ALLENDEVAUX.COM

ALLENDEVAUX & COMPANY

ESTABLISHING COMPLIANCE

- Certified Professionals Across all Areas of Competency
- ISO 27005 Risk Assessment and Treatment Plan
- Full implementation of the ISO27001 standard with ISO27002 controls
- Companywide Training Programme and Awareness Campaign
- Penetration Testing for Key Infrastructure and Services
- Cybersecurity Vulnerability Scorecard with Remediation Plan
- Spear Phishing Campaign for Awareness
- Compliance with GDPR and other Regulations
- Ongoing Audit Support

CAN YOU BE TRUSTED TO SAFEGUARD CUSTOMER DATA? GET CERTIFIED.

THE WORLD HAS DRAMATICALLY CHANGED.

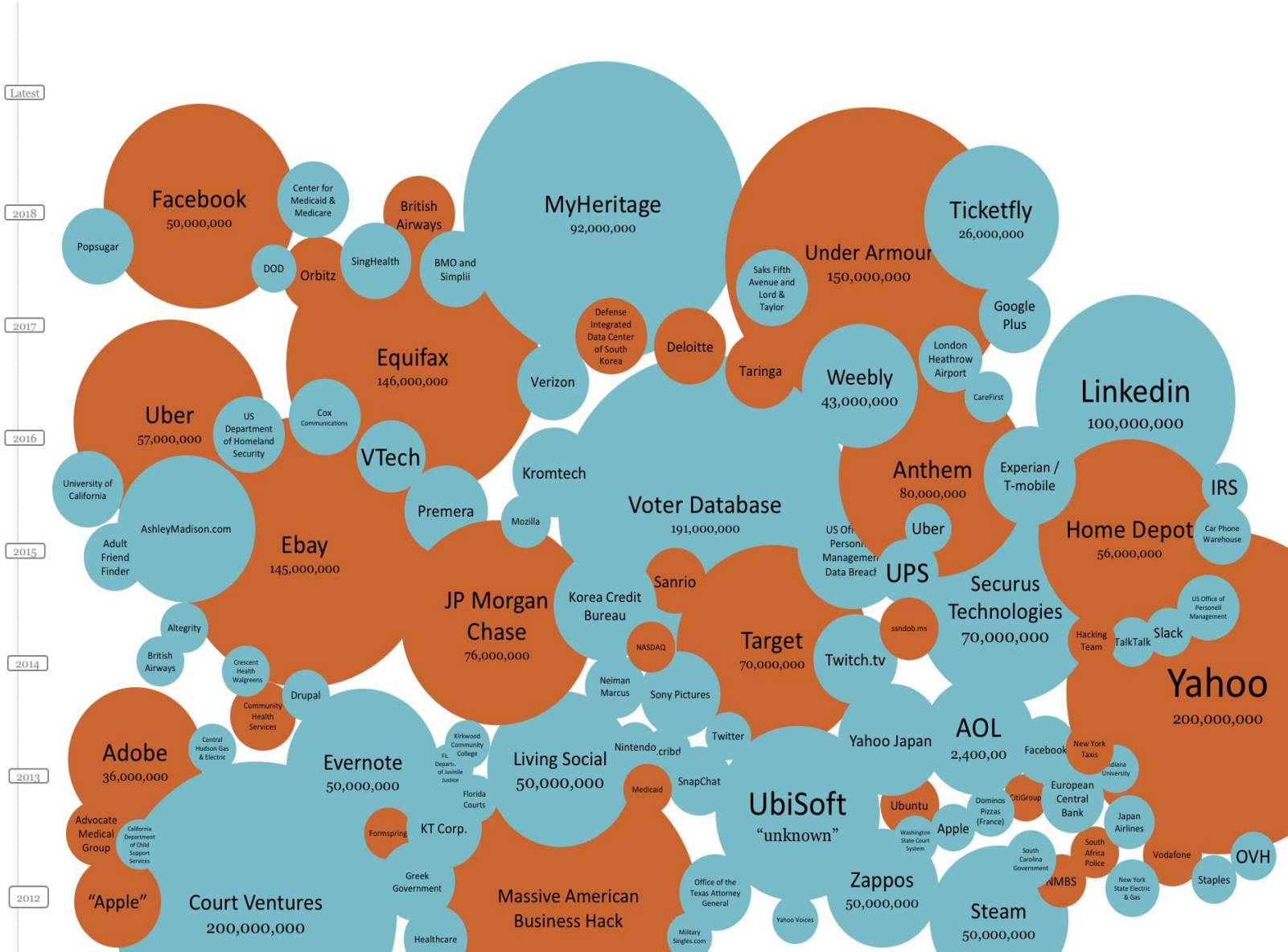
No longer are the largest companies automotive manufacturers and oil producers. Today's largest companies are data centric: Apple, Google, Microsoft, Facebook, Amazon.

