Kontrole (Controls):

- Managerial
    - Administrative controls
    - Security design, policies, procedures, processes, guidelines, risk management, account management, regulatory controls
    - Focused on managing risk
    - Documented in written policies
    - Organizational security policy, Risk assessments, Vulnerability assessments
- Operational
    - Controls implemented by people
    - Security guards, awareness programs
    - Focused on the day-to-day procedures of an organization
    - Used to ensure that the equipment continues to work as specified
    - Configuration management, Data backups, Awareness programs
- Technical
    - Logical controls
    - Controls implemented using systems
    - OS controls, firewalls, antivirus
    - Executed by computer systems (instead of people)
    - Implemented with technology

Typy kontroli (Control types):

- Preventing
    - Prevent access
    - Firewall, guard, door lock, hardening, separation of duties
    - Co mnie jako atakującego wprost powstrzyma?
- Detective
    - Identifies intrusion attempt
    - IDS, motion detector, Log monitoring, CCTV, security audits
- Corrective
    - Designed to mitigate damage
    - Backups and system recovery, IPS, Alternate site, Fire suppression system
- Deterrent
    - Zniechęca intruzów
    - Warning sign, banner, lights
- Compensating
    - Don’t prevent attacks, restores using other means
    - Hot site, backup power system, re-image, Temporary port blocking, Temporary service disablement
    - Jeszcze sandboxing był ale nie zbyt się zgadzam z tym
- Physical
    - Real world security
    - Fance, lock

Dokumenty, regulacje I zalecenia:

- NIST RMF – Risk Management Framework
    - mandatory IT security and risk management framework for U.S. federal government developed by NIST
    - 6 step process
    - Categorize system, selects the controls that apply to the system, implements the controls, and then assesses the success of the controls before authorizing the system
- NIST CSF – CyberSecurity Framework
    - NIST's voluntary framework outlining best practices for computer security
- ISO/IEC 27001 – standard for ISMS (Information Security Management System)
- ISO/IEC 27701 – PIMS – Privacy Information Management System
- ISO 31000 – Risk management practices
- ISO/IEC 27002 – code of practice for information security controls
- AICPA – The American Institute of Certified Public Accountants auditing standard:
    - Statement of Standards for Attestation Engagements number 18 (SSAE 18)
    - SOC – System and Organization Controls: firewalls, MFA, IDS
    - SOC 1 – financial reporting controls
    - SOC 2 – security controls
        - Type I audit – controls in place at a particular point in time
        - Type II audit – controls in place min. 6 months
    - SOC 3 – publicly accessible
- CSA – Cloud Security Alliance
    - nonprofit organization promoting best security practices related to cloud computing environments
    - CCM – Cloud Controls Matrix
        - cybersecurity control framework for cloud computing

Ukrywanie danych:

- Data masking (obfuscation)
    - Zamiast cyfr wyświetlane są gwiazdki
- Anonymization
    - Can’t be reversed
- Pseudo-anonymization
    - Ksywki, pseudonimy
    - Consistent replacement

Postacie/role:

- Data steward/custodian**
    - Manages governance process, responsible for data accuracy, privacy, security
    - Sensivity labels to the data
    - Ensures compliance with laws
    - Implements security controls
- Data steward/custodian - this role handles managing the system on which the data assets are stored. This includes responsibility for enforcing access control, encryption, and backup/recovery measures

- Data owner
    - Vp of sales – owns customer relationship data
    - Treasurer** – financial data**
    - responsible for setting the data classifications and approving the level of access given to personnel
    - protection and privacy
- System Owner:
    - Business processes and impact
- Data controller
    - ensure that the data subject consents and protect that data
- Data processor
- DPO – Data Protection Officer
    - Sets policies, implements processes and procedures
    - Responsible for the organization's data privacy

Uzupełnienie ról

- Privacy officer

o senior role with the ultimate responsibility for maintaining confidentiality, integrity, and availability in a system

o A data owner is responsible for the confidentiality, integrity, availability, and privacy of information assets. They are usually senior executives and somebody with authority and responsibility. A data owner is responsible for labeling the asset and ensuring that it is protected with appropriate controls. The data owner typically selects the data steward and data custodian and has the authority to direct their actions, budgets, and resource allocations.

