**CySA+ CS0-002 Exam Topics Notes**

\*\*\* Many of the un-linked topics (from 2.3 onwards) are from **CompTIA CySA+ Study   
 Guide** by Mike Chapple and David Seidl & **CCNA Cyber Ops SECFND 210-250 Official   
 Cert Guide** by Omar Santos, Joseph Muniz and Stefano de Crescenzo \*\*\*

\*\*\* Also check out [https://cheatsheetseries.owasp.org](https://cheatsheetseries.owasp.org/) from OWASP on many of the topics in 1.7 \*\*\*

**1.0 Threat and Vulnerability Management**

**1.1 Explain the importance of threat data and intelligence**

- Intelligence sources:

- **Open-source intelligence**

- **Proprietary/closed-source intelligence**

- **Timeliness**

- **Relevancy**

- **Accuracy**

- **Confidence levels**

- Indicator management:

- **STIX**

- **TAXII**

- **OpenIOC**

- Threat classification:

- **Known threat vs unknown threat**

- **Zero-day**

- **APT**

- Threat actors:

- **Nation-state**

- **Hacktivist**

- **Organised crime**

- Insider threat:

- **Intentional**

- **Unintentional**

- Intelligence cycle:

- **Requirements**

- **Collection**

- **Analysis**

- **Dissemination**

- **Feedback**

- **Commodity malware**

- Information sharing and analysis communities:

- **Healthcare**

- **Financial**

- **Aviation**

- **Government**

- **Critical infrastructure**

**1.2 Given a scenario, utilise threat intelligence to support organisational security**

- Attack frameworks:

- **MITRE ATT&CK**

- **The Diamond Model of Intrusion Analysis**

- **Kill chain**

- Threat research:

- **Reputational**

- **Behavioural**

- **IOC**

- **CVSS**

- Threat modelling methodologies:

- **Adversary capability**

- **Total attack surface**

- **Attack vector**

- **Impact**

- **Likelihood**

- Threat intelligence sharing with supported functions

- **Incident response**

- **Vulnerability management**

- **Risk management**

- **Security engineering**

- **Detection and monitoring**

**1.3 Given a scenario, perform vulnerability management activities**

- Vulnerability identification:

- **Asset criticality**

- **Active vs passive scanning**

- **Mapping/enumeration**

- Validation:

- **True positive**

- **False positive**

- **True negative**

- **False negative**

- Remediation/mitigation:

- **Configuration baseline**

- **Patching**

- **Hardening**

- **Compensating controls**

- **Risk acceptance**

- **Verification of mitigation**

- Scanning parameters and criteria:

- **Risks associated with scanning activities**

- **Vulnerability feed**

- **Scope**

- **Credentialed vs non-credentialed**

- **Server-based vs agent-based**

- **Internal vs external**

- Special considerations:

- **Types of data**

- **Technical constraints**

- **Workflow**

- **Sensitivity levels**

- **Regulatory requirements**

- **Segmentation**

- **IPS, IDS, and firewall settings**

- Inhibitors to remediation:

- **MOU**

- **SLA**

- **Organisational governance**

- **Business process interruption**

- **Degrading functionality**

- **Legacy systems**

- **Proprietary systems**

**1.4 Given a scenario, analyse the output from common vulnerability assessment tools**

- Web application scanner:

- **OWASP ZAP**

- **Burp suite**

- **Nikto**

- **Arachni**: [https://www.arachni-scanner.com](https://www.arachni-scanner.com/)

- Infrastructure vulnerability scanner:

- **Nessus**

- **OpenVAS**

- **Qualys**

- Software assessment tools and techniques:

- **Static analysis**

- **Dynamic analysis**

- **Reverse engineering**

- **Fuzzing**

- Enumeration:

- **Nmap**: [https://nmap.org](https://nmap.org/)

- **hping**: [http://www.hping.org](http://www.hping.org/)

- **Active vs passive**

- **Responder**: <https://github.com/SpiderLabs/Responder>

- Wireless assessment tools:

- **Aircrack-ng**: [https://www.aircrack-ng.org](https://www.aircrack-ng.org/)

