation and evaluation:
  - Estimation:
    - Extent of possible damage [EUR] for identified risks
    - Probability of occurrence of damage
  - Evaluation:
    - Definition of risk classes (2 to 4, e.g. tolerable, significant, high, catastrophic)
    - Consequences are related to the overall business activity of an organisation.
  - Residual Risks:
    - Risks to be categorised in one of two categories:
      - Risks to be taken without measures
      - Risks to be taken care of

Plan-f: ISMS **determination** and administration

- Options for risk treatment:
  Three possible options defined by ISO 270nm
  - Risk avoidance
    - Replacing values, systems, measures by comparable objects
    - Healing of vulnerabilities
    - Modification of external facts/influences
  - Transfer business risk to a third party
    - Insurances
    - Suppliers
    - Customers
  - Employment of measures for risk reduction
    - Identification/implementation of measures to reduce the risk -> new classification

Plan-g: ISMS **determination** and administration

- Controls and objectives for unhandled risks (risk management):
  - Controls and objectives can be found in:
    - ISO 27002
    - IT-Baseline Security
  - Organisation can define own controls and objective, should be used economically with regards to audit/certification
  - **Goal** -> downgrading of risks by application of adequate controls

Plan-h: ISMS **determination** and administration

- Management acceptance of residual risks:
  - Based on the work done in Plan-f and Plan-g the management needs to accept and document the acceptance of the residual risks.
  - ISO 270nm explicitly asks for acceptance of the residual risks by the management of the organisation.
  - Management could ask for additional reduction of residual risk.
  - One needs to keep in mind that there is always a chance to have overlooked some risks!

Plan-i: ISMS **determination** and administration

- Order to implement ISMS:
  - The results of Plan-a – Plan-h produced some of the information needed for a decision on the implementation of an ISMS
  - But some additional information is usually needed (not part of ISO 270nm):
    - Expected costs for implementation and operation
    - Necessary labour employment
    - Resource requirements for implementation and operation
  - Result -> Order to implement ISMS

Plan-j: ISMS **determination** and administration

- Statement of applicability:
  - Complete list of selected but not yet implemented controls and objectives
  - Each selected control and objective needs to be well-founded (detailed description).
  - Complete list of already implemented controls and objectives
  - The reason for not having selected specific controls and objectives needs to be well-founded to make sure that no control or objective was overlooked.

Result -> Initial planning phase completed

Plan-a*- c*: ISMS determination and **administration**

- Plan-a* - Field of application/boundaries:
  - Think over
  - Next step gradually
  - Adapt ISMS if too huge/too small
- Plan-b* - ISMS Information security policy:
  - Static, change of risk assessment criteria, new business processes, …
- Plan-c* - Risk assessment modalities:
  - Re-assessment of methods, lessons learned from security incidents

Plan-d*/e*: ISMS determination and **administration**

- Plan-d* - Identification of risks:
  - Identification of new risks
  - Existence/status of known risks (change of threats, vulnerabilities, importance of values)
- Plan-e* - Risk estimation and evaluation:
  - Approved risks
  - Risk valuation change
  - Estimation and evaluation of newly identified risks -> Plan-c -> change in risk assessment modalities (Plan-c*) ->new estimation/evaluation of all risks