- Data custodian**

o The data custodian is the role that handles managing the system on which the data assets are stored. This includes responsibility for enforcing access control, encryption, and backup/recovery measures.

- Data steward**

o The data steward is primarily responsible for data quality. This involves ensuring data are labeled and identified with appropriate metadata. That data is collected and stored in a format and with values that comply with applicable laws and regulations.

- Privacy officer

o The privacy officer is responsible for oversight of any PII/SPI/PHI assets managed by the company.

- Data protection officer

o Helps understand better how the PII data from a particular database is used within business operations.

o The primary role of the data protection officer (DPO) is to ensure that her organization processes the personal data of its staff, customers, providers, or any other individuals (also referred to as data subjects) in compliance with the applicable data protection rules. They must understand

how any privacy information is used within business operations. Therefore, they are the best person for the auditor to interview to get a complete picture of the data usage.

Pojęcia:

Różne dokumenty I porozumienia

- AUP – Acceptable Use of Policies
  - document stipulating rules of behavior to be followed by users of computers, networks, and associated resources
  - for employees
- EULA
  - For a single piece of software
  - Focuses on the client (and user)
- NDA – Non Disclosure Agreement
  - legal contract between the holder of confidential information and another person to whom that information is disclosed prohibiting that other person from disclosing the confidential information to any other party
- MSA – Measurement System Analysis
  - Don't make decisions based on incorrect data
  - Calculate measurement uncertainty
- MSA - Master Service Agreement
  - agreement that specifies generic terms to simplify the negotiation of future contracts between the signing parties
  - contract reached between parties, in which the parties agree to most of the terms that will govern future transactions or future agreements
  - The MSA is used when a pentester will be on retainer for a multi-year contract, and an individual SOW will be issued for each assessment to define the individual scopes for each one
  - Most terms negotiated ahead of time
- SOW - The Statement of Work
  - formal document stating what will and will not be performed during a penetration test
  - it should also contain the assessment's size and scope and a list of the assessment's objectives
- ISA – Interconnection Security Agreement
  - specifies security requirements for an interconnection between two organizations
  - governs the relationship between any federal agency and a third party interconnecting their systems
- SLA – Service Level Agreement
  - agreement between a service provider and users defining the nature, availability, quality, and scope of the service to be provided
  - agreement that specifies performance requirements for a vendor
- MOU – Memorandum Of Understanding
  - Informal letter of intent, not signed contract
  - Statements of confidentiality
  - general document established between two or more parties to define their respective responsibilities and expectations in accomplishing a particular goal or mission

- MOA – Memorandum Of Agreement
    - general document established between two or more parties to define their respective responsibilities and expectations in accomplishing a particular goal or mission
- LOA – Letter of Agreement = MOU = MOA
- BPA – Business Partnership Agreement
    - key document governing the relationship between two business organizations
- T&C – Terms of Use
    - Legal agreement between service provider and user
- Separation of duties
    - Split knowledge
    - Dual control
- Background check
- Adverse action – an action that denies employment based on the background check (also existing employees)
- On-boardzing / off-boarding
- Gamification
- CBT – Computer Based Training
- EOL – End Of Life
    - Stop selling, maybe continue support
- EOSL – End of Service Life
    - Stop selling, stop supporting
- Data retention – przechowywanie danych
- Change control
- Asset management
- Risk assessment
- Multi-party risk
- IP – Intellectual Property
- Risk register
    - Risk matrix / risk heat-map (assessment tool used for prioritizing the severity of different risks)
    - document containing detailed information on potential cybersecurity risks
- Inherent risk
    - Impact + likelihood
    - Risk that exists in the absence of controls
- Residual risk
    - Inherent risk + control effectiveness
    - Risk that exists after controls are considered
- Risk apetite
- HIPAA – Health Insurance Portability and Accountability Act
- Qualitative risk assessment
    - Identify significant risk factors
- ARO – Annualized Rate of Occurrence
- SLE – Single Loss Expectancy
- ALE – Annualized Loss Expectancy

