NIST is cheap (public domain)
NIST **800-145** - The NIST Definition of Cloud Computing
NIST **800-53 -** Security and Privacy Controls for Federal Information Systems and Organizations:

1. Insider Threats
2. Software applications
3. Social networking
4. Mobile devices
5. Cloud computing
6. Persistent Threat
7. Privacy

NIST **500-293 –** guide, framework how to migrate to cloud
NIST **800-292** – Cloud Reference Architecture
NIST **800-64** - SDLC
NIST **800-37** - Risk management
NIST **800-61** - Incident Response

**FedRamp 2011 -** standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. It prescribes the security requirements and process cloud service providers must follow in order for the government to use their service. Fed Agencies!

**FRCP / FRE** – USA eDiscovery

**SOX –** USA, public companies, annual, financial

**FIPS 140-2 NIST –** Crypto modules:

- Level1 – no physical security
- Level2 – show evidence of tampering
- Level3 – full IAM
- Level4 – all plus data protection, zeroization

**Common Criteria F-S-M-M-S-S-F –** ISO 15408 – SFR and SAR Functional and Assurance, good for TPSP assurance

- EAL1 – Functionality Tested
- EAL2 – Structurally Tested
- EAL3 – Methodically Tested
- EAL4 – Methodically Designed and Tested
- EAL5 – Semi Formally Designed and Tested
- EAL6 – Semi Formally Verified
- EAL7 – Formally Verified and Tested

ISO **17788**:2014 - Cloud computing - Overview and vocabulary
ISO **17789**:2014 - Cloud computing - Reference architecture
ISO **27001**:2013 – IS gold standard – 14 domains, including risk assessment
ISO **27050** – eDiscovery – multitenancy complicates it!
ISO **27018 –** privacy standard in cloud, annual.
ISO **31000**:2009 – standard for risk mgmt. but no certification, 11 principals
ISO **27034** – SDLC / Application Sec - ONF- list of ALL controls, ANF- list of application controls.
ISO **27035** - Incident Response
ISO **38500**:2015 - Governance of IT for the organization
ISO **27014**:2013 - Security techniques - Governance of information security

**ENISA** – EU framework for risk management for cloud, 35 risks, TOP 8

- Includes Programmatic mgmt. in oppose to ISC2 / NIST definitions.

NIST **800-146** – USA version of ENISA, risk mgmt. in cloud, federal computing
NIST RMF – based on perceived risks

**PRIVACY:**

- EU Directive 95/46
- EU Directive 2002/58 – cookies and tracking
- **GDPR 2018** – PII includes mobile phone! Addresses performance by Data Controller and Processor. Brazil does not have a law which complies with EU.
- **GLBA** PII in financial org, user must OPT-OUT
- **HIPPA** – USA medical, enforced
- **Safe Harbour** – USA, Dep of Commerce
- **526-FZ** – Russia
- **GAPP** – privacy standard focused on risk, USA and Canada.
- **PIPEDA** – Canada, private sector
- **OECD** – multinational 37 members, crates non-binding policies
  - Use limitation principal
  - Openness principal
  - Does NOT have right to be forgotten clause!

**AUDIT:**
SAS70, USA replaced by SSAE 16 (USA), published by AICPA:

- SOC1 Typ1 (spot-check) / Typ2 (6 months) – financial
- SOC2 Typ1/2 – **CIAP + security principal!** controls, design, and evaluation of effectiveness (2), internal only
- SOC3 – similar to SOC2 but public, Quick TPSP assurance, Attestation!

ISAE – like SOC but International

**IS Mgmt System - ISMS** – a formal program and utilises ISO 27k

**ARCHITECTURE:**

- **SABSA** – business security architecture, look at security from business!
- **TOGAF** – open source architecture – security mixed with business
- **ITIL** best practices – 5 domains (Strategy, Design, Transition, Operation, Improvement) – Service Delivery!
- ISACA - **COBIT** - A Business Framework for the Governance and Management of Enterprise IT

**IETF** - is an international organization of network designers and architects who work together in establishing standards and protocols for the Internet.