Plan-f*-h*: ISMS determination and **administration**

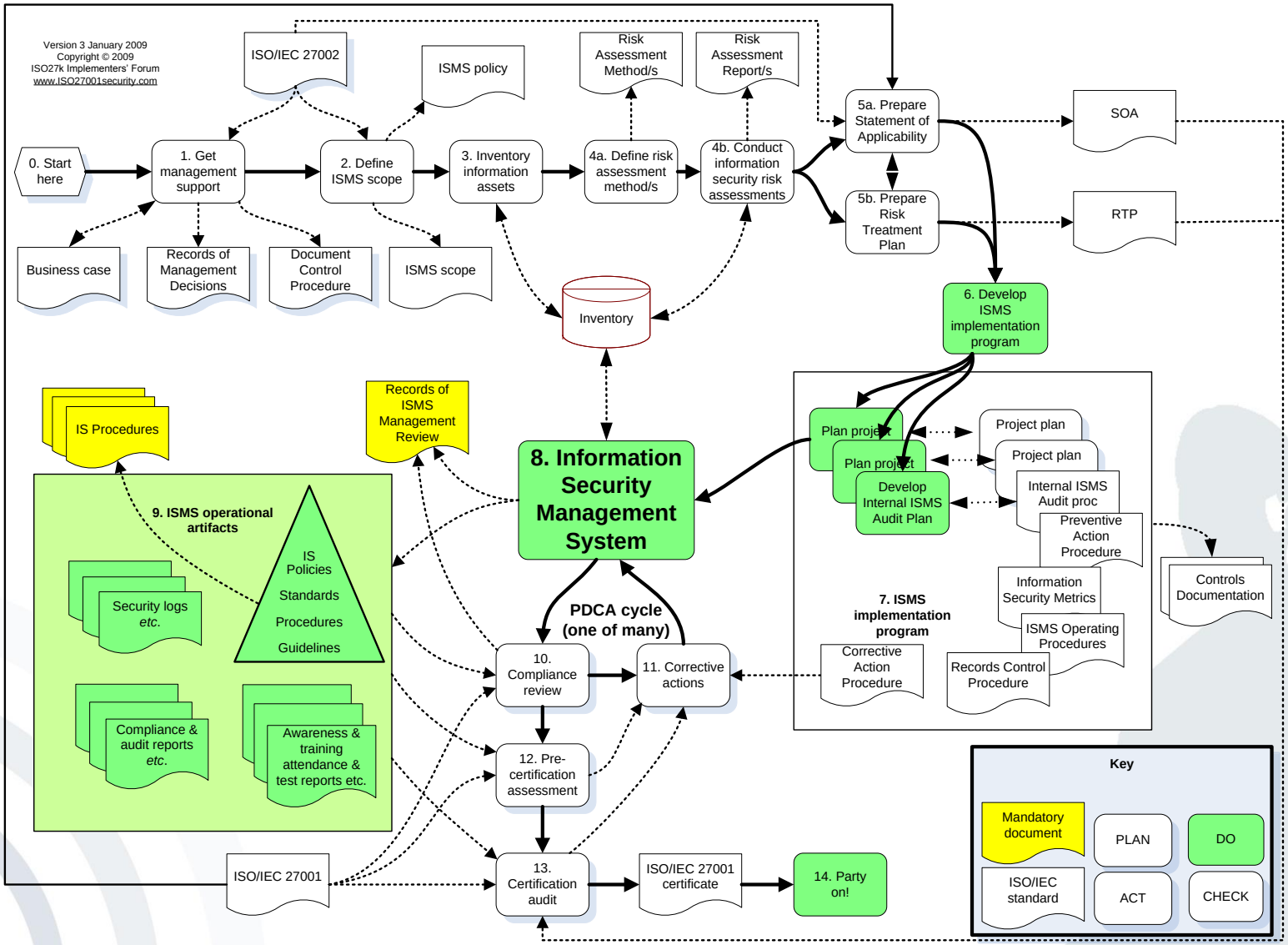
- Plan-f* - Options for risk treatment:
  - Check for new opportunities/duties (contacts, law, …) effectiveness of risk transfer, alternative options
- Plan-g* - Controls and objectives for unhandled risks - risk management:
  - Controls adequate for new risks (Plan-d*)
  - Review of initial controls and objectives
- Plan-h* - Management acceptance of residual risks:
  - Necessary if either change of residual risks or modification of risk assessment methods

Plan-i*/j*: ISMS determination and **administration**

- Plan-i* - Order to implement ISMS:
  - Serious changes to ISMS need management approval
- Plan-j* - Statement of applicability:
  - Amendments to existing statement if document serious changes

Result -> planning phase completed

Do: ISMS implementation and operation



Do: ISMS implementation and operation

- Main purpose of Do-Phase:
  - Implementation of an ISMS based on results of the “Plan”-phase
  - Operation of the ISMS

Do-a: ISMS implementation and operation

- Definition of risk treatment plan:
  - Appropriate management actions
    - Documentation and implementation of ISMS policy
    - Communication of importance of:
      - Compliance with ISMS policy
      - Achieving of security goals
      - Continuous improvement
  - Resources
  - Responsibilities
  - Priorities