Within one decade, information has become the single-most valuable commodity with no slowdown in sight.

But information has also become the biggest *target*.

In an era when data breaches span weekly headlines, how can customers have confidence that their data is secure on your systems? How do they know their confidential information will not become the next data breach?

Can you be trusted?



WHY IMPLEMENT ISO 27001?

HOW TO BUILD TRUST AND CONFIDENCE WITH CUSTOMERS AND STAKEHOLDERS

Today's customers demand heightened levels of data protection assurance, but how is that achieved in an era of weekly data breaches? An ISO 27001 certification is the most recognized answer. Companies bearing this seal mean they have implemented a systematic set of policies and procedures to provide enhanced levels of protections, audited by third party certified assessors.

Passing the third-party audit results in many trustworthy improvements. Companies find that going through the process:

- **Lowers risks** by implementing a methodology for identifying threats and vulnerabilities
- **Bolsters assurance in the supply chain** and ensure flow-down terms are implemented
- **Provides evidence of best practice** when tendering contracts
- **Promotes stakeholder satisfaction** by investing in exemplary practice to safeguard information
- **Minimizes financial loss** by protecting from cyberattacks or negligence
- **Improves processes** through a framework of policies and procedures that are consistent, repeatable and maintainable
- **Achieves regulatory compliance** with GDPR, PIPEDA, MiFID II, GLBA or other regulations to which the organisation must comply
- **Earns worldwide respect** a recognized international standard for information security

"With the implementation guidance of Allendevaux & Company, companies have exhaustively implemented the necessary security controls and practices to protect data."

–David Maldow, Analyst, Let's Do Video

WWW.ALLENDEVAUX.COM

ISO/IEC CERTIFICATION

An Overview of What to Expect

At Allendevaux & Company, we have created an non-intrusive programme to establish and implement an information security management system (ISMS) through a 7-step process. Our certified professionals report to a stakeholder within your organisation that you appoint.

Anticipated Timeframe for Certification. Once we conduct a "phase 2 discovery" and perform a "phase 3 risk assessment" we will know what's required and generally how much time it will take to achieve ISO/IEC certification. Depending on the size of the organisation and its current practices, the timeframe can take from 9 months to 15 months, with complex scenarios taking as long as 24 months. Average time is 11 to 12 months.

Working with Allendevaux Professionals. While it is helpful to conduct working sessions onsite, many meetings and work activity may be conducted remotely using unified communication and collaboration tools. It is also helpful, but not required, for the Allendevaux team to be issued company email addresses during the lifetime of the engagement. This practice ensures all confidential information remains within your enterprise, and it will be recommended that all documentation created be saved to your secure repository.

Fee Structure for Security-as-a-Service. There are four fees you can anticipate during this process: (1) The Allendevaux fixed monthly fee which for InfoSec-as-a-Service including all tools and resources; (2) reimbursement for any pre-approved travel expenses as may be necessary during the engagement; (3) the fixed fee to bring in a third-party auditor to audit the final implementation; (4) a final, daily fee if Client desires Allendevaux to help support and defend the certification by the third-party auditor, something Allendevaux highly recommends, charged at a daily rate.