**DMCA** – intellectual property, USA

**Data Center Standards:**

- BICSI – cabling
- IDCA – infinity paradigm, comprehensive, design and operation
- NFPA – fire protection
- Uptime Institute:
    - Tier1 – Basic controls, non-constant, good for archive
    - Tier2 – Redundant power and cooling, non-constant, good for archive
    - Tier3 – Concurrently Maintainable, always on
    - Tier4 – adding Fault Tolerance

**CSA Cloud Controls Matrix – CCM and CAIQ – framework of controls**

- Lists HIPPA, FERPA (student data) and PIPEDA (Canada, privacy)
- Lists COBIT, PCI and ISO and FedRamp
- Simplifying Compliance
    1. Application Security
    2. Audit Assurance and Compliance
    3. BCP
    4. Change and Configuration Mgmt
    5. Data Security
    6. Data Center Security
    7. Encryption
    8. Governance and Risk
    9. Human Resources
    10. IAM
    11. Infra and Virtual Security
    12. Interoperability and Portability
    13. Mobile Security
    14. IRM and eDiscovery
    15. Supply Chain and TPSP
    16. Threat and Vulnerability Mgmt

**CSA STAR Ratings:**

- Level 1 is a self-assessment
- Level 2 third-party assessment of the provider
- Level 3 requires continual monitoring by a third party

**Cloud Characteristics**:

- On demand
- Broad Network
- Resource pooling
- Rapid elasticity
- Measure service
- Multitenancy

**Cloud Cross-Cutting Aspects:**

- Interoperability
- Performance, Availability and Resilience
- Portability
- SLA
- Regulatory Requirements
- Security
- Privacy
- Auditability
- Governance

1. Maintenance and Versioning
2. Reversibility

**CSA Top Threats:**

1. Data breach
2. Data loss
3. Insufficient Identity Mgmt
4. Insecure API
5. System vulnerabilities
6. Account hijacking
7. Malicious insider
8. APT
9. Insufficient due diligence
10. Abuse use of cloud – sprawl
11. DoS
12. Shared technology issues

**Data lifecycle CSU-SAD, its not a cycle!:**

1. Create – classification (assign security control), new or modify. Can be Automatic or Manual
2. Store – storage, security controls
3. Use – read only
4. Share – internally and externally, use of DLP
5. Archive
6. Destroy

**DLP Data states – DAR vs DIT vs DIU**

**Masking:**

- Static – separate copy, test env, script
- Dynamic – live in prod, need to have full and masked on the same system
- Algorithmic – bi-directional

**Data Discovery:**

Metadata – Labels – Content (keywords, patterns, frequency)
Biggest challenges – location,

**DRM:**

A. Persistence
B. Disabling screencap capabilities
C. Automatic expiration
D. Dynamic policy control – access policy
E. Support formats

**Federation:**

- **SAML** – XML only, IdP and Service Provider, SAML assertation, authentication and authorization. Good for SSO. Developed by OASIS.
- **WS-Federation** – XML, SOAP and WSDL, realms, brokering, using building block. defines mechanisms for allowing different security realms to broker information on identities, identity attributes and authentication.
- **OpenID** – HTTP/URL only, authentication, based on OAuth, external IdP, cross-platform,
- **OpenID Connect** – REST and JSON; authentication, it was specifically designed with mobile apps in mind, instead of only web-based federation.
- **OAuth** – HTTP only via JSON, authorization framework. Good for API.
- **Shibboleth** – SSO based on SAML, open source, universities.
- **SSO** – opaque tokens, limited to one organization!
- **XACML** - standard for defining attribute-based access controls/authorizations. It is a policy language for defining access controls at a Policy Decision Point and then passing them to a Policy Enforcement Point. What an entity is allowed to do based on attrib. It works with SAML and OAuth.
- **Cross-domain Identity Management (SCIM)** is a standard for exchanging identity information between domains. It can be used for provisioning and deprovisioning accounts in external systems and for exchanging attribute information.
- **Proxy –** TPSP acts on behalf
- **Web of trust** – all are IdPs
- **CASB** is usually the IdP.

**SIEM:**

- Aggregation and Correlation
- Alerting
- Reporting / Compliance
- Dashboards
- Retention
- Continues Optimization

**Software Defined Networks - SDN:**

- Separate data traffic from control plane, zones
- Web portals and management of network appliances
- Filtering and forwarding is separated
- The NBI usually handles traffic between the SDN controllers and SDN applications.

**Converged Networking Model -** combines the underlying storage and IP networks to maximize the benefits of a cloud workload.

**Content distribution network - CDN,** is a geographically distributed network of proxy servers and their data centers. The goal is to provide high availability and performance by distributing the service spatially relative to end users. CDNs are often used to place large stores of multimedia data in a location geographically near to the end users who will consume that data; this approach is designed mostly to accomplish a reduction in data degradation due to distance between resource and user.