Do-b: ISMS implementation and operation

- Implementation of risk treatment plan (control objectives)
  - Call for tender for external services and equipment
  - Provision of resources
  - Delegation and carrying out of tasks
  - Check results
  - Impracticable tasks need to be equally replaced
  - Management of arising problems

-> Day-to-day project business

Do-c: ISMS implementation and operation

- Implementation of risk controls
  - Difference between Do-b and Do-c (ISO 270nm)
    - Objectives vs. controls

->In practice no differentiation/separation of Do-b and Do-c

Do-d: ISMS implementation and operation

- Definition of how to measure effectiveness of controls:
  - Important but difficult task to estimate effectiveness of controls with regard to the objectives
  - Important conditions
    - Uniform applicable
    - Comparable results for different controls
    - Repeatable identical results under equal conditions

->In practice qualitative (classifications) instead of quantitative measuring based on grouped controls

Do-e: ISMS implementation and operation

- Employee sensitization and training
  - Continuous approach, planned yearly, documentation needed,
  - Communication by management important
  - Training of daily duties and behaviour in exceptional cases
  - New employees informed and trained immediately
  - Role specific training based on a common standard training
  - …

Do-f: ISMS implementation and operation

- ISMS operational management
  - Completeness and effectiveness of controls
  - Adaptation to organisational and business process changes
  - Adjustment of ISMS policy
  - Integration of ISMS related tasks into daily business
  - monitoring the maintenance of controls → part of management reports

Do-g: ISMS implementation and operation

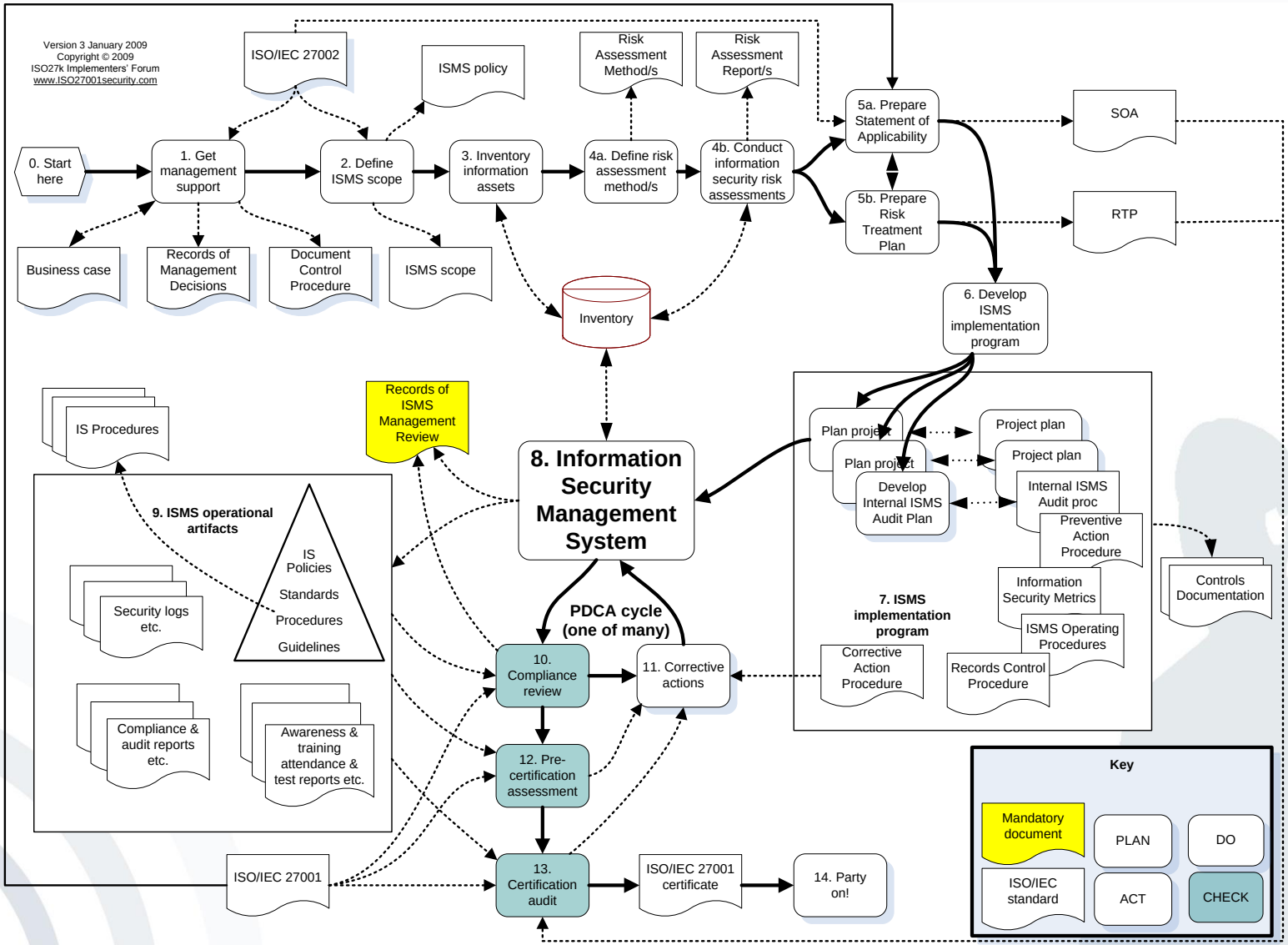
- ISMS resource management
  - Provisioning of needed resources (budget, staff, …)
  - Annual task planning
  - Cost-benefit analysis based on resource planning and controls measurement
  - Audit / Certification

