بسم الله الرحمن الرحيم

KHAWAJAGAN Technologies

SP 2025

# Secure Software Design and Development

CYC386

LECTURE 003 – 28-FEB-2025

FAISAL SHAHZAD

SP 2025

## Compliance Requirements

## Regulations & Compliance

- Regulations and compliance drive many activities in an enterprise.
- Failure to comply with rules and regulations can lead to direct, and in some cases substantial, financial penalties.
- Compliance failures can carry additional costs, as in increased scrutiny, greater regulation in the future, and bad publicity.
- Since software is a major driver of many business processes, a Developer/Auditor needs to understand the basis behind various rules and regulations and how they affect the enterprise in the context of their own development efforts.
- This enables decision-making as part of the software development process that is in concert with these issues and enables the enterprise to remain compliant.

## Regulations & Compliance

- Regulations can come from several sources, including industry and trade groups and government agencies.
- The penalties for noncompliance can vary as well, sometimes based on the severity of the violation and other times based on political factors.
- The factors determining which systems are included in regulation and the level of regulation also vary based on situational factors.
- Typically, these factors and rules are published significantly in advance of instantiation to allow firms time to plan enterprise controls and optimize risk management options.
- Although not all firms will be affected by all sets of regulations, it is also not uncommon for a firm to have multiple sets of regulations across different aspects of an enterprise, even overlapping on some elements.
- This can add to the difficulty of managing compliance, as different regulations can have different levels of protection requirements.

SP 2025

## Security Standards

## Security Standards - SS

- Standards serve a function by defining a level of activity that allows different organizations to interact in a known and meaningful way.
- Standards also facilitate comparisons between organizations.
- The process of security in an enterprise is enhanced through the use of standards that enable activities associated with best practices.
- Security standards serve a role in promoting interoperability as in software design and development, there will be many cases where modules from different sources will be interconnected.
- Wellknown security standards classes includes ISO, NIST, FISMA, HIPAA, HITECH and PCI-DSS

## SS – ISO

- ISO is the International Organization for Standardization, a group that develops and publishes international standards.
- The United States has an active relationship to ISO through the activities of the U.S. National Committee, the International Electrotechnical Commission (IEC), and the American National Standards Institute (ANSI).
- ISO has published a variety of standards covering the information security arena.
- To ensure that these standards remain relevant with respect to ever-changing technology and threats, ISO standards are on a five-year review cycle.
- The relevant area of the standards catalog are under
  - JTC 1 – Information Technology, specifically subcommittees 7 (Software and Systems Engineering)
  - 27 (IT Security Techniques).

## SS – ISO

| | |
|---|---|
| ISO/IEC 25010:2011 | Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – System and software quality models. |
| ISO/IEC 10746 | Information Technology – Open distributed processing. Multipart series standard. |
| ISO/IEC/IEEE 12207:2017 | Systems and Software Engineering – Software life cycle processes |
| ISO/IEC 14143 | Information Technology – Software measurement – Functional size measurement. Multipart series standard. |
| ISO/IEC/IEEE 15026-1:2019 | Systems and software engineering – Systems and software assurance. |
| ISO/IEC/IEEE 15288:2015 | Systems and Software Engineering – System life cycle processes |

## SS – ISO

| | |
|---|---|
| ISO/IEC 15408 | Information technology – Security techniques – Evaluation criteria for IT security (Common Criteria) |
| ISO/IEC 21827 | Information Technology – Security techniques – Systems Security Engineering – Capability Maturity Model (SSE-CMM) |
| ISO/IEC 27000:2018 | Information Security Management System (ISMS) Overview and Vocabulary |
| ISO/IEC 27002:2013 | Code of Practice for Information Security Management |
| ISO/IEC 27003:2017 | Information security management systems — Guidance |
| ISO/IEC 27004:2016 | Information Security Management – Monitoring, measurement, analysis and evaluation |
| ISO/IEC 27005:2018 | Information Security Risk Management |

## SS – ISO/IEC 15408 Common Criteria

- The Common Criteria(CC) is a framework where security functional and assurance requirements can be specified in precise terms, allowing vendors to implement and/or make claims about the security attributes of their products.
- Testing laboratories can evaluate the products to determine if they actually meet the claims stated using the CC framework.
- The CC provide a measure of assurance that specific objectives are present in a given product.
- CC use specific terminology to describe activity associated with the framework.
  - The Target of Evaluation (TOE) is the product or system that is being evaluated.
  - The Security Target (ST) is the security properties associated with a TOE.
  - The Protection Profile (PP) is a set of security requirements associated with a class of products; i.e., firewalls have PPs and operating systems have PPs, but these may differ.
  - PPs help streamline the comparison of products within product classes.

## SS – ISO/IEC 15408 Common Criteria

- The output of the Common Criteria process is an evaluation assurance level (EAL), a set of seven levels, from 1, the most basic, through 7, the most comprehensive.
- The higher the EAL value, the higher the degree of assurance that a TOE meets the claims. Higher EAL does not indicate greater security.
- Criteria:

| Evaluation Assurance Level (EAL) | TOE Assurance |
|---|---|
| EAL 1 | Functionally tested |
| EAL 2 | Structurally tested |
| EAL 3 | Methodically tested and checked |
| EAL 4 | Methodically designed, tested, and reviewed |
| EAL 5 | Semiformally designed and tested |
| EAL 6 | Semiformally verified, designed, and tested |
| EAL 7 | Formally verified, designed, and tested |

# SS – ISO/IEC 9126: SW Engg. Quality

- Product quality is an international standard for the evaluation of software quality.
- The standard provides a framework that defines a quality model for the software product and addresses internal metrics that measure the quality of the software and external metrics that measure the software results during operation.
- Quality-of-use metrics are included to examine the software in particular scenarios which are as follows.
  - Functionality
  - Reliability
  - Usability
  - Efficiency
  - Maintainability
  - Portability

# SS – ISO/IEC/IEEE 12207

- Systems and Software Engineering – Software Life Cycle Processes
- This standard establishes a set of processes covering the lifecycle of the software.
- Each process has a defined set of activities, tasks, and outcomes associated with it.
- The standard acts to provide a common structure so all parties associated with the software development effort can communicate through a common vocabulary.

# SS – ISO/IEC 33001:2015

- Process assessment, also known as SPICE (Software Process Improvement and Capability Evaluation) - international concerns over the term evaluation has resulted in the substitution of the term determination (SPICD).
- ISO 33001 is a set of technical standards documents for the computer software development process derived from ISO/IEC 12207 and ISO 15504, the process lifecycle standard, and from maturity models like the CMM.
- ISO 33001 is used for process capability determination and process improvement efforts related to software development.

| Level | Name |
|---|---|
| 5 | Optimizing process |
| 4 | Predictable process |
| 3 | Established process |
| 2 | Managed process |
| 1 | Performed process |
| 0 | Incomplete process |

# NIST

- The National Institute of Standards and Technology is a federal agency working with industry to develop technology, measurements, and standards that align with the interests of the U.S. economy.
- The Computer Security Division is the element of NIST for computer security issues, including those necessary for compliance with the Federal Information Security Management Act of 2002 (FISMA) and its successors.
- NIST develops and publishes several relevant document types associated with information security. The two main types of documents are Federal Information Processing Standards (FIPS) and the Special Publication (SP) 800 series from the NIST Information Technology Laboratory (ITL).
- The ITL's Computer Security Division also publishes security bulletins on an average of six times a year, presenting an in-depth discussion of a single topic of significant interest to the information systems community.
- NIST also publishes Interagency or Internal Reports (NISTIRs) that describe research of a technical nature.