1. Plan & Host Kickoff
2. Conduct Discovery
3. Perform ISO27005 Risk Assessment
4. Build the ISMS
5. Conduct Cybersecurity Campaign
6. Launch Training Programme
7. Conduct Internal Audit

IMPLEMENTING A PHASED APPROACH TO

ISO/IEC CERTIFICATION

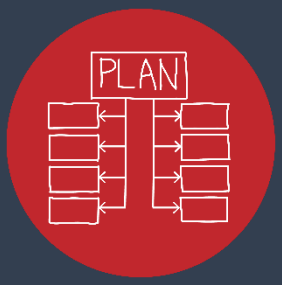
7-PHASES FROM KICKOFF TO THE START OF THE CERTIFICATION

As an overview, the following provides a high level summary of what each phase of activity covers. From start to finish, the seven phases outline the roadmap which prepares the organisation to undergo the final audit by a third-party auditor.

1. **Plan & Host Kickoff**
   Identify key stakeholders and interested parties. Build online project environment. Host soft kickoff.
2. **Conduct Discovery**
   Setup stakeholder interviews. Develop compliance requirements. Identify regulatory compliance and contractual obligations.
3. **Perform ISO27005 Risk Assessment**
   Inventory assets. Develop risk criteria. Identify threat sources and events & predisposing conditions. Determine likelihood of impact.
4. **Build the ISMS**
   Write tier 1-2 policies/procedures. Write tier 3 local work instructions and integrate ISO27002 control objectives. Develop BCD plan and breach escalation matrix.
5. **Conduct Cybersecurity Campaign**
   Perform vulnerability scanning internally and externally and generate CVSS scores. Perform spear phishing campaign. Perform penetration testing.
6. **Launch Training Programme**
   Develop awareness campaign and training programme. Launch the training programme; test the user base on InfoSec & compliance and record performance.
7. **Conduct Internal Audit**
   Perform an internal audit to measure implementation. This is the final step that prepares the organisation to under audit by a third-party auditor for certification.

1

Plan and Host Kickoff



PREPARE THE ENGAGEMENT PROJECT PLAN

COORDINATION

- Plan the kickoff meeting
- Identify key stakeholders and meeting participants
- Develop an online project environment and extend access
- Invite kickoff participants
- Host kickoff meeting
- Review engagement scope and goals
- Distribute invites for online collaboration
- Review example output of engagement deliverables
- Review project plan and associated schedule
- Determine stakeholder participants for the discovery session
- Coordinate discovery meeting specifics
- Confirm engagement connectivity venue
- Send invite for discovery session

PRELIMINARY DISCUSSIONS

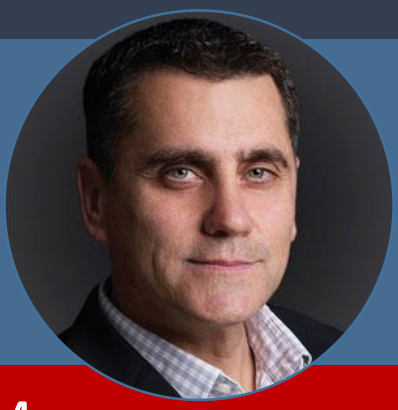
- Request names of relevant interviewees across applicable areas
- Request interview time slots by email
- Schedule interviews with calendar invites

PROJECT MANAGEMENT

- Host regular progress meetings and distribute updates

"Pinnaca has been working with Allendevaux & Company to deepen and broaden its information security practices across its offices in Asia, Europe, and the Americas. These activities span regulatory compliance conformance such as the GDPR, HIPAA, PIPEDA and others."

–Dan Tanel, Chief Operating Officer, Pinnaca, Toronto



2 Conduct Discovery

Stage 2 of the engagement focuses on discovery exercises, largely focused on understanding the regulatory landscape to which the organisation must comply in terms of where it processes data.