Do-h: ISMS implementation and operation

- Recognition and management of security incidents
  - Incident management plan
    - Classification (low, medium, high/emergency)
    - Treatment based on classification
    - Emergency needs special treatment/escalation
    - Incident handling:
      - Identification
      - Notification (helpdesk, Incident manager)
      - Recording, in urgent cases immediate reaction
      - Classification
      - Escalation (management involvement)
      - Treatment, as far as possible
      - Restart
      - Analysis (lessons learned, feedback)

→ Incident handling and restart are subject to regular training.

Check: ISMS monitoring and checking



Check: ISMS monitoring and checking

- Main objectives of the phase “Check” are monitoring and checking of the status and protection level of the implemented ISMS
- Key to successful management of the ISMS
- Collected information used to further develop and improve ISMS
- Help to uncover and correct potential wrong turns

Check-a: ISMS monitoring and checking

- Monitoring and Checking
  - Recognition of data processing errors
  - Identification of attempted and successful security incidents/attacks
  - Deriving indicators for early incident diagnosis (IDS)
  - Verify if all safety-critical activities carried out as expected by responsible employees
  - Assessment of activities to remedy security violations

Check-b: ISMS monitoring and checking

- Regular inspection of ISMS' effectiveness
  - Level of commitment to ISMS policy
  - Extent to which security goals are reached
  - Effectiveness of each implemented control
  - …

  → Results to be used as input to management valuation (Check-f)
- Estimation of the controls' effectiveness

- Regular repetition of risk assessment

Check-c/d: ISMS monitoring and checking

- Check-c: Estimation of the controls' effectiveness
  - Based on the definition in Do-d
  - Results of the estimation/measurement of controls and operating conditions to be documented
  - Reporting of controls discovered as inappropriate
- Check-d: Regular repetition of risk assessment
  - Annually, at least biannually
  - In addition event driven assessments (e.g. change of business goals or processes)

Check-e: ISMS monitoring and checking

- Conducting regular internal audits
  - Conducted by internal staff
  - Announced or unannounced
  - Partly (e.g. to see effect on a specific business process), or
  - Complete ISMS (e.g. usually to discover actual state or as preparation to an external audit/certification)
  - Audit report:
    - Documents use for auditing
    - Course of the audit and participants
    - Complete list of positive or negative observations
    - Proposal how to remove deficit

Check-f: ISMS monitoring and checking

- Regular management valuation
  - Review of field of application to ensure reasonability
  - ISMS-process optimization/adaption
  - Deduction of improvement potentials
  - Time span during implementation of ISMS quarterly, during operation yearly