# NIST – FIPS / SP-800

- **Federal Information Processing Standards (FIPS)**
  - The Federal Information Processing Standards (FIPS) are mandatory sets of requirements on federal agencies and specific contractors.
  - Although limited in number, they are wide sweeping in authority and scope.
  - Older FIPS had sections describing a waiver process, but since the passage of FISMA, all aspects of FIPS are now mandatory, and the waiver process is no longer applicable.
- **NIST SP 800 Series**
  - The more common set of NIST publications utilized by industry is the 800 series of Special Publications which are designed to communicate the results of relevant research and guidelines associated with securing information systems.
  - The 800 series has documents ranging from describing cryptographic protocols, to security requirements associated with a wide range of system elements, to risk management framework elements associated with information security governance.

# NIST – FIPS / SP-800

| | |
|---|---|
| FIPS 200 | Minimum Security Requirements for Federal Information and Information Systems |
| FIPS 199 | Standards for Security Categorization of Federal Information and Information Systems |
| FIPS 197 | Advanced Encryption Standard (AES) |
| FIPS 186-3 | Digital Signature Standard (DSS) |
| FIPS 190-4 | Secure Hash Standard (SHS) |
| FIPS 140 series | Security Requirements for Cryptographic Modules |
| SP 800-152 | A Profile for U.S. Federal Cryptographic Key Management Systems (CKMS) |
| SP 800-107 | Recommendation for Applications Using Approved Hash Algorithms |
| SP 800-100 | Information Security Handbook: A Guide for Managers |
| SP 800-63 | Digital Identity Guidelines (a 4 volume set of documents) |
| SP 800-53 | Security and Privacy Controls for Information Systems and Organizations |
| SP 800-30 | Guide for Conducting Risk Assessments |
| SP 800-12 | An Introduction to Computer Security |

# NIST – RMF

- NIST has responded with a series of publications detailing a security lifecycle built around a risk management framework.
- NIST SP 800-39 is a six-step process to create an RMF is designed to produce a structured and flexible methodology of managing the risk associated with information systems.
- The six steps are

# Industry Standards

SP 2025

# Industry Standards - SAFECode

- SAFECode is an industry-backed organization that is committed to increasing communication between firms on the topic of software assurance.
- This group was formed by members who voluntarily share their practices, which together form a best practice solution.
- SAFECode is dedicated to communicating best practices that have been used successfully by member firms.
- A sampling of SAFECode's publications include
  - Software Assurance: An Overview of Current Industry Best Practices
  - Fundamental Practices for Secure Software Development, 3rd Edition
  - Overview of Software Integrity Controls
  - Security Engineering Training

SAFECode

# Industry Standards - OWASP

- The Open Web Application Security Project (OWASP) is a worldwide free and open community focused on improving the security of application software.
- OWASP publishes a series of Top Ten vulnerability lists highlighting the current state-of-the-art threats facing web application developers.
- OWASP maintains a website (www.owasp.org) with significant resources to help firms build better software and eliminate these common and pervasive problems.

OWASP
Open Web Application Security Project

# Industry Standards – PCI-DSS

- PCI stands for Payment Card Industry, an industry group established to create, manage, and enforce regulations associated with the securing of cardholder data.
- PCI standards are contractual requirements if a firm accepts payment cards, stores payment card data, or makes products associated with payment cards and can carry severe financial penalties for failing to comply.
- Three main standards designed to provide a basic level of protection for cardholder data are:
  - The Data Security Standard (PCI DSS)
  - The Payment App. Data Security Standard (PA DSS)
  - PIN Transaction Security (PTS).

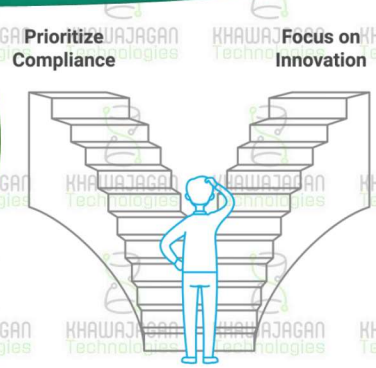
PCI Security Standards Council

# Industry Standards – PCI-DSS

- PCI DSS
  - The PCI DSS is the governing document that details the contractual requirements for members that accept and process bank cards.
  - This standard includes requirements for security management, policies and procedures, network architecture, software design, and other critical protective measures for all systems associated with the processing and storing of cardholder data.
  - Arranged in six groups of control objectives, 12 high-level requirements are detailed.
  - Under each of these requirements are a significant number of sub-requirements and testing procedures that are used to determine a baseline security foundation.
- PA DSS
  - The PA DSS standard is a set of requirements used by software vendors to validate that a payment application is compliant with the requirements associated with PCI DSS.
- PTS
  - One of the most important elements of the cardholder data is the PIN, and security aspects associated with the PIN are governed by the PTS standard.
  - The majority of this standard applies to hardware devices known as PIN entry devices (PEDs).

SP 2025

# Government Regulations




## FISMA

- The Federal Information Security Management Act of 2002 (FISMA) is a federal law that requires each federal agency to implement an agency-wide information security program.
- The National Institute of Standards and Technology (NIST) was designated the agency to develop implementation guidelines and did so through the publication of a risk management framework (RMF) for compliance.
- The initial compliance framework included the following set of objectives, which were scored on an annual basis by the Inspector General's office:
  - Inventory of systems
  - Categorize information and systems according to risk level
  - Security controls
  - Certification and accreditation of systems (including risk assessment and system security plans)
  - Training

## Sarbanes-Oxley

- The Sarbanes-Oxley Act of 2002 was a reaction to several major accounting and corporate scandals, costing investors billions and shaking public confidence in the stock markets.
- Although composed of many parts, the primary element concerned with information security is Section 404, which mandates a specific level of internal control measures.
- In simple terms, the information systems used for financial accounting must have some form of security control over integrity so that all may have confidence in the numbers being reported by the system.
- Criticized by many for its costs, it is nonetheless the current law, and financial reporting systems must comply.

## Gramm-Leach-Bliley (GLBA)

- The Financial Modernization Act of 1999, also known as the Gramm-Leach-Bliley Act (GLBA), contains elements designed to protect consumers' personal financial information (PFI).
- From a software perspective, it is important to understand that the act specifies rules as to the collection, processing, storage, and disposal of PFI.
- The three primary rules worth noting are
  - The Financial Privacy Rule, which governs the collection and disclosure of PFI, including companies that are nonfinancial in nature
  - The Safeguards Rule, which applies to financial institutions and covers the design, implementation, and maintenance of safeguards deployed to protect PFI
  - The Pretexting Protections, which addresses the use of pretexting (falsely pretending) to obtain PFI

## HIPAA and HITECH

- While GLBA deals with PFI, the Healthcare Insurance Portability and Accountability Act (HIPAA) deals with personal health information (PHI).
- PHI contains information that can have significant value to criminal organizations.
- Enacted in 1996, the privacy provisions of HIPAA were not prepared for the industry movement to electronic records.
- The Health Information Technology for Economic and Clinical Health Act (HITECH Act) is part of the American Recovery and Reinvestment Act of 2009 (ARRA) and is designed to enhance privacy provisions of electronic personal health information records.