- **Reaver**: <https://tools.kali.org/wireless-attacks/reaver>

- **oclHashcat**: <https://hashcat.net/wiki/doku.php?id=oclhashcat>

- Cloud infrastructure assessment tools:

- **ScoutSuite**: <https://github.com/nccgroup/ScoutSuite>

- **Prowler**: <https://github.com/toniblyx/prowler>

- **Pacu**: <https://github.com/RhinoSecurityLabs/pacu>

**1.5 Explain the threats and vulnerabilities associated with specialised technology**

- **Mobile**

- **IoT**

- **Embedded**

- **RTOS**

- **SoC**

- **FPGA**

- **Physical access control**

- **Building automation systems**

- Vehicles and drones:

- **CAN bus**

- **Workflow and process automation systems**

- **ICS**

- SCADA:

- **Modbus**

**1.6 Explain the threats and vulnerabilities associated with operating in the cloud**

- Cloud service models:

- **SaaS**

- **PaaS**

- **IaaS**

- Cloud deployment models:

- **Public**

- **Private**

- **Community**

- **Hybrid**

- **FaaS/serverless architecture**

- **IaC**

- **Insecure API**

- **Improper key management**

- **Unprotected storage**

- Logging and monitoring:

- **Insufficient logging and monitoring**

- **Inability to access**

**1.7 Given a scenario, implement controls to mitigate attacks and software vulnerabilities**

[https://cheatsheetseries.owasp.org](https://cheatsheetseries.owasp.org/)

- Attack types:

- **XML attack**

- **SQL injection**

- Overflow attack:

- **Buffer**

- **Integer**

- **Heap**

- **Remote code execution**

- **Directory traversal**

- **Privilege escalation**

- **Password spraying**

- **Credential stuffing**

- **Impersonation**

- **Man-in-the-middle attack**

- **Session hijacking**

- **Rootkit**

- Cross-site scripting:

- **Reflected**

- **Persistent**

- **DOM**

- Vulnerabilities:

- **Improper error handling**

- **Dereferencing**

- **Insecure object reference**

- **Race condition**

- **Broken authentication**

- **Sensitive data exposure**

- **Insecure components**

- **Insufficient logging and monitoring**

- **Weak or default configurations**

- Use of insecure functions:

- **strcpy**

**2.0 Software and Systems Security**

**2.1 Given a scenario, apply security solutions for infrastructure management**

- **Cloud vs on-premises**

- Asset management:

- **Asset tagging**

- Segmentation:

- **Physical**

- **Virtual**

- **Jumpbox**

- System isolation:

- **Air gap**

- Network architecture:

- **Physical**

- **Software-defined**

- **VPC**

- **VPN**

- **Serverless**

- **Change management**

- Virtualisation:

- **VDI**

- **Containerisation**

- Identity and access management:

- **Privilege management**

- **MFA**

- **SSO**

- **Federation**

- **Role-based**

- **Attribute-based**

- **Mandatory**

- **Manual review**

- **CASB**

- **Honeypot**

- **Monitoring and logging**

- **Encryption**

- **Certificate management**

- **Active defense**

**2.2 Explain software assurance best practices**

- Platforms:

- **Mobile**

- **Web application**

- **Client/server**

- **Embedded**

- **SoC**

- **Firmware**

- **SDLC integration**

- **DevSecOps**

- Software assessment methods:

- **User acceptance testing**

- **Stress test application**

- **Security regression testing**

- **Code review**

- Secure coding best practices:

- **Input validation**

- **Output encoding**

- **Session management**

- **Authentication**

- **Data protection**

- **Parameterised queries**

- **Static analysis tools**

- **Dynamic analysis tools**

- **Formal methods for verification of critical software**

- Service-oriented architecture:

- **SAML**

- **SOAP**

- **REST**

- **Microservices**

**2.3 Explain hardware assurance best practices**

- Hardware root of trust:

- **TPM**: <https://security.stackexchange.com/questions/88744/what-are-the-differences-between-tpm-and-hsm>