RTO, RPO, MTTF, MTBF, MTTR

- RTO – Recovery Time Objective (co to jest poczytaj)
    - maximum tolerable period of time required for restoring business functions after a failure or disaster
    - amount of time it takes to identify that there is a problem and then perform recovery (restore from backup or switch in an alternative system, for instance)
    - targeted duration of time and a service level within which a business process must be restored after a disaster (or disruption) to avoid unacceptable consequences associated with a break in business continuity.
    - Czas potrzebny na przywrócenie funkcji biznesowych w przypadku awarii pojedynczego systemu, ale nie musi być to naprawa tylko np. podmiana
- RPO – Recovery Point Objective
    - maximum tolerable point in time to which systems and data must be recovered after an outage
    - amount of data loss that a system can sustain, measured in time
    - if a virus destroys a database, an RPO of 24 hours means that the data can be recovered (from a backup copy) to a point not more than 24 hours before the database was infected
    - chodzi o dane, nie czas w szczególności. RPO definiuje przez jak długi okres czasu możemy bezpiecznie tracić dane – dane można odtworzyć z backup'ów
- MTTR – Mean Time To Repair
    - Time to correct a fault to restore the system to full operation
    - Czas potrzebny na całkowitą naprawę systemu
    - Average time to replace or recover a system or product
- MTBF – Mean Time Between Failures
    - expected lifetime of a product before it fails and must be replaced or repaired
- MTTF – Mean Time To Failure
- BIA – Business Impact Analysis
    - MTD – Maximum Tolerable Downtime, MTD = WRT + RTO
    - MTTR
    - MTBF
    - RTO
    - RPO
    - WRT – Work Recovery Time
- DRP – Disaster Recovery Plan
- PIA – Privacy Impact Assesment
- PII – Personally Identifiable Information
- PHI – Personally Health Information
- CIS - nonprofit organization focused on developing globally-recognized best practices for securing IT systems and data against cyberattacks
- GLBA – Gram-Leach-Biley Act
- ESF – Enterprise Security Framework
    - Use existing guidelines where possible as a starting point
- Defense in Depth / Layered Security – diversity of vendors, controls
- Job creep / responsibility creep – nabywanie uprawnień zmieniając pozycje w zespołach, gdy ktoś zapomina odbierać te uprawnienia
- IA – Information Assurance

    - When dealing with computer hardware and software, risk management is also known as IA
- RCSA – Risk Control Self Assesment
    - Process by which management and staff of all levels identify and evaluate risks and associated controls
- EPHI – Electronic Protected Health Information
- HITECH – Health Information Technology for Economic and Clinical Health
- SOX – Sarbanes-Oxley Act
    - Financial reporting, created to protect investors
    - Sarbanes-Oxley (SOX) is a United States federal law that sets new or expanded requirements for all US public company boards, management, and public accounting firms
- Qualitative analysis
    - Assessment that assigns a numerical value to the probability of a risk and the impact it can have on the system or network
    - No monetary value is assigned to assets or possible losses
- Quantitative
    - Assign monetary exact value
- SPOF – Single Point of Failure

Wszystkie akty:

- FERPA - The Family Educational Rights and Privacy Act (FERPA) requires that educational institutions implement security and privacy controls for student educational records.

- GLBA - Gramm-Leach-Bliley Act (GLBA) institutes requirements that help protect the privacy of an individual's financial information held by financial institutions and others, such as tax preparation companies. The privacy standards and rules created as part of GLBA safeguard private information and set penalties in the event of a violation.

- SOX - Sarbanes-Oxley Act (SOX) dictates requirements for storing and retaining documents relating to an organization's financial and business operations, including the type of documents to be stored and their retention periods. It is relevant for any publicly-traded company with a market value of at least $75 million.

- HIPAA - The Health Insurance Portability and Accountability Act (HIPAA) establishes several rules and regulations regarding healthcare in the United States. With the rise of electronic medical records, HIPAA standards have been implemented to protect patient medical information privacy through restricted access to medical records and regulations for sharing medical records.

- FISMA - The Federal Information Security Management Act (FISMA) is a United States federal law that defines a comprehensive framework to protect government information, operations, and assets against natural or human-made threats. FISMA requires that government agencies and other organizations that operate systems on behalf of government agencies comply with security standards.

- COPPA - the Children's Online Privacy Protection Act (COPPA) is a United States federal law that imposes certain requirements on operators of websites or online services directed to children

under 13 years of age and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age.