CONDUCT DISCOVERY SESSIONS

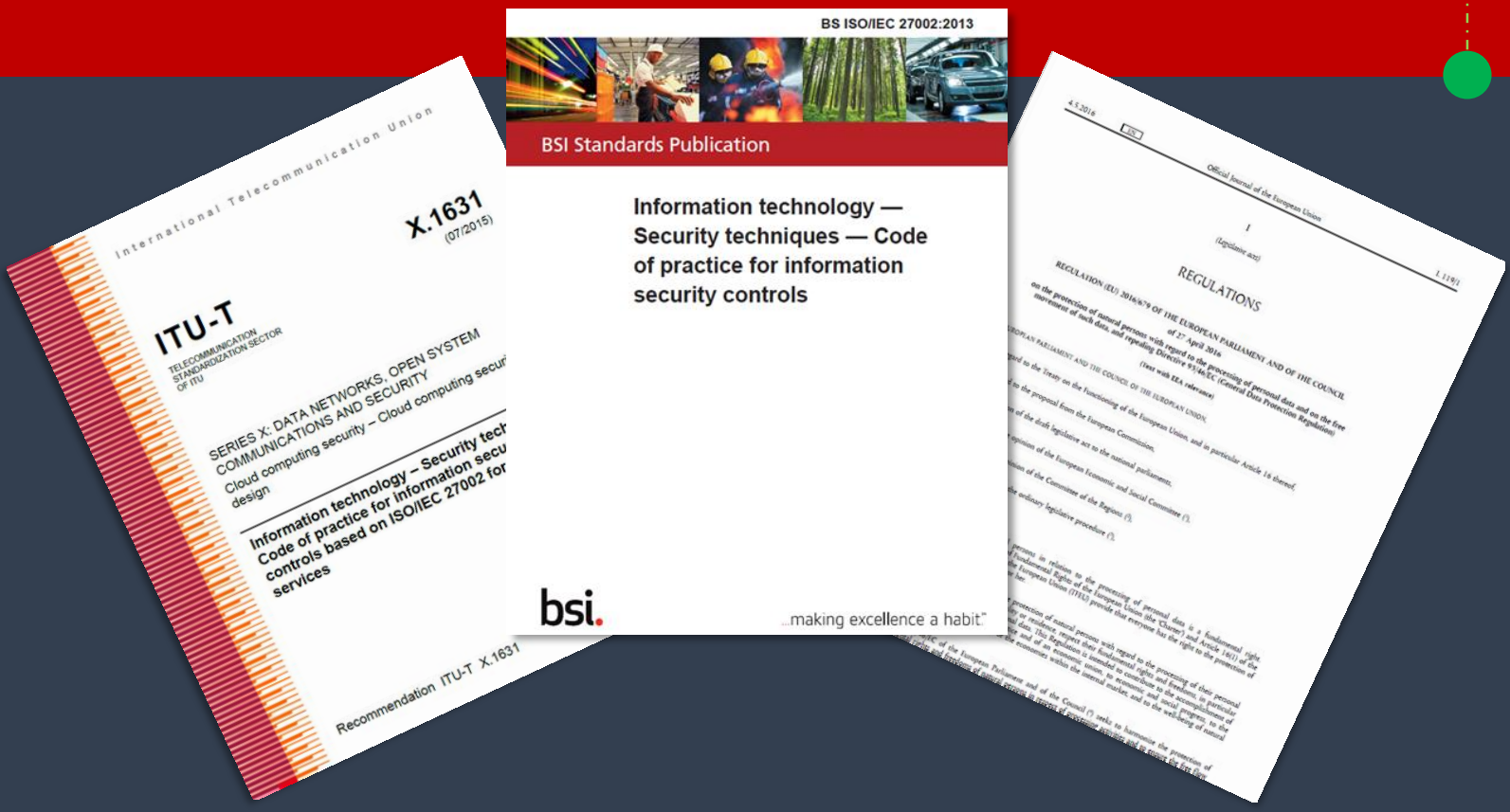
- Setup stakeholder interviews for various SBUs.
- Leverage existing interviews from past sessions.
- Collect existing policies and procedures from each department.
- Develop an overall set of compliance requirements as an output of the discovery.