- **HSM**: <https://security.stackexchange.com/questions/88744/what-are-the-differences-between-tpm-and-hsm>

- **eFuse**: <https://en.wikipedia.org/wiki/IBM_eFUSE>

- **UEFI**: <https://www.makeuseof.com/tag/what-is-uefi-and-how-does-it-keep-you-more-secure/>

- **Trusted foundry**: <https://en.wikipedia.org/wiki/Trusted_Foundry_Program>

- Secure processing:

- **Trusted execution**: <https://en.wikipedia.org/wiki/Trusted_Execution_Technology>

- **Secure enclave**: <https://www.howtogeek.com/339705/what-is-apples-secure-enclave-and-how-does-it-protect-my-iphone-or-mac/>

- **Processor security extensions**: [http://infocenter.arm.com/help/index.jsp?topic=/](http://infocenter.arm.com/help/index.jsp?topic=/com.arm.doc.ddi0344k/Beidagja.html)

[com.arm.doc.ddi0344k/Beidagja.html](http://infocenter.arm.com/help/index.jsp?topic=/com.arm.doc.ddi0344k/Beidagja.html)

- **Atomic execution**: <https://en.wikipedia.org/wiki/Thread_safety>

- **Anti-tamper**: <https://en.wikipedia.org/wiki/Tamperproofing>

- **Self-encrypting drive**: <https://www.computerweekly.com/feature/Self-encrypting-drives-SED-the-best-kept-secret-in-hard-drive-encryption-security>

- **Trusted firmware updates**: <https://github.com/ARM-software/arm-trusted-firmware/blob/master/docs/components/firmware-update.rst>

- **Measured boot and attestation**: <https://forums.juniper.net/t5/Security/What-s-the-Difference-between-Secure-Boot-and-Measured-Boot/ba-p/281251>

<https://seclab.stanford.edu/pcl/cs259/projects/cs259_final_lavina_jayesh/CS259_report_lavina_jayesh.pdf>

- **Bus encryption**: <https://en.wikipedia.org/wiki/Bus_encryption>

**3.0 Security Operations and Monitoring**

**3.1 Given a scenario, analyse data as part of security monitoring activities**

- **Heuristics**:

- **Trend analysis**:

- Endpoint:

- Malware:

- **Reverse engineering**:

- **Memory**

- System and application behaviour:

- **Known-good behaviour**

- **Anomalous behaviour**

- **Exploit techniques**: <https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/Sophos-Comprehensive-Exploit-Prevention-wpna.pdf>

- **File system**

- **UEBA**: <https://digitalguardian.com/blog/what-user-and-entity-behavior-analytics-definition-ueba-benefits-how-it-works-and-more>

- Network:

- URL and DNS analysis:

- **Dynamically generated algorithms**: <https://en.wikipedia.org/wiki/Domain_generation_algorithm>

- **Flow analysis**

- Packet and protocol analysis:

- **Malware**: <https://isc.sans.edu/forums/diary/Packet+Analysis+Where+do+you+start/22001/>

- Log review:

- **Event logs**

- **Syslog**:

- **Firewall logs**: <https://www.manageengine.com/products/firewall/firewall-logs.html>

- **WAF**: <https://docs.aws.amazon.com/waf/latest/developerguide/waf-incident-response.html>

- **Proxy**: <https://www.vanimpe.eu/2016/10/21/proxy-server-logs-incident-response/>

- **IDS/IPS**: <https://www.manageengine.com/products/eventlog/ids-ips-monitoring-reporting.html>

- Impact analysis:  
 - **Organisation impact vs localised impact**

- **Immediate vs total**

- SIEM review:

- **Rule writing**: <https://www.exabeam.com/siem/siem-threat-detection-rules-or-models/>

- **Known-bad IP**: [https://ipremoval.sms.symantec.com](https://ipremoval.sms.symantec.com/)

- **Dashboard**: <https://logz.io/blog/siem-dashboard-aws-elk-stack/>

- Query writing:

- **String search**: <https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/search-queries>

- **Script**: <https://devblogs.microsoft.com/scripting/event-log-queries-using-powershell/>