Check-g: ISMS monitoring and checking

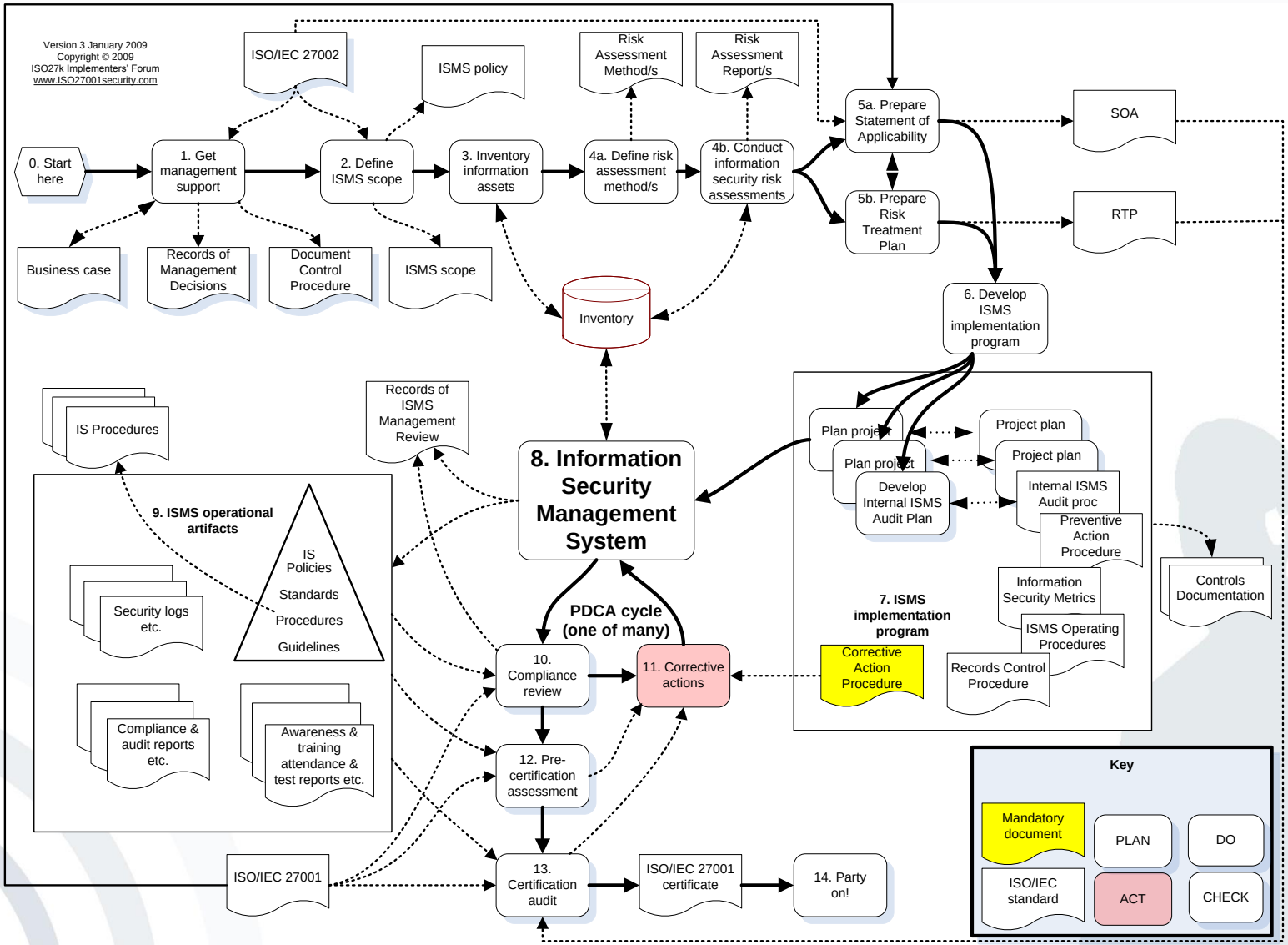
- Update security plans
  - Standard has no clear definition of security plans
  - Focus on incident management plan(Do-h)
    - Reactions to catastrophic incidents
    - Behaviour in emergency situations
    - Restart after business interruption
    - With particular reference to Check-c and Check-d

Check-h: ISMS monitoring and checking

- Documentation of activities and incidents
  - Resource planning
  - Deliver proof of training
  - Internal and external audit protocols and reports
  - Security incidents
  - Estimation of effectiveness (protocols and reports)
  - Management valuation protocols and cumulated task lists
  - …

mobile business

Act: ISMS cultivation and improvement



Act: ISMS cultivation and improvement

- Main goals of phase “Act”:
  - Conclusions for further development /optimization of the ISMS derived from experience with the operation
  - Information, opinions, evaluation results from Check-Phase as foundation for the further development
  - Lessons learned

  - Four corresponding tasks: a, b, c, d.