## GDPR

- Two factors led to what can only be seen as a complete rewrite of EU data protection regulations.
- In light of the Snowden revelations, the EU began a new round of examining data protection when shared with the United States and others.
- This brought Safe Harbor provisions into the spotlight as the EU wanted to renegotiate stronger protections.
- Then, the European Court of Justice invalidated the Safe Harbor provisions.
- This led the way to the passage of the General Data Protection Regulation (GDPR), which went into effect in May 2018.

## GDPR

- The GDPR ushers in a brand-new world with respect to data protection and privacy. With global trade being important to all countries, the ability to transfer data, including personal data, between parties becomes important.
- Enshrined in the Charter of Fundamental Rights of the EU is the fundamental right to the protection of personal data, including when such data elements are transferred outside the EU.
- For all firms that want to trade with the EU, there is now a set of privacy regulations that will require specific programs to address the requirements.
- The GDPR brings many changes, one being the appointment of a data protection officer (DPO). This role may be filled by an employee or a third-party service provider (for example, consulting or law firm), and it must be a direct report to the highest management level.
- The DPO should operate with significant independence, and provisions in the GDPR restrict control over the DPO by management.

## GDPR

- The GDPR specifies requirements regarding consent, and they are significantly more robust than previous regulations.
- Consent requirements are also delineated for specific circumstances:
  - Informed/affirmative consent to data processing. Specifically, "a statement or a clear affirmative action" from the data subject must be "freely given, specific, informed and unambiguous."
  - Explicit consent to process special categories of data. Explicit consent is required for "special categories" of data, such as genetic data, biometric data, and data concerning sexual orientation.
  - Explicit parental consent for children's personal data.
  - Consent must be specific to each data-processing operation, and the data subject can withdraw consent at any time.

## GDPR

- Under GDPR, personal data is defined as any information relating to an identified or identifiable natural person.
- This includes the following if they are capable of being linked back to the data subject:
  - Online identifiers
  - IP addresses
  - Cookies
- This also includes indirect information, including physical, physiological, genetic, mental, economic, cultural, or social identities that can be traced back to a specific individual.

## GDPR

- GDPR demands that individuals must have full access to information on how their data is processed, and this information should be available in a clear and understandable way.
- When companies obtain data from an individual, some of the issues that must be made clear to the individual whose data is being collected are
  - The identity and contact details of the organization behind the data request (who is asking)
  - The purpose of acquiring the data and how it will be used (why they are asking)
  - The period for which the data will be stored (how long they will keep it)
  - Whether the data will be transferred internationally (where else it can go)
  - The individual's right to access, rectify, or erase the data (right to be forgotten)

## California Consumer Privacy Act 2018

- In June 2018, California passed a sweeping privacy bill that holds many similarities to GDPR.
- Passed in response to the threat of a ballot initiative, AB 375 mandates several key elements.
- While individuals must opt out of sharing, they
  - Have a right to know how personal data is being used
  - Have a right to disclosure and objection relating to who data is being sold to
  - Have a right to know who data has been provided to
  - Experience no discrimination if they object to data being sold
  - Have a right to access the data being held
- The full ramifications of AB 375 are not yet known as the bill only became law in mid-2020 and it may take years to fully understand the implications.
- Privacy laws are going to multiply in the future.

SP 2025

# Other SW Security Related Concepts

## Intellectual Property

- Intellectual property is a legal term that recognizes that creations from the mind can be and are property to which exclusive control can be granted to the creator.
- A variety of different legal mechanisms can be used to protect the exclusive control rights.
- The association of legal mechanism to the property is typically determined by the type of property.
- The common forms of legal protection are patents, copyrights, trademarks, trade secrets, and warranties.

## Patents

- A patent is an exclusive right for inventor granted by a government for a specified period of time.
- Patents are used to protect the inventor's rights in exchange for a disclosure of the invention.
- Patents allow an inventor time to recoup their investment in the creation of an invention. They give their owners the right to prevent others from using a claimed invention, even if the other party claims they independently developed a similar item and there was no copying involved.
- Patent applications are highly specialized legal documents requiring significant resources.
- For patent protection to occur, patents must be applied for prior to disclosure of the invention, with the specifics differing by country.
- Patent law can differ between countries. In the United States,
  - The requirements of an invention is that it represent something new, useful, and nonobvious.
  - It can be a process, a machine, an article of manufacture, or a composition of matter.
  - Patents for software and designs have drawn considerable attention in recent years as to whether the ideas are nonobvious and "new."

## Copyrights

- A copyright is a form of intellectual property protection applied to any expressible form of an idea or information that is substantive and discrete.
- Copyrights gives the creator of an original work exclusive rights to it, usually for a limited time.
- Copyrights apply to a wide range of creative, intellectual, or artistic items. The rights given include the right to be credited for the work, to determine who may adapt the work to other forms, who may perform the work, who may financially benefit from it, and other related rights.
- Copyrights are governed internationally through the Berne Convention, which requires its signatories to recognize the copyright of works of authors from other signatory countries in the same manner as it recognizes the copyright of its own authors.
- For copyright to be enforceable, an application must be made to the copyright office detailing what is being submitted as original work and desiring protection.
- Unlike patents, this filing is relatively straightforward and affordable even by individuals.

## Trademarks

- A trademark is a recognizable quality associated with a product or firm.
- The nature of the trademark is to build a brand association, and hence, copying by others is prohibited.
- Trademarks can be either common law–based or registered. Registering a trademark with the government provides significantly more legal protection and recovery options.
- Internationally, trademarks are managed through the World Intellectual Property Organization, using protocols developed in Madrid, referred to as the Madrid System.
- Names are commonly trademarked to protect a brand image. E.g., Amazon.com is trademarked, as it is used to project the image of the firm.
- Common terms or simply descriptive terms are not eligible for trademark protection.
- Trademark holders must protect their trademarks from general generic use not aligned with their products, as they can lose a trademark that becomes a generic term.

## Trade Secrets

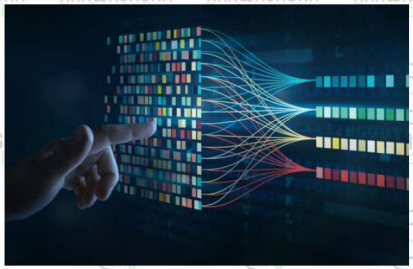
- Trade secrets offer the ultimate in time-based protection for intellectual property.
- A trade secret is just that—a secret. Trade secrets are protected by a variety of laws, with the requirement that a firm keep a secret a secret, or at least make a reasonable attempt to do so.
- The most famous trade secrets typically revolve around food and taste, such as Coca-Cola's recipe or Kentucky Fried Chicken's recipe. Should someone manage to steal the recipes, they could then attempt to sell them to a competitor, but such attempts fail, as no respectable corporation would subject itself to the legal ramifications of attempting to circumvent legal protections for intellectual property.
- One issue with trade secrets is that should someone independently discover the same formula, then the original trade secret holder has no recourse.
- Trade secrets are difficult to use in software, as the distribution of software, even compiled, provides the end user with access to much information.
- There are limited cases where cryptographic algorithms or seeds may be considered trade secrets, as they are not passed to clients and can be protected.
- There is a limited amount of related protection under the reverse-engineering provisions of the U.S. Digital Millennium Copyright Act, where reverse-engineering of security safeguards is prohibited.