EXPLORE COMPLIANCE LEGISLATION

- Compile geographic or national regulatory requirement to which the ISMS must conform.
- Compile province, state and territorial legislation to which the ISMS must conform.
- Compile industry requirements such as (PCI DSS) to which the ISMS must conform.
- Create a superset of requirements to which the ISMS must conform.

SELECT FRAMEWORK AND CONTROLS

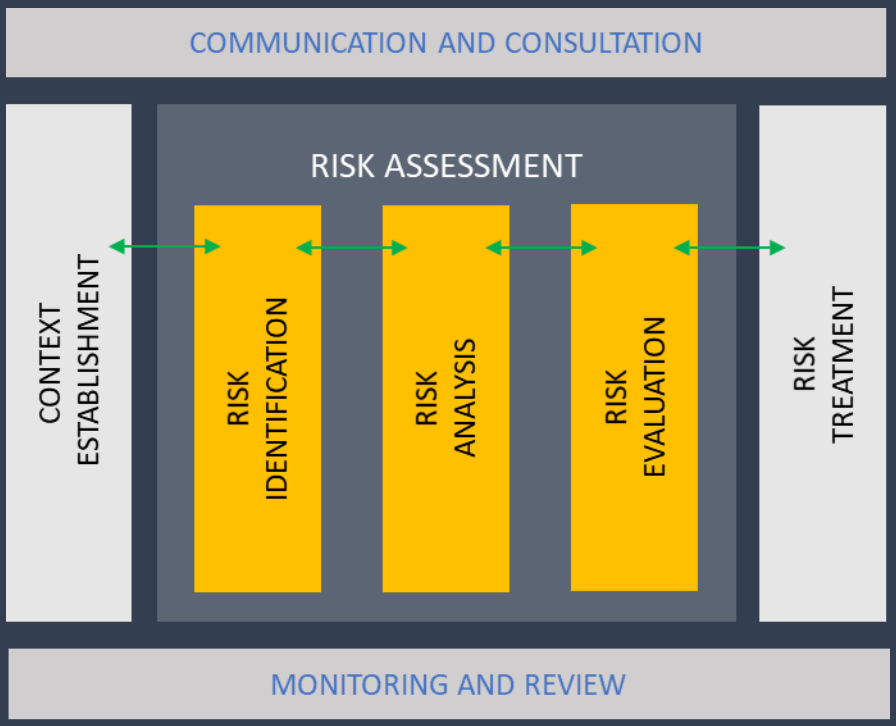
- Determine standard to implement.
- Determine controls to apply to the standard.
- Determine a measurement framework to utilize.



3 Perform ISO/IEC 27005 Risk Assessment

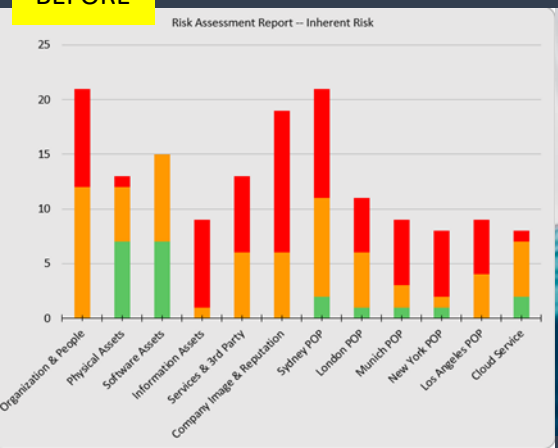
Stage 3 of the engagement applies a systematic approach to security risk management to identify organisational needs regarding information security requirements, determining the risk levels and treatment plan in order to reduce risk to an acceptable level.

- Identify assets
- Create an asset inventory.
- Identify potential threats.
- Note any vulnerability
- Measure exposure
- Calculate exposure factor (EF).
- Calculate risk in terms of the likelihood that a threat will be exploited (risk=threat x vulnerability).
- Assess the annualized rate of occurrence (ARO).
- Determine safeguards
- Apply risk assignment and acceptance/rejection.
- Select countermeasures for next section.