Act-a: ISMS cultivation and improvement

- Realisation of identified improvement potentials
  - Based on information from phase “Check” and management valuation(Check-f) a set of potential improvements was derived and needs to be implemented.
  - Input from employees
  - Decisions on equally suitable controls based on budget
  - Improvement suggestions which are not taken into account should be documented for potential future use.

Act-b: ISMS cultivation and improvement

- Corrective and preventive measures
  - Correction/redefinition/replacement of unsuccessful controls
  - Take preventive measures to avoid incidents happened in other organisations or known to be possible.
  - Based on the incident related information acquired by Do-h and during the phase “Check”.
  - Completed with information from “outside”: conferences, press, consulting, …

Act-c: ISMS cultivation and improvement

- Communication of planned improvements
  - All planned improvements need to be communicated to the target groups inside and outside the organisation in an adequate manner.
  - Employees need to be asked for their opinion/feedback.
  - Externally relevant changes need to be checked against contractual side-effects and negotiated with the external partner

Act-d: ISMS cultivation and improvement

- Performance review of realised improvements
  - Usually done with the next regular management valuation (Check-f)
  - In special cases (cost- or personnel-intensive, higher complexity, …) immediate or continuous review could be needed.
  - But management needs to define the modes and intervals of reviews.

→Party on ...

Summary

- Information Security is a process: therefore, management of Information security is needed.
- Information Security has impact on business and vice versa, so top management needs to take responsibility for the process.
- Information Security as quality is important to business relations; therefore standards and certifications are useful.
- Internationality in business relations produce a need for a common culture independent understanding of Information Security, so an international standard is needed -> ISO 270nm is one.

Reference

- Kersten, Heinrich; Reuter, Jürgen; Schröder, Klaus-Werner: IT-Sicherheitsmanagement, Vieweg + Teubner Verlag -ISBN 978-3-8348-0605-5
- Kersten, Heinrich: Der IT-Security Manager, Vieweg +Teubner Verlag - ISBN 978-3-8348-0429-7
- ISO27001 Security home; http://www.iso27001security.com/

mobile business

Takeaway

IT-Sicherheitsmanagement für Ihr Unternehmen

Wir helfen Ihnen dabei, Ihr Unternehmen sicherer zu machen

Deutschland sicher im Netz e.V. hat es sich zum Ziel gesetzt, kleine und mittlere Unternehmen bei der Umsetzung eines bedarfsgerechten Sicherheitsmanagements zu unterstützen. Denn IT-Sicherheit ist mehr denn je eine wesentliche Grundlage für eine reibungslose Geschäftsabwicklung in den Unternehmen.

In einer Umfrage bei Unternehmen haben wir ermittelt, mit welchen Sicherheitsrisiken sich Mittelständler konfrontiert sehen und welche Vorkehrungen sie bereits getroffen haben. Darauf aufbauend führten wir Workshops durch und erarbeiteten Empfehlungen, wie Sicherheitslösungen für den Mittelstand erfolgreich eingesetzt werden können.

Als Extrakt der Umfrage und der Workshops wollen wir Ihnen die 10 wichtigsten Handlungsempfehlungen präsentieren.

Impressum

Deutschland sicher im Netz e.V.
Albrechtstraße 10 a
10117 Berlin
Tel. +49 (0) 30 27576-310
Fax +49 (0) 30 27576-51310
info@sicher-im-netz.de
www.sicher-im-netz.de

IT-Sicherheitsmanagement
für Ihr Unternehmen

DsiN.de

Deutschland sicher im Netz e.V.