## Warranties

- Warranties represent an implied or contractually specified promise that a product will perform as expected.
- When you buy computer hardware, the warranty will specify that for some given period of time the hardware will perform to a level of technical specification and, should it fail to do so, will outline the vendor's responsibilities.
- The warranty typically does not guarantee that the hardware will perform the tasks the user bought it for—merely that it will work at some specified technical level.
- With respect to software, the technical specification, i.e., the program performs as expected, is typically considered by the end user to be fitness for use on the end user's problem.
- This is not what a vendor will guarantee; in fact, most software licenses specifically dismiss this measure, claiming the software is licensed using phrases such as "as-is" and "no warranty as to use" or "no vendor responsibility with respect to any failures resulting from use."

SP 2025

# Data Related Aspects



## Data Classification

- Data can be classified in several different manners, each with a level of significance for security.
- Data can be classified as to its state, its use, or its importance from a security perspective.
- As these are overlapping schemes, it is important to understand all aspects of data classification before determining how data should be handled as part of the development process.
- Data classification is a risk management tool, with the objective to reduce the costs associated with protecting data.
- One of the tenets of security is to match the level of protection and cost of security to the value of the asset under protection.
- Data classification is one of the tools that are used to align protection and asset value in the enterprise.
- Data classification can be simple or fairly complex, depending on the size and scope of the enterprise. A small enterprise may be sufficiently covered with a simple strategy, whereas a large enterprise may have a wide range of data protection needs.
- In large enterprises, it may be desirable to actually determine separate, differing protection needs based on data attributes such as confidentiality, integrity, and availability. These attributes may be expanded to include specific compliance requirements.

## Data States

- Data can be considered a static item that exists in a particular state at any given time.
- For the purposes of development and security, these states are
  - At rest, or being stored
  - Being created
  - Being transmitted from one location to another
  - Being changed or deleted
- In addition, one should consider where the data is currently residing:
  - On permanent media (hard drive, CD/DVD/optical disc)
  - On remote media (USB, cloud/hosted storage)
  - In RAM on a machine
- When considering data states, it is easy to expand this idea to the information lifecycle model (ILM), which includes generation, retention, and disposal.

## Data Usages

- Align the data with how it is used in the business and provide clues as to how it should be shared, if appropriate.
- The classifications include
  - Internal data initialized in the application, used in an internal representation, or computed within the application itself
  - Input data read into a system and possibly stored in an internal representation or used in a computation and stored
  - Output data written to an output destination following processing
- Data can be considered security sensitive, marked as containing personally identifiable information (PII) or to be hidden. These categories include
  - Security-sensitive data A subset of data of high value to an attacker
  - PII data that contains PII elements
  - Hidden data that should be concealed to protect it from unauthorized disclosure using obfuscation techniques

## Data Risk Impact

- Data can be classified as to the specific risk associated with the loss of the data.
- This classification is typically labeled high, medium, and low, although additional caveats of PII or compliance may be added to include elements that have PII or compliance issues if disclosed.
- Data that is labeled high risk is data that if disclosed or lost could result in severe or catastrophic adverse effect on assets, operations, or people.
- The definition of severe will vary from firm to firm in financial terms, as what is severe for a small firm may be of no consequence to a multinational firm.
- Data that is labeled medium risk is data that if disclosed would have serious consequences.
- Low-risk data is data that has limited, if any, consequences if lost or disclosed.
- Each firm, as part of its data management plan, needs to determine the appropriate definitions of severe, serious, and limited, both from a dollar loss point of view and from an operational impact and people impact point of view.

SP 2025

# Data Lifecycle

## Data Lifecycle

- Data in the enterprise has a lifecycle.
- It can be created, used, stored, and even destroyed.
- Although data storage devices have come down in price, the total cost of storing data in a system is still a significant resource issue.
- Data that is stored must also be managed from a backup and business continuity/disaster recovery perspective.
- Managing the data lifecycle is a data owner's responsibility.
- Ensuring the correct sets of data are properly retained is a business function, one that is best defined by the data owner.

## Data Lifecycle - Generation

- Data can be generated in the enterprise in many ways.
- It can be generated in a system as a result of operations, or it can be generated as a function of some input.
- Regardless of the path to generation, data that is generated has to be managed at this point—is it going to be persistent or not?
  - If the data is going to be persistent, then it needs to be classified and have the appropriate protection and destruction policies assigned.
  - If it is not going to be persistent—that is, it is some form of temporary display or calculation—then these steps are not necessary.

## Data Lifecycle - Data Ownership

- Data does not really belong to people in the enterprise; it is actually the property of the enterprise or company itself.
- As the enterprise has limited methods of acting except through the actions of its employees, contractors, and other agents, hence, for practical reasons, data will be assigned to people in a form of an ownership or stewardship role.
- Ownership is a business-driven issue, as factors for ownership responsibilities are business reasons.
- Data Owner
  - Data owners act in the interests of the enterprise when managing certain aspects of data.
  - The data owner is the party who determines who has specific levels of access associated with specific data elements: who can read, who can write, who can change, delete, and so on.
- Data Custodian
  - Data custodians support the business use of the data in the enterprise.
  - They are responsible for ensuring that the processes safely transport, manipulate, and store the data.
  - Data custodians are aware of the data management policies issued by the data owners and are responsible for ensuring that during operations these rules and regulations are followed.

## Data Lifecycle - Data Labeling

- Because data can exist in the enterprise for an extended period of time, it is important to label the data in a manner that can ensure it is properly handled.
- For data in the enterprise, the use of metadata fields (data about the data) can be used to support data labeling.
- The protection of the data can be ensured by providing a label describing the importance of the data.
- Data can have different levels of sensitivity within an organization.
  - Payroll data can be sensitive, with employees having restricted access. But some employees, based on position, may need specific access to this type of data. A manager has a business reason to see and interact with salary and performance data for people under his or her direct management, but not others. HR personnel have business reasons to access data.
- Understanding and properly managing sensitive data can prevent issues.
- The commonsense approach is built around business purpose—if someone has a legitimate business purpose, they should have appropriate access. If not, then they should not have access.
- The challenge is in defining the circumstances and building the procedures and systems to manage data according to sensitivity.

## Data Lifecycle - Data Impact

- The impact that data can have when improperly handled is a much wider concern than sensitivity.
- Virtually all data in the enterprise can, and should, be classified by impact.
- Data can be classified by the impact the organization would suffer in the event of data loss, disclosure, or alteration.
- Impact is a business-driven function, and although highly qualitative in nature, if the levels of high, medium, and low impact are clearly defined, then the application of the impact designation is fairly straightforward:
  - Typically, three levels are used: high, medium (or moderate), and low.
  - Separate levels of impact may be defined by data element for each attribute of CIA.
  - For example, a specific data element could have high impact for confidentiality and high for integrity, but low for availability.