- **Piping**: <https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/get-started-queries>

- E-mail analysis:

- **Malicious payload**: <https://www.proofpoint.com/au/threat-reference/malicious-email-attachments>

- **DKIM**: <https://www.dmarcanalyzer.com/dkim/>

- **DMARC**: <https://www.sparkpost.com/resources/email-explained/dmarc-explained/>

- **SPF**: <https://www.dmarcanalyzer.com/spf/>

- **Phishing**: <https://drive.google.com/file/d/1du2MhdvEDW6pWijVc976CV3cRtUeS9y5/view>

- **Forwarding**: <https://logrhythm.com/blog/detecting-and-preventing-auto-forwarding-and-phishing-attacks-in-office-365/>

- **Digital signature**: <https://support.office.com/en-us/article/secure-messages-by-using-a-digital-signature-549ca2f1-a68f-4366-85fa-b3f4b5856fc6>

- **E-mail signature block**: <https://en.m.wikipedia.org/wiki/Signature_block>

- **Embedded links**: [https://www.websense.com/content/support/library/email/v85/](https://www.websense.com/content/support/library/email/v85/email_help/url_analysis.aspx)

[email\_help/url\_analysis.aspx](https://www.websense.com/content/support/library/email/v85/email_help/url_analysis.aspx)

- **Impersonation**: <https://blog.ironbastion.com.au/email-impersonation-scams-phishing-what-your-staff-can-do/>

- **Header**: <https://mlhale.github.io/nebraska-gencyber-modules/phishing/email-headeranalysis/#email-headers>

**3.2 Given a scenario, implement configuration changes to existing controls to improve   
 security**

- **Permissions**

- **Whitelisting**: <https://techterms.com/definition/whitelist>

- **Blacklisting**: <https://blog.finjan.com/blacklisting-vs-whitelisting-understanding-the-security-benefits-of-each/>

- **Firewall**: <https://computer.howstuffworks.com/firewall2.htm>

- **IPS rules**: <https://help.fortinet.com/cli/fos50hlp/56/Content/FortiOS/fortiOS-cli-ref-56/config/ips/rule.htm>

- **DLP**: <https://digitalguardian.com/blog/what-data-loss-prevention-dlp-definition-data-loss-prevention>

- **EDR**: <https://www.crowdstrike.com/epp-101/what-is-endpoint-detection-and-response-edr/>

- **NAC**

- **Sinkholing**

- Malware signatures:

- **Development/rule writing**[: https://insights.sei.cmu.edu/sei\_blog/2012/11/writing-effective-yara-signatures-to-identify-malware.html](https://insights.sei.cmu.edu/sei_blog/2012/11/writing-effective-yara-signatures-to-identify-malware.html)

- **Sandboxing**

- **Port security**

**3.3 Explain the importance of proactive threat hunting**

- **Establishing a hypothesis**: [https://resources.infosecinstitute.com/category/enterprise/threat-hunting/threat-hunting-process/threat-hunting-methodologies/ - gref](https://resources.infosecinstitute.com/category/enterprise/threat-hunting/threat-hunting-process/threat-hunting-methodologies/#gref)

- **Profiling threat actors and activities**: <https://cis.verint.com/2019/10/15/how-threat-actor-profiling-enhances-security-resilience-part-1/>

- Threat hunting tactics:

- **Executable process analysis**: <https://niiconsulting.com/checkmate/2017/08/threat-hunting-for-masquerading-windows-processes/>

- **Reducing the attack surface area**: <https://www.securitymagazine.com/articles/89283-ways-to-reduce-your-attack-surface>

- **Bundling critical assets**: <https://www.dummies.com/business/accounting/auditing/what-does-it-mean-to-bundle-assets/> (although this refers to the financial assets, the concepts can be applicable to security as well)

- **Attack vectors**: <https://searchsecurity.techtarget.com/definition/attack-vector>

- **Integrated intelligence**: <https://integratedintelsolutions.com/what-we-do/integrated-intelligence/>

- **Improved detection capabilities**: <https://blog.gigamon.com/2018/09/27/how-threat-hunting-can-evolve-your-detection-capabilities/>