Ein gemeinsames Handlungsversprechen von:

SAP utimaco safeware BITKOM

Die 10 Handlungsempfehlungen für ein sicheres Unternehmen

1 Wirtschaftsspionage ist Realität – seien Sie sich der Gefahr bewusst

Sicherlich haben Sie sich auch schon für die Preislisten eines Wettbewerbers interessiert. Oft sind solche Informationen öffentlich. Manche Unternehmen oder Geheimdienste gehen aber einen Schritt weiter. Gerade der deutsche innovative Mittelstand ist im Visier der Spione.

2 Führen Sie eine Sicherheitsrisikoanalyse durch und entscheiden Sie dann über Ihre Schutzmaßnahmen.

Nur wer sich mit der Gefahr befasst, kann ihr begegnen. Jedes Unternehmen hat eine eigene Bedrohungslage. Je nach Größe oder Branche ergibt sich ein unterschiedlicher Schutzbedarf. Einen ersten Kurzcheck, der sie nicht mehr als 10 Minuten Zeit kostet, können sie auf unserer Website www.sicher-im-netz.de machen.

3 Sensibilisieren Sie Ihre Mitarbeiter

Der Mensch ist und bleibt das wichtigste Glied in der Sicherheitskette. Auch technische Maßnahmen nutzen nichts, wenn die Mitarbeiter sie nicht umsetzen. Schulungen und Kommunikationsmaßnahmen erhöhen das Bewusstsein für Sicherheit.

Verantwortung der Geschäftsführung

4 Führen Sie Sicherheitsregeln ein

Mitarbeiter brauchen praktische und konkrete Handlungsanweisungen, die den Umgang zum Thema Sicherheit regelt. Nur so ist sicher gestellt, dass das Thema Sicherheit in Ihrem Unternehmen in den Arbeitsalltag einfließt.

5 Ernennen Sie einen Verantwortlichen für das Thema Sicherheit

Das Tagesgeschäft lässt oft keine Zeit, sich mit dem Thema Sicherheit zu befassen. Umso wichtiger ist es, einen Verantwortlichen zu benennen, der das Thema als festen Bestandteil seiner Aufgaben hat.

6 Machen Sie sich mit den rechtlichen Anforderungen vertraut

Als Geschäftsführer oder Inhaber haften Sie für bestimmte Sicherheitsthemen. Das berühmte„Unwissenheit schützt vor Strafe nicht" gilt auch für das Thema Sicherheit. Dürfen Ihre Mitarbeiter privat surfen oder E-Mails versenden?

7 Gehen Sie mit Vorbild voran

Sicherheit ist Chefsache. Wenn deutlich wird, dass Sie das Thema Sicherheit ernst nehmen, folgen Ihnen die Mitarbeiter.

8 Schützen Sie auch persönliche Daten

Im Informationsschutz geht es nicht nur um Geschäftsgeheimnisse. Gerade persönliche Daten z.B. Ihrer Mitarbeiter genießen den besonderen Schutz des Datenschutzgesetzes.

9 Nutzen Sie das Know-how von externen Beratern

Man kann nicht alles wissen und gerade das Thema Sicherheit hat ein breites Spektrum. Nutzen Sie für diese Spezialthemen externe Fachleute. Deutschland sicher im Netz e.V. bietet Ihnen zu Ihrer Unterstützung eine Beraterdatenbank.

Was Deutschland sicher im Netz e.V. für Sie tun kann

10 Nutzen Sie unser Angebot

Die Informationen des IT-Mittelstandpaketes geben Ihnen konkrete Hilfsmittel an die Hand, die Sie sofort in Ihrem Unternehmen umsetzen können:

Für den täglichen Gebrauch haben wir Ihnen eine umfangreiche Sammlung an Sicherheitsrichtlinien, Verfahrensanweisungen, Checklisten sowie Notfallplänen zusammengestellt und bedarfsgerecht aufbereitet.

DsiN hat auch zum Thema Haftung eine Übersicht auf der Website bereitgestellt und ein kleines Pocketseminar entwickelt.

In unserem IT Sicherheitspaket für den Mittelstand finden Sie zudem Schulungsunterlagen und Poster, die Sie sofort und kostenlos nutzen können.

Besuchen Sie uns im Internet unter
https://www.sicher-im-netz.de/unternehmen/Starthilfe_Sicherheit.aspx