## Data Lifecycle - Data Impact

| Impact | Personnel | Customer | Financial (Specific $ May Vary) |
|---|---|---|---|
| High | Death or maiming | Severe impact to current and future customer relations | Loss of $1 million or more |
| Medium | Severe injury, loss of functionality | Significant impact to current and future customer relations | Loss of $100,000 or more |
| Low | Minor injury | Minor impact to current and future customer relations | Loss of less than $100,000 |

## Data Lifecycle - Data Privacy

- Privacy is the principle of controlling information about one's self: who it is shared with, for what purpose, and how it is used and transferred to other parties.
- Control over one's information is an issue that frequently involves making a choice.
- While it may seem that the answer to many privacy issues is simple anonymization, and with the proper technology it could be done, the practical reality requires a certain level of traceable sharing.
- To obtain certain goods, a user must consent to share their information.
- The issues with privacy then become one of data disposition—what happens to the data after it is used as needed for the immediate transaction.
- If the data is stored for future orders, safeguards are needed.
- In the case of credit card information, regulations such as PCI DSS dictate the requirements for safeguarding such data.

## Data Lifecycle – Privacy Policy

- The privacy policy is the high-level document that describes the principles associated with the collection, storage, use, and transfer of personal information within the scope of business.
- A privacy policy will detail the firm's responsibility to safeguard information.
- A business needs to collect certain amounts of personal information in the course of regular business and has a responsibility to properly secure the information from disclosure to unauthorized parties.
  - A business may have partners with which it needs to share elements of personal information in the course of business.
  - A firm may also choose to share the information with other parties as a revenue stream.
- The privacy policy acts as a guide to the employees as to their responsibilities associated with customer information.
- A customer-facing privacy policy, commonly referred to as privacy disclosure statement, is provided to customers to inform them of how data is protected, used, and disposed of in the course of business.
- In the financial sector, the Gramm-Leach-Bliley Act mandates that firms provide clear and accurate information as to how customer information is shared.

## Data Lifecycle – PII

- Personally Identifiable Information
  - Information that can be used to specifically identify an individual is referred to as personally identifiable information.
  - PII is viewed as a technical term, but it has its roots in legal terms.
  - One of the primary challenges associated with PII is the effect of data aggregation.
  - Obtaining several pieces from different sources, a record can be constructed that permits the identification of a specific individual.
- The U.S. government defines PII using the following from an Office of Management and Budget (OMB) Memorandum:
  - Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

## Data Lifecycle – Common PII Elements

- The following items are commonly used to identify a specific individual and are, hence, considered PII:
  - Full name (if not common)
  - National identification number (i.e., SSN)
  - IP address (in some cases)
  - Home address
  - Motor vehicle registration plate number
  - Driver's license or state ID number
  - Face, fingerprints, or handwriting
  - Credit card and bank account numbers
  - Date of birth
  - Birthplace
  - Genetic information

## Data Lifecycle – PHI

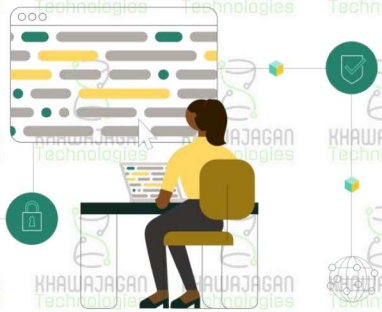
- Personal health information (PHI), also sometimes called protected health information, is the set of data elements associated with an individual's healthcare that can also be used to identify a specific individual.
- These elements can include, but are not limited to, PII elements, demographic data, medical test data, biometric measurements, and medical history information.
- PHI and associated medical data are sought after by cybercriminals because they contain both insurance information and financial responsibility information, including credit cards, both of which can be used in fraud.
- In addition, there is sufficient PII for an identity to be stolen, making health records a highly valued source of information for cybercriminals.
- This data can have significant risk factors to an individual should it fall into the possession of unauthorized personnel.
- For this reason, as well as general privacy concerns, PHI is protected by a series of statutes, including HIPAA and the HITECH Act.

## Data Lifecycle – Breach Notification

- When security fails to secure information and information is lost to parties outside of authorized users, a breach is said to have occurred.
- Data breaches trigger a series of events. First is the internal incident response issue—what happened, how it happened, what systems/data were lost, and other questions that need to be answered.
- In a separate vein, customers whose data was lost deserve to be informed.
- The state of California was the first to address this issue with SB 1386, a data disclosure law that requires
  - A state agency, or a person or business that conducts business in California, that owns or licenses computerized data that includes personal information, as defined, to disclose in specified ways, any breach of the security of the data, as defined, to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

SP 2025

# Privacy Enhancing Technologies (PET)



## Privacy Enhancing Technologies (PET)

- One principal connection between information security and privacy is that without information security, you cannot have privacy.
- If privacy is defined as the ability to control information about oneself, then the aspects of confidentiality, integrity, and availability from information security become critical elements of privacy.
- Just as technology has enabled many privacy-impacting issues, technology also offers the means in many cases to protect privacy.
- An application or tool that assists in such protection is called a privacy-enhancing technology (PET). Major PETs are
  - Encryption
  - Data Minimization
  - Data Masking
  - Tokenization
  - Anonymization / Pseudo-anonymization

## PET - Encryption

- Encryption is at the top of the list of PETs for protecting privacy and anonymity.
- Encryption can keep secrets secret, and it's a prime choice for protecting information at any stage in its lifecycle.
- The development of Tor routing to permit anonymous communications, coupled with high-assurance, low-cost cryptography, has made many web interactions securable and safe from eavesdropping.
- Other PETs include small application programs called cookie cutters that are designed to prevent the transfer of cookies between browsers and web servers.
- Some cookie cutters block all cookies, while others can be configured to selectively block certain cookies.
- Some cookie cutters also block the sending of HTTP headers that might reveal personal information but might not be necessary to access a website, as well as block banner ads, pop-up windows, animated graphics, or other unwanted web elements.
- Some PET tools are designed specifically to look for invisible images that set cookies (web beacons/web bugs).
- Other PETs are available to PC users, including encryption programs that allow users to encrypt and protect their own data, even on USB keys.

## PET - Data Minimization

- Data minimization is one of the most powerful privacy-enhancing technologies involving not keeping what you don't need strategy.
- Limiting the collection of personal information to that which is directly relevant and necessary to accomplish a specified purpose still allows the transactions to be accomplished, but it also reduces risk from future breaches and disclosures by not keeping "excess" data.
- In the EU, privacy rules are built around the idea that individuals own the rights to the reuse of their data, and unless they grant it to a company, the right to store and reuse the data beyond the immediate transaction is prohibited.
- This serves several purposes, but one important outcome is that when a breach/disclosure event occurs, the reach of the PII loss is limited.
- While you may need to have a reasonable amount of PII to process and ship an order, once that process has concluded, do you need the data?
- There may be a need for a reasonable period for returns, warranty claims, and so on, but once that period has passed, destroying unneeded PII removes it from the chance of disclosure.