**3.4 Compare and contrast automation concepts and technologies**

- **Workflow orchestration**: <https://www.bmc.com/blogs/workflow-orchestration/>

- **Scripting**: <https://www.papercut.com/support/resources/manuals/ng-mf/common/topics/customize-scripting.html>

- **API integration**: <https://www.hcltech.com/technology-qa/what-is-api-integration>

- **Automated malware signature creation**: [https://patents.google.com/patent](https://patents.google.com/patent/US8201244B2/en)

[/US8201244B2/en](https://patents.google.com/patent/US8201244B2/en)

- **Data enrichment**: <https://www.securonix.com/data-enrichment-the-key-ingredient-for-siem-success/>

- **Threat feed combination**: <https://www.exabeam.com/siem/threat-intelligence-feeds/>

- **Machine learning**: <https://www.cisco.com/c/en/us/products/security/machine-learning-security.html#~how-ml-helps-security>

- Use of automation protocols and standards:

- **SCAP**

- **Continuous integration**

- **Continuous deployment/delivery**

**4.0 Incident Response**

**4.1 Explain the importance of the incident response process**

- Communication plan:

- **Limiting communication to trusted parties**: <https://searchsecurity.techtarget.com/tip/Incident-response-How-to-implement-a-communication-plan>

- **Disclosing based on regulatory/legislative requirements**: <https://www.oaic.gov.au/privacy/notifiable-data-breaches/>

- **Preventing inadvertent release of information**

- **Using a secure method of communication**: [https://www.riskmanagement](https://www.riskmanagementmonitor.com/secure-messaging-in-incident-response-and-business-continuity/)

[monitor.com/secure-messaging-in-incident-response-and-business-continuity/](https://www.riskmanagementmonitor.com/secure-messaging-in-incident-response-and-business-continuity/)

- **Reporting requirements**: <https://thycotic.com/company/blog/2019/03/19/cyber-security-incident-response-reporting-process/>

- Response coordination with relevant entities:

- **Legal**

- **Human resources**

- **Public relations**

- **Internal and external**: <https://www.securitymagazine.com/articles/78810-incident-response-communication-is-key-1>

- **Law enforcement**

- **Senior leadership**

- **Regulatory bodies**: [https://www.sans.org/reading-room/whitepapers/](https://www.sans.org/reading-room/whitepapers/legal/paper/37487)

[legal/paper/37487](https://www.sans.org/reading-room/whitepapers/legal/paper/37487)

- Factors contributing to data criticality:

- **PII**: <https://www.getfilecloud.com/blog/2015/03/what-is-pii-and-phi-why-is-it-important/#.XfdSvC2B1TY>

- **PHI**: <https://www.getfilecloud.com/blog/2015/03/what-is-pii-and-phi-why-is-it-important/#.XfdSvC2B1TY>

- **SPI**: <https://www.boldonjames.com/blog/gdpr-effective-approaches/>

- **High value asset**: <https://www.cisa.gov/sites/default/files/publications/CISAInsights-Cyber-SecureHighValueAssets_S508C.pdf>

- **Financial information**: <https://definitions.uslegal.com/f/financial-information/>

- **Intellectual property**: <https://www.ipaustralia.gov.au/understanding-ip>

- **Corporate information**: <https://www.lawinsider.com/dictionary/corporate-information>

**4.2 Given a scenario, apply the appropriate incident response procedure**

- Preparation:

- **Training**: <https://digitalguardian.com/blog/five-steps-incident-response>

- **Testing**: <https://www.securitymetrics.com/blog/6-phases-incident-response-plan>

- **Documentation of procedures**

- Detection and analysis:

- **Characteristics contributing to severity level classification**

- **Downtime**

- **Recovery time**

- **Data integrity**

- **Economic**

- **System process criticality**: <https://www.nist.gov/publications/criticality-analysis-process-model>

- **Reverse engineering**

- **Data correlation**

- Containment:

- **Segmentation**

- **Isolation**

- Eradication and recovery:

- **Vulnerability mitigation**

- **Sanitisation**: <https://clarabyte.com/blogs/news/what-is-media-sanitization>

- **Reconstruction/reimaging**

- **Secure disposal**: <https://advisera.com/27001academy/blog/2018/10/22/5-practical-tips-for-media-disposal-according-to-iso-27001/>

- **Patching**

- **Restoration of permissions**

- **Reconstitution of resources**: <https://blogs.getcertifiedgetahead.com/implementing-incident-response-procedures/>

- **Restoration of capabilities and services**: <https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901>

- **Verification of logging/communication to security monitoring**: [https://www.](https://www.manageengine.com.au/products/service-desk/itil-incident-management-guide.html)

[manageengine.com.au/products/service-desk/itil-incident-management-guide.html](https://www.manageengine.com.au/products/service-desk/itil-incident-management-guide.html)

- Post-incident activities:

- **Evidence retention**

- **Lessons learned report**

- **Change control process**

- **Incident response plan update**

- **Incident summary report**

- **IOC generation**: <https://www.projectsharp.org/2019/07/04/incident-response-and-ioc/>

- **Monitoring**: <https://www.secpod.com/blog/the-need-for-continuous-monitoring-and-incident-response/>

**4.3 Given an incident, analyse potential indicators of compromise**

- Network-related:

- **Bandwidth consumption**

- **Beaconing**

- **Irregular peer-to-peer communication**

- **Rogue device on the network**

- **Scan/sweep**

- **Unusual traffic spike**

- **Common protocol over non-standard port**: [https://security.stackexchange.com](https://security.stackexchange.com/questions/185503/what-are-non-standard-ports-and-protocols)

[/questions/185503/what-are-non-standard-ports-and-protocols](https://security.stackexchange.com/questions/185503/what-are-non-standard-ports-and-protocols)

- Host-related:

- **Processor consumption**

- **Memory consumption**

- **Drive capacity consumption**

- **Unauthorised software**

- **Malicious process**

- **Unauthorised change**

- **Unauthorised privilege**

- **Data exfiltration**

- **Abnormal OS process behaviour**: <https://www.sans.org/security-resources/posters/dfir-find-evil/35/download>

- **File system change or anomaly**: <https://www.symantec.com/connect/articles/incident-response-tools-unix-part-two-file-system-tools>

- **Registry change or anomaly**: <https://www.sans.org/security-resources/posters/dfir-find-evil/35/download>

- **Unauthorised scheduled task**: [https://blog.malwarebytes.com/cybercrime/2015](https://blog.malwarebytes.com/cybercrime/2015/03/scheduled-tasks/)

[/03/scheduled-tasks/](https://blog.malwarebytes.com/cybercrime/2015/03/scheduled-tasks/)

<https://www.csoonline.com/article/3373498/how-to-audit-windows-task-scheduler-for-cyber-attack-activity.html>

- Application-related:

- **Anomalous activity**

- **Introduction of new accounts**

- **Unexpected output**

- **Unexpected outbound communication**

- **Service interruption**

- **Application log**

**4.4 Given a scenario, utilise basic digital forensics techniques**

- Network:

- **Wireshark**

- **tcpdump**

- Endpoint:

- **Disk**

- **Memory**

- **Mobile**

- **Cloud**

- **Virtualisation**: <https://www.astroarch.com/tvp_strategy/virtualization-forensics-how-different-is-it-5126/>

<https://resources.infosecinstitute.com/category/computerforensics/introduction/areas-of-study/digital-forensics/forensic-issues-with-virtual-systems/#gref>

- **Legal hold**: <https://www.logikcull.com/guide/legal-holds-data-preservation>

- **Procedures**

- Hashing:

- **Changes to binaries**

- **Carving**: <http://www.forensicexplorer.com/data-carve.php>

- **Data acquisition**

**5.0 Compliance and Assessment**

**5.1 Understand the importance of data privacy and protection**

- **Privacy vs security**: <https://us.norton.com/internetsecurity-privacy-privacy-vs-security-whats-the-difference.html>

- Non-technical controls:

- **Classification**

- **Ownership**

- **Retention**

- **Data types**

- **Retention standards**: <https://assets.kpmg/content/dam/kpmg/nl/pdf/2018/advisory/data-retention.pdf>

- **Confidentiality**: <https://www1.udel.edu/security/data/confidentiality.html>

- **Legal requirements**: <https://en.wikipedia.org/wiki/Privacy_law#United_States>

- **Data sovereignty**: <https://rgtechnologies.com.au/resources/data-sovereignty/>

- **Data minimisation**: <https://www.experian.co.uk/business/glossary/data-minimisation/>

- **Purpose limitation**: <https://iapp.org/news/a/on-the-death-of-purpose-limitation/>

- **NDA**: <https://www.ipaustralia.gov.au/ip-for-digital-business/idea/non-disclosure-agreements>

- Technical controls:

- **Encryption**: <https://digitalguardian.com/blog/what-data-encryption>

- **DLP**

- **Data masking**: <https://searchsecurity.techtarget.com/definition/data-masking>

- **Deidentification**: <https://www.truevault.com/resources/developer/what-is-data-de-identification>

- **Tokenisation**: <https://www.tokenex.com/about/what-is-tokenization>

- DRM:

- **Watermarking**: <https://en.wikipedia.org/wiki/Digital_rights_management#Watermarks>

<https://www.locklizard.com/document-security-blog/document-security-watermark/>

- **Geographic access requirements**

- **Access controls**

**5.2 Given a scenario, apply security concepts in support of organisational risk mitigation**

- **Business impact analysis**: <https://resources.infosecinstitute.com/category/certifications-training/securityplus/sec-domains/risk-management-in-security/business-impact-analysis-concepts/#gref>

- **Risk identification process**: <https://www.mitre.org/publications/systems-engineering-guide/acquisition-systems-engineering/risk-management/risk-identification>

- Risk calculation:

- **Probability**

- **Magnitude**

- **Communication of risk factors**: <https://www.isaca.org/Journal/archives/2010/Volume-1/Pages/Performing-a-Security-Risk-Assessment1.aspx>  
 - Risk prioritisation:

- **Security controls**: <https://www.project-risk-manager.com/blog/risk-prioritisation/>

- **Engineering tradeoffs**: <https://risk-engineering.org/risk-management/>

- **Systems assessment**

- **Documented compensating controls**

- Training and exercises:

- **Red team**

- **Blue team**

- **White team**

- **Tabletop exercise**: <https://www.csoonline.com/article/2838365/planning-for-a-security-emergency-from-the-tabletop-down.html>

- Supply chain assessment:

- **Vendor due diligence**: <https://rfp360.com/vendor-due-diligence/>

- **Hardware source authenticity**

**5.3 Explain the importance of frameworks, policies, procedures, and controls**

- Frameworks:

- **Risk-based**

- **Prescriptive**

- Policies and procedures:

- **Code of conduct/ethics**: [https://s21.q4cdn.com/798735247/files/doc\_downloads/](https://s21.q4cdn.com/798735247/files/doc_downloads/corporate_governance/Code-of-Conduct-Policy.pdf)

[corporate\_governance/Code-of-Conduct-Policy.pdf](https://s21.q4cdn.com/798735247/files/doc_downloads/corporate_governance/Code-of-Conduct-Policy.pdf)

- **AUP**

- **Password policy**

- **Data ownership**

- **Data retention**

- **Account management**

- **Continuous monitoring**

- **Work product retention**: [https://www.nfib.com/Portals/0/PDF/AllUsers/legal/guides/](https://www.nfib.com/Portals/0/PDF/AllUsers/legal/guides/document-retention-policy-guide-nfib.pdf)

[document-retention-policy-guide-nfib.pdf](https://www.nfib.com/Portals/0/PDF/AllUsers/legal/guides/document-retention-policy-guide-nfib.pdf)

- Control types:

- **Managerial**

- **Operational**

- **Technical**

- **Preventative**

- **Detective**

- **Responsive**

- **Corrective**

- Audits and assessments:

- **Regulatory**

- **Compliance**