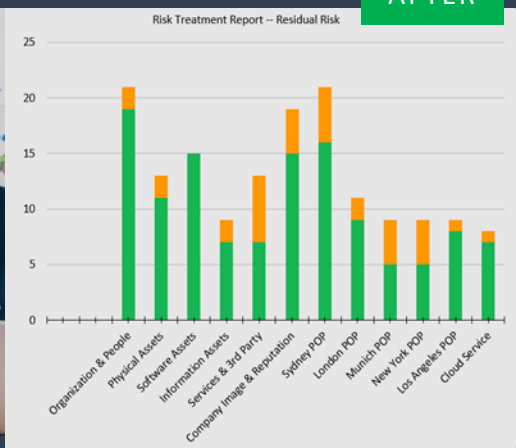


Following ISO 27005 best practices produces an asset inventory with current risk measurements (inherent risk) to the confidentiality, integrity and availability of each resource. By applying mitigating measures (controls), risk to the organisation can be managed and brought into acceptable tolerance levels (residual risk). This process should be conducted during phase 3.

BEFORE



AFTER



4

Build the ISMS
Stage 4a

Stage 4a, writing ISMS policies.

ISO27001:2013 POLICY

- Create leadership policy that demonstrates commitment, sets objectives, establishes roles, highlights responsibilities, and establishes authority to ensure the ISMS conforms to the requirements of ISO27001:2013.
- Create risk treatment policy to address risks and opportunities to ensure the ISMS can be achieved, including risk acceptance criteria, identity of risk owners, risk levels, risk treatment, and security objectives.
- Create support policy to ensure resource allocation to establish, implement, maintain, and continually improve the ISMS with regards to competence, awareness, communication and documentation.
- Create operational policy in relation to the ISMS for planning and control, and reassessment of risk due to change management.
- Create performance evaluation policy for monitoring, measuring, analysing and evaluating overall behavioural effectiveness of the ISMS in association with internal audits and management review.
- Create improvement policy including nonconformity, correction action, and continual improvement guidelines.

CONTROL OBJECTIVES: ISO27002

- Policy for information security such as segregation of duties, contact with authorities, contact with special interest groups, etc.
- Policy for mobile devices and teleworking.
- Policy for HR prior to employment: screening controls.
- Policy for HR during employment: management responsibilities, awareness, training, disciplinary action.
- Policy for HR termination or change of employment.
- Policy for asset management including responsibility, inventory, ownership, acceptable use, return.
- Policy for information classification schema including, labelling and handling.
- Policy for media handling, including management of removable media, disposal, and physical media transfer.
- Policy for access control, network access, user registration and deregistration, access provisioning, privilege access rights, secret authentication information of users, review of user access rights, removal or adjustment of access rights, use of secret authentication information, information access restriction, secure log-on procedures, password management system, use of privileged utility programs, access control to program source code.
- Policy for cryptographic controls and key management.

4

Build the ISMS Part 4b

Stage 4b, ISO27002 controls.

- Policy for physical and environmental security including physical security perimeter, physical entry controls, securing offices and facilities, protecting against external and environmental threats, working in secure areas, delivery and loading areas, equipment sitting and protection, supporting utilities, cabling security, equipment maintenance, removal of assets, security of equipment and assets off-premises, secure disposal or reuse of equipment, unattended user equipment, clear desk and clear screen policy.
- Policy for operations security for documented operating procedures, change management, capacity management, separation of development and testing, protection from malware, backup, logging and monitoring and clock synchronization, control of operational software installation, technical vulnerability management, restrictions on software installation, audit considerations.
- Policy for communications security for network controls, network service security, segregation in networks, information transfer procedures, agreements on information transfer, electronic messaging, confidentiality or nondisclosure agreements.
- Policy for system acquisition, development and maintenance.
- Policy for security in development and support processes including change control procedures, review after operating platform changes, restrictions on changes to software packages, secure system engineering principles, secure development environment, outsourced development, system security testing, system acceptance testing, protection of test data.
- Policy for supplier relationships to ensure protection of the organization's assets that is accessible by suppliers including to managing changes to the supplier services.