## PET - Data Masking

- Data masking involves the hiding of data by substituting altered values.
- A mirror version of a database is created, and data modification techniques such as character shuffling, encryption, and word or character substitution are applied to change the data.
- Another form is to physically redact elements by substituting a symbol such as * or x.
- This is seen on credit card receipts, where the majority of the digits are removed in this fashion.
- Data masking makes reverse engineering or detection impossible.

## PET - Tokenization

- Tokenization is the use of a random value to take the place of a data element that has traceable meaning.
- A good example of this is when you have a credit card approval, you do not need to keep a record of the card number, the cardholder's name, or any of the sensitive data concerning the card verification code (CVC) because the transaction agent returns an approval code, which is a unique token to that transaction.
- You can store this approval code, the token, in your system, and if there comes a time you need to reference the original transaction, this token provides you with complete traceability to it and yet, if disclosed to an outside party, reveals nothing.
- Tokens are used all the time in data transmission systems involving commerce because they protect the sensitive information from being reused or shared, yet they maintain the desired nonrepudiation characteristics of the event.
- Tokenization is not an encryption step because encrypted data can be decrypted.
- By substituting a nonrelated random value, tokenization breaks the ability for any outside entity to "reverse" the action because there is no connection.

## PET - Anonymization

- Data anonymization is the process of protecting private or sensitive information by removing identifiers that connect the stored data to an individual.
- Separating the PII elements such as names, Social Security numbers, and addresses from the remaining data through a data anonymization process retains the usefulness of the data but keeps the connection to the source anonymous.
- Data anonymization is easier said than done, because data exists in many places in many forms.
- This permits data aggregators to collect multiple instances and then, through algorithms and pattern match

## PET - Pseudo-anonymization

- Pseudo-anonymization is a de-identification method that replaces private identifiers with fake identifiers or pseudonyms (for example, replacing the value of the name identifier "Mark Sands" with "John Doe").
- Not all uniquely identifying fields are changed because some, such as date of birth, may need to be preserved to maintain statistical accuracy.
- Noise can be added to some fields to remove direct connections, while maintaining the approximate value;
- for example, randomly adding or subtracting three days to/from the actual date of birth preserves the age but de-identifies the original record.
- Pseudonymization preserves statistical accuracy and data integrity, allowing the modified data to be used for training, development, testing, and analytics while protecting data privacy.

KHAWAJAGAN Technologies

SP 2025

# Security In The Design

## Security Modeling

- Even when security and resilience requirements are determined and documented, they often run the risk of being dropped from the backlog or being lost in translation owing to the constraints of time and budget and/or a lack of understanding of their importance by the business or client.
- Product owners and Scrum masters should plan and allow for time and budget to ensure that these constraints are included in the design work.
- "Testing into compliance" is a poor approach for Agile, and a terrible approach if goal is to have secure and resilient applications representing your brand and your reputation.
- The exercise of mapping how users might interact with an application provides a good understanding of the potential for abuse.

## Security Modeling

- If potential abuses (or unsupported uses) are not properly considered, vulnerabilities will exist and can be exploited.
- Use this knowledge you gain to add important information to the acceptance criteria and Definition of Done (DoD).
- For security architects and engineers, these scenarios, along with a detailed model for the application's design, are excellent starting points for developing a threat model.
- In addition, testers can substantially benefit from conducting more robust security tests if they understand all the potential uses of a system.
- Another possibly useful tool is a requirements traceability matrix to assist in tracking the misuse cases to the features of the application.
- This can be performed formally or informally but is helpful in discovering common desirable elements that can be documented as reusable snippets of acceptance criteria across user stories.

## Security Design Architecture / Review

- In most software development projects, time and budget are fixed values, and the introduction of the "extra work" tied to security and resilience requirements are generally not well received by software development teams (at first).
- The best place to introduce the security design and architecture review is when the Scrum team is engaged in the functional design and architecture review of the software.
- When conducting a security review, the assurance requirements of the software should be considered, bearing in mind the cost and time constraints and the need for trade-offs.
- Generating a security plan from the review is a good start for documenting the security design and using it as a check-and-balance guide during and after development. Architecture reviews should be both broad and deep.

SP 2025

# Threat Modeling

## SDAR – Threat Modeling

- Threat modeling is an iterative-structured technique used to identify the threats to the software under design.
- Threat modeling breaks the software into physical and logical constructs generating software artifacts that include data flow diagrams, end-to-end deployment scenarios, documented entry and exit points, protocols, components, identities, and services.
- Attack surface analysis is a subset of threat modeling and can be performed when generating the software context to zero-in on the parts of the software that are exposed to untrusted users. These areas are then analyzed for security issues.
- Once the software context is generated, pertinent threats and vulnerabilities can be identified.
- Threat modeling is performed during design work so that necessary security controls and countermeasures can be defined for the development phase of the software.

## SDAR – Threat Modeling

- OWASP describes the benefits of threat modeling:
  - Builds a secure design
  - Efficient investment of resources; appropriately prioritize security, development, and other tasks
  - Brings security and development together to collaborate on a shared understanding, informing development of the system
  - Identifies threats and compliance requirements and evaluates their risk
  - Defines the need for required controls
  - Balances risks, controls, and usability
  - Identifies where building a control is unnecessary, based on acceptable risk
  - Documents threats and mitigation
  - Ensures that business requirements (or goals) are adequately protected in the face of a malicious actor, accidents, or other causes of impact
  - Identifies specific types of security tests and scenarios to test the application under the acceptance criteria dictates

## SDAR – Threat Modeling

- SANS Institute Cyber Defense offers a handy seven-step recipe for conducting threat modeling and application risk analysis. The recipe is as follows:
  - Step 1: Make a list of what you're trying to protect.
  - Step 2: Draw a diagram and add notes.
  - Step 3: Make a list of your adversaries and what they want.
  - Step 4: Brainstorm threats from these adversaries.
  - Step 5: Estimate probability and potential damage (the overall risk).
  - Step 6: Brainstorm countermeasures and their issues.
  - Step 7: Plan, test, pilot, monitor, troubleshoot and repeat.

## SDAR – TM - STRIDE

- Step 4 of the recipe calls for brainstorming threats from your adversaries.
- One of the more popular brainstorming techniques was popularized by Microsoft and is called STRIDE.
- STRIDE stands for:
  - Spoofing
  - Tampering
  - Repudiation
  - Information disclosure
  - Denial of service
  - Elevation of privilege
- The central idea behind STRIDE is that you can classify all your threats according to one of the six STRIDE categories.
- Because each category has a specific set of potential mitigations, once you have analyzed, categorized, and prioritized threats, you will know how to mitigate or eliminate the defect that could lead to an exploit.

## SDAR – TM - STRIDE

- **Spoofing**
  - A spoofing attack occurs when an attacker pretends to be someone they are not.
  - An attacker using DNS hijacking and pretending to be www.microsoft.com would be an example of a spoofing attack.
- **Tampering**
  - Tampering attacks occur when the attacker modifies data in transit.
  - An attacker that modified a TCP stream by predicting the sequence numbers would be tampering with those data flows.
  - Data stores can be tampered with—that is what happens when the attacker writes specially crafted data into a file to exploit a vulnerability.
- **Repudiation**
  - Repudiation occurs when someone performs an action and then claims that they did not actually perform it.
  - Primarily this shows up on activities such as credit card transactions: a user purchases something and then claims that they did not.
  - Another way that this shows up is in email—if I receive an email from you, you can claim that you never sent it.