**ABAC** is better than **RBAC** in the cloud!

**BC/DR:**

NIST **800-61** - Incident Response
ISO **27035** - Incident Response
RPO – data (replication affects it) | RTO – time | RSL – percentage of service level
Do not restore to soon - risky!
BIA helps during the process. Remote Access is useful.

<u>**BC/DR Steps:**</u>

1. Define Scope
2. Gather Reqs – RTO and RPO
3. Analyze
4. Assess Risk
5. Design – technical controls
6. Implement
7. Test
8. Report
9. Revise

**API:**

- **REST –** caching, <u>JSON and XML</u>, HTTP, no crypto, client-server, IAM, make web request via URI; WWW is a RESTful protocol; uses TLS
- **SOAP –** envelopes, no caching, <u>XML only</u>, lower performance, less scalable; message level encryption

**SDLC:**

NIST **800-64** – SDLC
ISO **27034** – SDLC / Application Sec - ONF- list of ALL controls, ANF- list of application controls.

- **DAST –** TEST / PROD, discover paths and interfaces, simulated negative test cases
- **SAST –** TEST, code analysis
- **RASP –** tune based on variables, PROD

<u>**SDLC Steps:**</u>

1. Req Gathering and Feasibility – security req
2. Req Analysis – planning / deadlines
3. Design – what language, platform? Software construction?
4. Coding
5. Testing – DAST / PenTest
6. Maintanance – hot fixed, patches

**Threat modelling:**

**STRIDE -** Spoofing | Tampering | Repudiation | Inf Disclosure | DoS | Elevation of Priv.
**DREAD – Quantitative!**
Damage | Reproducibility | Exploitability | Affected Users | Discoverability
Threat vector has the most effect on EF

**Risk Assessment:**

NIST **800-37** - Risk management
ISO **31000**:2009 – standard for risk mgmt. but no certification, 11 principals
Framing – Assess – Monitor and Respond
ALE = SLE * ARO = $20
SLE= $10 and ARO=2
ARO – collect historical data!
Impact resulting from risk is measured in MONEY!

**Audit Plan:**

1. Define Objectives
2. Define Scope
3. Conduct Audit
4. Lesson Learned

**Monitoring:**
**A. Synthetic performance monitoring -** Synthetic agents can simulate user activity in a much faster, broader manner and perform these actions 24/7 without rest. More expensive than RUM
**B. Real-user monitoring (RUM):**

- Privacy concerns
- harvests information from actual user activity, making it the most realistic
- depiction of user behaviour.

**C. Security information and event management (SIEM)**
**D. Database application monitor (DAM)**

**HVAC systems:**

- cost impact – external ambient temp
- HALON is illegal due to harm to env.
- Floor raised by 24 inches / 2 feet

**Roles:**
**DELIVERY - Cloud Service Manager:** The cloud service manager is responsible for the delivery of cloud services, the provisioning of cloud services, and the overall management of cloud services. This person is typically responsible for policy design, business agreement, pricing model, and some elements of the SLA.
**MONITORING - Cloud Service Operations Manager** - is responsible for preparing systems for the cloud, administering and monitoring services, providing audit data as requested or required, and managing inventory and assets.
**MANAGING - Cloud Service Deployment Manager** - is responsible for gathering metrics on cloud services, managing cloud deployments and the deployment process, and defining the environments and processes.

**Dynamic resource scheduling (DRS)** is used within all clustering systems as the method for clusters to provide high availability, scaling, management, and workload distribution and balancing of jobs and processes. From a physical infrastructure perspective, DRS is used to balance compute loads between physical hosts in a cloud to maintain the desired thresholds and limits on the physical hosts.
**Dynamic optimization - DO:** constantly maintaining that resources are available

**Forensic / eDiscovery:**

- Evidence Inadmissible if it has no probative value
- Tests should not be tailored or customized!

**SSMS storage -** encrypting a data set, then splitting the data into pieces, splitting the key into pieces, then signing the data pieces and key pieces and distributing them to various cloud storage locations

**Data Custodian -** tasked with securing and maintaining the privacy data on a regular basis, daily, on behalf and under the guidance of the controller and steward.
**Data Steward –** simply put, Data Stewards are responsible for what is stored in a data field.
**Data Controller -** makes the determination of purpose and scope of privacy-related data sets. Data Custodians are responsible for the technical environment and database structure.
**Data Processor -** The entity that uses privacy data on behalf of the controller
**Data Owner** – Grant access to a data set