"Applying specific controls to protect assets is foundational for any ISMS. We select controls from best practice frameworks such as ISO 27002, NIST, ISO 27017, ISO 27018 and other recognized frameworks."

–Rebekah Allendevaux, Senior Partner, CIPP/E, CIPM, CIS LI, CIS LA

WWW.ALLENDEVAUX.COM

4

Build the ISMS Part 4c

Stage 4c, ISO 27002 controls.

- Policy for information security incident management to ensure consistent and effect approach to the management of information security incidents, including communication on security events and weaknesses:
- Responsibilities and procedures
- Reporting information security events
- Reporting information security weaknesses
- Assessment of and decision on information security events
- Response to information security incidents
- Learning from information security incidents
- Collection of evidence.
- Policy for information security aspects of business continuity management so that information security continuity shall be embedded in the organization's business continuity management systems:
- Planning information security continuity
- Implementing information security continuity
- Verify, review and evaluate information security continuity
- Redundancies to ensure availability of information processing facilities.
- Policy for compliance to avoid breaches of legal, statutory, regulatory or contractual obligation related to information security and any of security requirements:
- Identification of applicable legislation and contractual requirements
- Intellectual property rights
- Protection of records
- Privacy and protection of personally identifiable information
- Regulation of cryptographic controls
- Information security reviews by independent auditors to ensure information security is implemented and operation in accordance with the organizational policies and procedures.
- Compliance with security polices and standards.
- Technical compliance review.

"We send our sincere thanks to Allendevaux & Company for your guidance and effort to establish our ISMS and ensure regulatory compliance with sectoral and geographic regulations."

–Kjell Oksendal, Chief Marketing Officer, Media Network Services, Oslo

WWW.ALLENDEVAUX.COM

5

Vet Cyber Readiness

Ensuring a sound information security postures involves a properly conducted cybersecurity campaign, including vulnerability scanning of internal and external assets, penetration testing of key infrastructure, and spear phishing drive.

VULNERABILITY SCANNING

- Compile assets/subnets to be scanned.
- Define scoring rubric.
- Create DocuSign permissions.
- Conduct scanning campaign & generate report.

PENETRATION TESTING

- Determine asset listing.
- Determine attack vector & privileges.
- Determine white/black/grey test.
- Generate DocuSign permissions.
- Conduct penetration tests by white hackers.

SPEAR PHISHING CAMPAIGN

- Identify spoofing originators; design spoof.
- Determine and acquire domain & certs.
- Prepare attack.
- Release attack; monitor & tabulate results.

COOKIEBOT ASSESSMENT

- Identify web URLs
- Compliance with GDPR Article 7, 12, 21
- ePrivacy Directory & Consent Framework
- Digital Advertising Alliance (DAA)
- Network Advertising Initiative (NAI)

"The certified practitioners at Allendevaux & Company give professional attention to vulnerability scanning, penetration testing and spear phishing campaigns to ensure third party testing and readiness."

–Berdina Facko, Cybersecurity Practice Lead, Net+

WWW.ALLENDEVAUX.COM

6

Launch Training Programme

AWARENESS CAMPAIGN AND TRAINING PROGRAMME

The Media Services group at Allendevaux & Company creates training content to reflect the implemented ISMS. This ensures the enterprise understands the programme that has been implemented, and it ensures training mandated by government requirement is properly administered.