## SDAR – TM - STRIDE

- **Information disclosure**
  - Information disclosure threats are usually quite straightforward: can the attacker view data that they are not entitled to view?
  - When you are transferring data from one computer to another over a network, if the attacker can pull the data off the wire, then your component is subject to an information disclosure threat.
  - Data stores are also subject to information disclosure threats: if an unauthorized person can read the contents of the file, it is an information disclosure issue.
- **Denial of service**
  - Denial of service threats occur when an attacker can degrade or deny service to users. If an attacker can crash your component, redirect packets into a black hole, or consume all the CPU on the box, you have a denial of service situation.
- **Elevation of privilege**
  - An elevation of privilege threat occurs when an attacker has the ability to gain privileges that they would not normally have.
  - One of the reasons that classic buffer overflows are so important is that they often allow an attacker to raise their privilege level—for instance, a buffer overflow in any Internet facing component allows an attacker to elevate their privilege level from anonymous to the local user.

## SDAR – TM - STRIDE

- The STRIDE process is really a brainstorming activity conducted in person or via media sharing channels (e.g., WebEx).
- Participants use the documentation to identify assets in the architecture, their purpose, and their relative value to assess if these become the targets for would-be attackers.
- Next, identify possible attackers and what they would want from the system:
  - Who are your actual or likely adversaries?
  - What do they want to achieve?
  - What are their skills and resources?
  - How determined are they?
  - What would they be willing to risk or give up in order to achieve their goals?
  - What about insiders?

## SDAR – TM - DREAD

- The step 5 is about Risk Analysis and Assessment and quoted as "Estimate probability and potential damage (the overall risk)".
- Microsoft another approach known as DREAD will be considered for this step.
- DREAD scores 5 categories which are added together and divided by 5, yielding a result from 0–10, where 0 is for little / no impact and 10 is the house-on-fire situation:
- $Risk\ Outcome = \frac{(DAMAGE\ POTENTIAL + REPRODUCIBILITY + EXPLOITABILITY + AFFECTED\ USERS + DISCOVERABILITY)}{5}$

| Threat Identified: Threat ID nnn — Tampering, Privilege Escalation | | |
|---|---|---|
| Category | Score | Rationale |
| Damage | 6 | Significant disruption |
| Reproducibility | 8 | Code path is easily understood, condition exists in legacy code |
| Exploitability | 2 | Difficult as application is implemented |
| Affected Users | 8 | All cloud computing users |
| Discoverability | 10 | Assumed to be 10 |
| DREAD SCORE: 31/5 = 6.2 – Important — fix as priority | | |

## SDAR – TM – DREAD-Damage Potential

- Damage Potential
  - If the vulnerability is exploited, how much damage will be caused?
    - 0 = Nothing
    - 3 = Individual user data is compromised or affected or availability denied
    - 5 = A subset of data is compromised or affected or availability denied
    - 7 = All data is compromised or affected, or its availability denied
    - 7 = Availability of a specific component/service is denied
    - 8 = Availability of all components is denied
    - 9 = Underlying infrastructure data is compromised or affected
    - 10 = Complete system or data destruction, failure, or compromise

## SDAR – TM – DREAD-Reproducibility

- Reproducibility
  - How reliably can the vulnerability be exploited?
    - 0 = Very hard or impossible, even for administrators. The vulnerability is unstable or statistically unlikely to be reliably exploited.
    - 5 = Some extra steps are required; tooling/scripting readily available.
    - 10 = Unauthenticated users can trivially and reliably exploit using only a Web browser.

## SDAR – TM – DREAD-Exploitability

- Exploitability
  - How difficult is the vulnerability to exploit?
    - 0 = N/A (The assertion here is that every vulnerability is exploitable, given time and effort. All scores should be 1–10.)
    - 1 = Even with direct knowledge of the vulnerability, we do not see a viable path for exploitation.
    - 2 = Advanced techniques are required, bespoke tooling. Only exploitable by authenticated users.
    - 5 = Exploit is available/understood, usable with only moderate skill by authenticated users.
    - 7 = Exploit is available/understood, usable by non-authenticated users.
    - 10 = Trivial—just a web browser.

## SDAR – TM – DREAD-Affected Users

- Affected Users
  - How many users will be affected?
    - 0 = None
    - 5 = Specific to a given project
    - 10 = All users impacted

## SDAR – TM – DREAD-Discoverability

- Discoverability
  - How easy is it to discover the threat, to learn of the vulnerability?
    - 0 = Very hard to impossible to detect even given access to source code and privilege access to running systems.
    - 5 = Can figure it out by guessing or by monitoring network traces.
    - 9 = Details of faults like this are already in the public domain and can be easily discovered using a search engine.
    - 10 = The information is visible in the web browser address bar or in a form.

## SDAR – TM – DREAD-Discoverability

- Discoverability
  - How easy is it to discover the threat, to learn of the vulnerability?
    - 0 = Very hard to impossible to detect even given access to source code and privilege access to running systems.
    - 5 = Can figure it out by guessing or by monitoring network traces.
    - 9 = Details of faults like this are already in the public domain and can be easily discovered using a search engine.
    - 10 = The information is visible in the web browser address bar or in a form.

SP 2025

# Other Risks

## SDAR – Miscellaneous Considerations

- Other risk analysis considerations include:
- Environmental Issues
  - Threats and vulnerabilities that exist in the project's environment or that result from interaction with other systems.
- External / Open Source Code
  - Code that was created by external development groups in either source or object form.
  - It's vitally important to evaluate carefully any code from sources external to your team, including purchased libraries and Open Source components and libraries that may be present.
  - Failing to do so might cause security vulnerabilities the team does not know about or learns about too late.
- Legacy Code
  - Threat models should include all legacy code if the project is a new release of an existing program.
  - Such code could have been written before much was known about software security, and therefore it likely contains vulnerabilities.

## SDAR – Miscellaneous Considerations

- A detailed privacy analysis to document your project's key privacy aspects.
- Important issues to consider include:
  - What personal data is collected?
  - What is the compelling customer value proposition and business justification?
  - What notice and consent experiences are provided?
  - What controls are provided to both internal and external users of the application?
  - How is unauthorized access to personal information prevented?

## SDAR – Defect Removal / Mitigation

- Following are some rules of thumb to use while performing threat modeling.
  - If the data has not crossed a trust boundary, you do not really need to care about it.
  - If the threat requires that the attacker is already running code on the client at your privilege level, you do not really need to care about it.
  - If your code runs with any elevated privileges, you need to be concerned.
  - If your code invalidates assumptions made by other entities, you need to be concerned.
  - If your code listens on the network, you need to be concerned.
  - If your code retrieves information from the Internet, you need to be concerned.
  - If your code deals with data that came from a file, you need to be concerned.
  - If your code is marked as safe for scripting or safe for initialization, you need to be concerned.

## SDAR – Needs for Info Assurance

- It's vital for an application with enough security and resilience controls and constraints that provide the following:
  - Assurance that users and client applications are identified and that their identities are properly verified
  - Assurance that users and client applications can only access data and services for which they have been properly authorized
  - Ability to detect attempted intrusions by unauthorized people and client applications
  - Assurance that unauthorized malicious programs (e.g., viruses) do not infect the application or component
  - Assurance that communications and data are not intentionally corrupted
  - Assurance that parties to interactions with the application or component cannot later repudiate those interactions
  - Assurance that confidential communications and data are kept private
  - Ability for security personnel to audit the status and usage of the security mechanisms
  - Assurance that applications can survive attack or operate in a degraded mode
  - Assurance that system maintenance does not unintentionally disrupt the security mechanisms of the application or any of its components

## SDAR – Needs for Threat Modeling

- Once your threat identification and prioritization steps are completed, you should have the following sets of information available for the next steps of identifying different design choices, countermeasures that should be added, and improvements in the design based on the reviews.
- Completed threat-model documentation should include:
  - A diagram and an enumeration and description of the elements in your diagram.
  - A threat and risk analysis, because that is the core of the threat model.
  - For each mitigated threat that you identify in the threat analysis, you should include the bug or defect number associated with the mitigation plan to add to your backlog of required work.
  - You should also have a one- or two-paragraph description of your software components and what they do. Maintaining a list of key contacts for questions is also useful.
  - Confirm that threat model data and associated documentation (functional/ design specifications) is stored using the document control system used by the development team.
  - You should consider reviews and approvals of threat models and referenced mitigations reviewed by at least one developer, one tester, and one program or project manager.
  - Ask architects, developers, testers, program managers, and others who understand the software to contribute to the threat models and to review them. Solicit broad input and reviews to ensure the threat models are as comprehensive as possible.

## SDAR–OWASP Top10 Proactive Controls

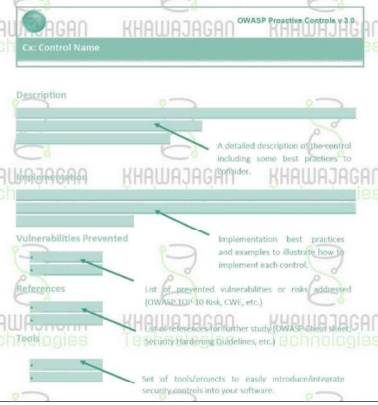
- In 2018, OWASP released the OWASP Top 10 Proactive Controls ordered by importance, with control number 1 being the most important
- They are a set of security techniques that should be included in every software development project.

| | | | |
|---|---|---|---|
| C1 Define Security Requirements | C2 Leverage Security Frameworks and Libraries | C3 Secure Database Access | C4 Encode and Escape Data |
| C5 Validate All Imputs | C6 Implement Digital Identity | C7 Enforce Access Control | C8 Protect Data Everywhere |
| | C9 Implement Security Logging and Monitoring | C10 Handle All Errors and Exceptions | |

## SDAR–OWASP Top10 Proactive Controls

- Structure of OWASP Top 10 Proactive Controls Documentation

(Source: OWASP, Licensed under Creative Commons BY-SA)



# SDAR–OWASP Design Review Checklist

- The OWASP Secure Application Design Project offers an architecture and design review checklist that covers most security and resilience aspects of the architecture and design stages of the SDLC, including the following areas:
  - Authentication
  - Authorization
  - Configuration management
  - Sensitive data
  - Session management
  - Cryptography
  - Parameter manipulation
  - Exception management
  - Auditing and logging

# SDAR–OWASP Design Review Checklist

Checklist for Securing Application Design

| | Category | Vulnerable Area | Facts to ANALYSE |
|---|---|---|---|
| Design | Code Flow – Division of code based on MVC | Presence of backdoor parameters/functions/files | 1. Are there backdoor/unexposed business logic classes? |
| | | | 2. Are there unused configurations related to business logic? |
| | | | 3. If request parameters are used to identify business logic methods, is there a proper mapping of user privileges and methods/actions allowed to them? |
| | | Placement of checks | 1. Are security checks placed before processing inputs? |
| | | Insecure Data Binding Mechanism | 1. Check if unexposed instance variables are present in form objects that get bound to user inputs. If present, check if they have default values. |
| | | | 2. Check if unexposed instance variables present in form objects that get bound to user inputs. If present, check if they get initialized before form binding. |
| | Authentication and Access Control Mechanism | Insecure authentication and access control logic | 1. Is the placement of authentication and authorization check correct? |
| | | | 2. Is there execution stopped/terminated after for invalid request? i.e. when authentication/authorization check fails? |
| | | | 3. Are the checks correct implemented? Is there any backdoor parameter? |
| | | | 4. Is the check applied on all the required files and folder within web root directory? |
| | | Redundant configuration | 1. Is there any default configuration like Access- ALL? |
| | | | 2. Does the configuration get applied to all files and users? |
| | | | 3. Incase of container managed authentication - Is the authentication based on web methods only? |
| | | | 4. Incase of container managed authentication - Does the authentication get applied on all resources? |
| | | Insecure Session management | 1. Does the design handle sessions securely?.... |
| | | Weak Password Handling | 1. Is Password Complexity/Check enforced on the password? |
| | | | 2. Is password stored in an encryptedformat? |
| | | | 3. Is password disclosed to user/written to a file/logs/console? |
| | Data Access Mechanism | Presence of sensitive data in configuration/code files Presence/support for different insecure data sources and their related flaws | 1. Are database credentials stored in an encrypted format? |
| | | | 1. Does the design support weak datastores like flat files |

# SDAR–OWASP Design Review Checklist

| | | | |
|---|---|---|---|
| | Centralized Validation and Interceptors | Weakness in any existing security control | 1. Does the centralized validation get applied to all requests and all the inputs? |
| | | | 2. Does the centralized validation check block all the special characters? |
| | | | 3. Does are there any special kind of request skipped from validation? |
| | | | 4. Does the design maintain any exclusion list for parameters or features from being validated? |
| Architecture | Entry Points | Insecure Data handling and validation | 1. Are all the untrusted inputs validated? |
| | External Integrations | Insecure data transmission | 1. Is the data sent on encrypted channel? Does the application use HTTPClient for making external connections? |
| | | | 2. Does the design involve session sharing between components/modules? Is session validated correctly on both ends? |
| | | Elevated privilege levels | 1. Does the design use any elevated OS/system privileges for external connections/commands? |
| Configuration | External API's used | Known flaws present in 3rd party APIs/functions | 1. Is there any known flaw in API's/Technology used? For eg: DWR |
| | Inbuilt Security Controls | Common Security Controls | 1. Does the design framework provide any inbuilt security control? Like <%, %> in ASP.NET MVC. |
| | | | 2. Are are there any flaw/weakness in the existing inbuilt control? |
| | | | 3. Are all security setting enabled in the design? |

# SDAR–OWASP Design Review Checklist

- Use this checklist to help you conduct architecture and design reviews to evaluate the security of your web applications and to implement the design guidelines.
- This checklist should evolve based on the experience you gain from performing reviews and may need to be extended now and then to accommodate new approaches to application development and operations, including microservices, web services, IoT, and cloud migrations.

KHAWAJAGAN Technologies