CONDUCT AWARENESS CAMPAIGN

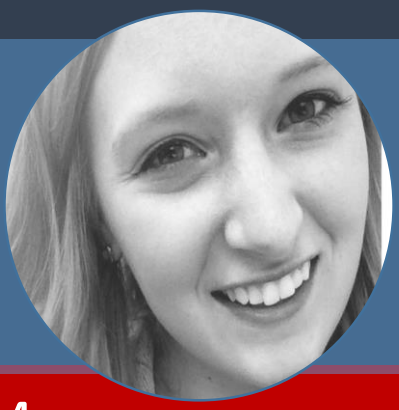
- Ensure compliance with regulatory obligations.
- Establish executive sponsor.
- Instill privacy & security requirements.
- Define the privacy message (value, strategy, policy).
- Document desired tactical outcomes.
- Provide examples of case studies and considerations.

CONDUCT TRAINING PROGRAMME

- Build training system venue
- Load content into system
- Create quizzes to be delivered to trainees
- Launch training programme
- Record attendance and scores

"Awareness campaigns and training programmes are created by the Media Services Group foster a security minded culture that puts data protection at the forefront of everyone's mind and satisfies regulations."

–Brianna Kinne, Media Services Group



WWW.ALLENDEVAUX.COM

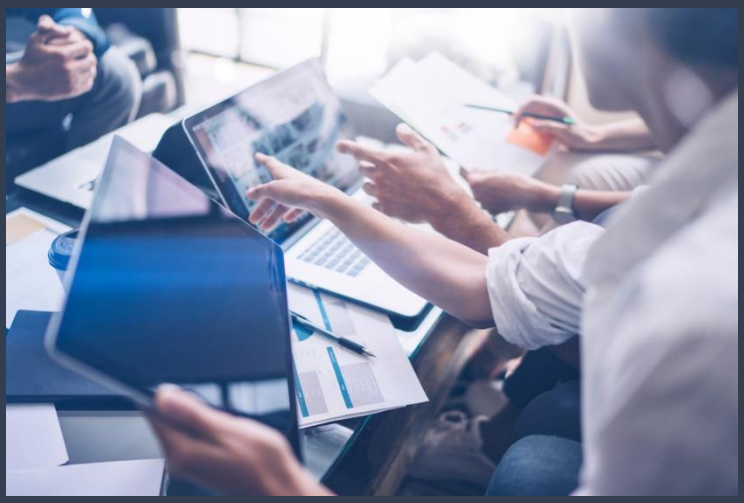
7

Conduct Internal Audit

INTERNAL AUDIT FOR CERTIFICATION READINESS

INTERNAL AUDIT

- Context of the organisation
- Leadership and commitment
- Planning & actions to address risk
- Support for resources & competence
- Operation
- Performance evaluation
- Improvement
- Management direction
- Organisation of information security
- Human resource security
- Access control, cryptography
- Physical security, operations, comms
- System acquisition, supplier vetting
- Incident management, compliance



THIRD-PARTY AUDIT & CERTIFICATION

During the certification process, an independent company (EY CertifyPoint, Deloitte, BSI Group, etc.) will audit the implementation. Allendevaux can support and defend the Stage 1 & Stage 2 audit on behalf of the Client, and charges a daily fee to support the certification. The quantity of audit days is determined by the independent auditing entity based on a formula that includes the company size.

"When aligning ISMS policy with regulatory obligations, it's important to ensure geographic and sectoral compliance is researched and vetted wherever data is processed."

–Anessa Santos, JD, Regulatory Compliance

WWW.ALLENDEVAUX.COM

ALLENDEVAUX.COM

ALLENDEVAUX & COMPANY

ACHIEVING COMPLIANCE

Advisory Area Practice Leads

Rebekah Allendevaux
Senior Partner,
CIPP/E, CIS-LI, CIS-LA, CIPM

Sarah Berdina Facko
Cybersecurity Practice Lead, Net+

Anya Krupina, J.D.
Legal Regulatory Compliance Advisor,
CIS-LI, CIS-LA

Scott Allendevaux
Senior Partner, CISSP,
CIPP/US, CIPT, CIPM, HCISPP

ALLENDEVAUX.COM

ALLENDEVAUX & COMPANY

CONTACT US

Email: info@allendevaux.com
Web: www.allendevaux.com

US: +1 213 279 1055
UK: +44 2038 802 321
CH: +41 44 585 92 15