Threat Modeling Using STRIDE

By:

Girindro Pringgo Digdo, M.T., CSX-F

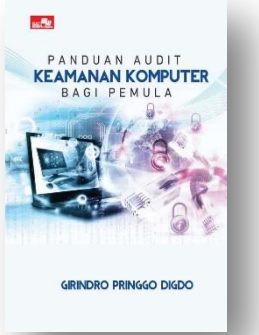
http://www.girindropringgodigdo.net/

girindigdo@gmail.com

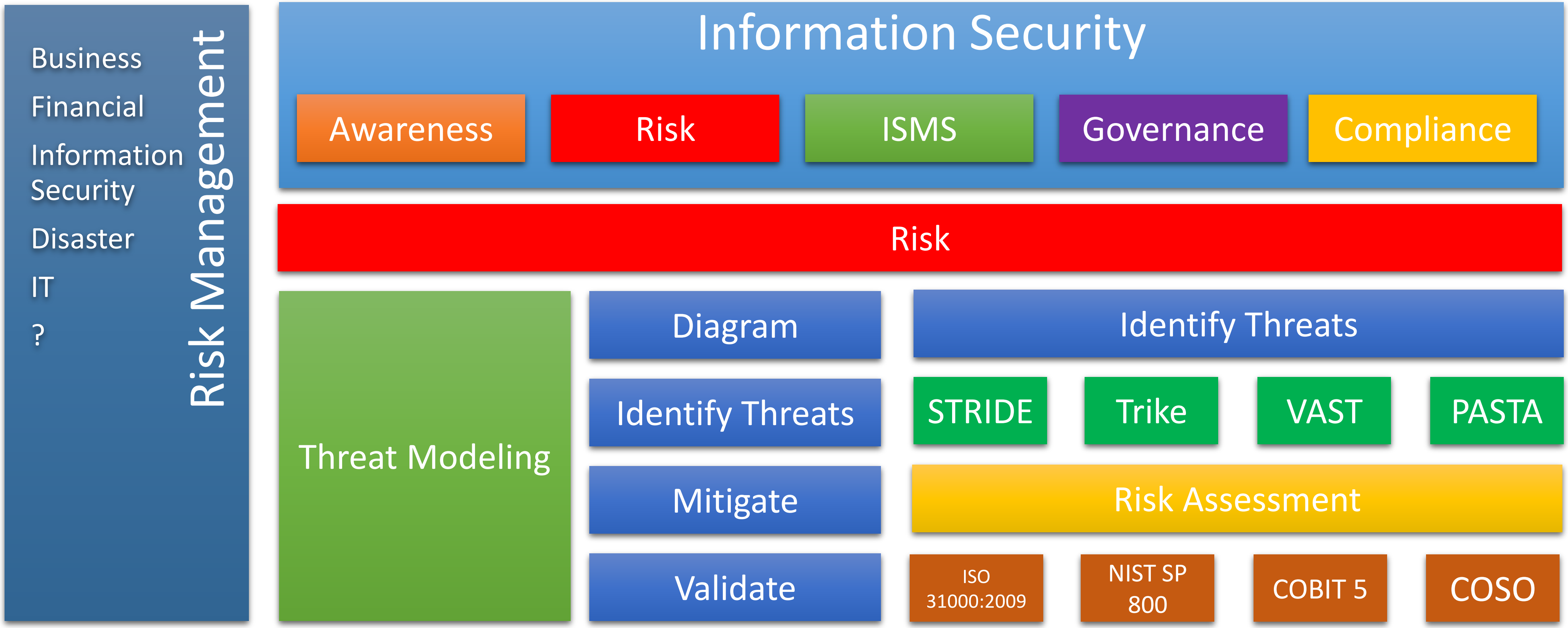
About

- Dealing with Information Security Fields:
  - VAPT
  - Generate New Attack Scenario
  - Information Security Management System
  - Information Security Risk Management
  - Education

- Book Author



Big Picture



Risk Management

Business

Financial

Information Security

Disaster

IT

?

Information Security

Awareness

Risk

ISMS

Governance

Compliance

Risk

Threat Modeling

Diagram

Identify Threats

Mitigate

Validate

Identify Threats

STRIDE

Trike

VAST

PASTA

Risk Assessment

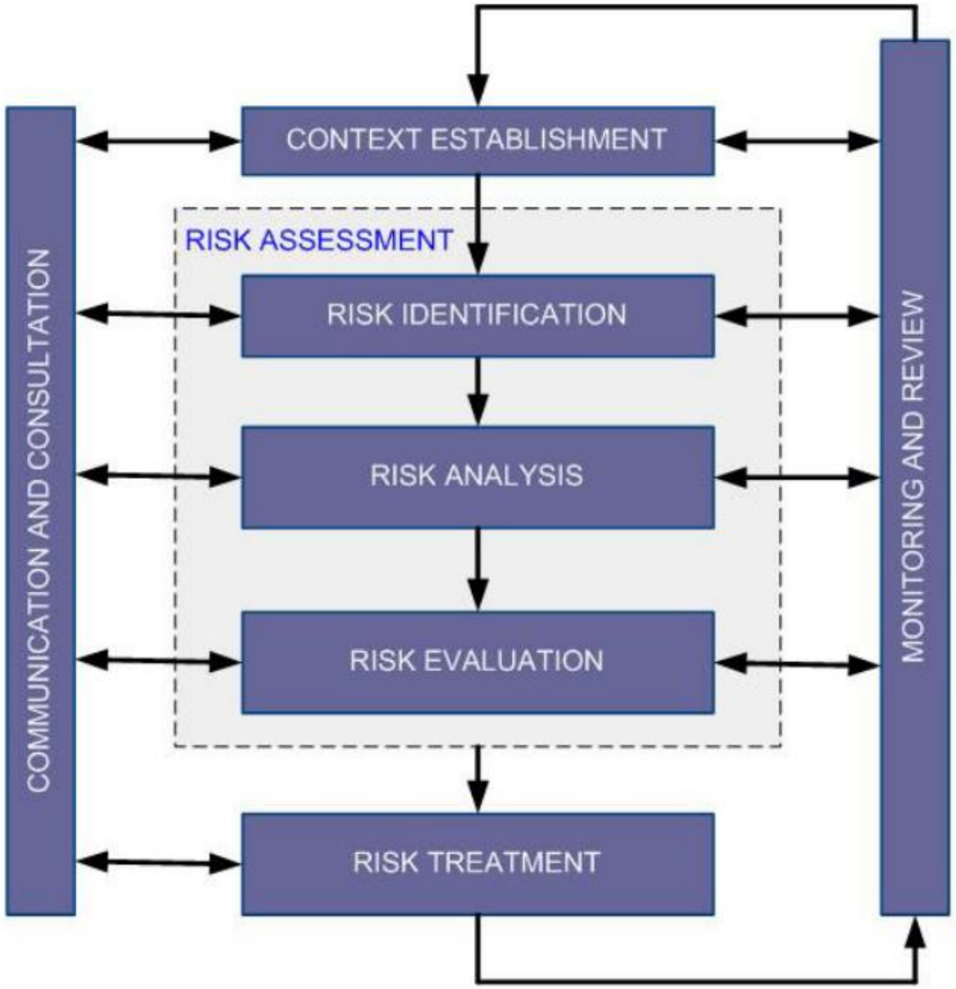
ISO 31000:2009

NIST SP 800

COBIT 5

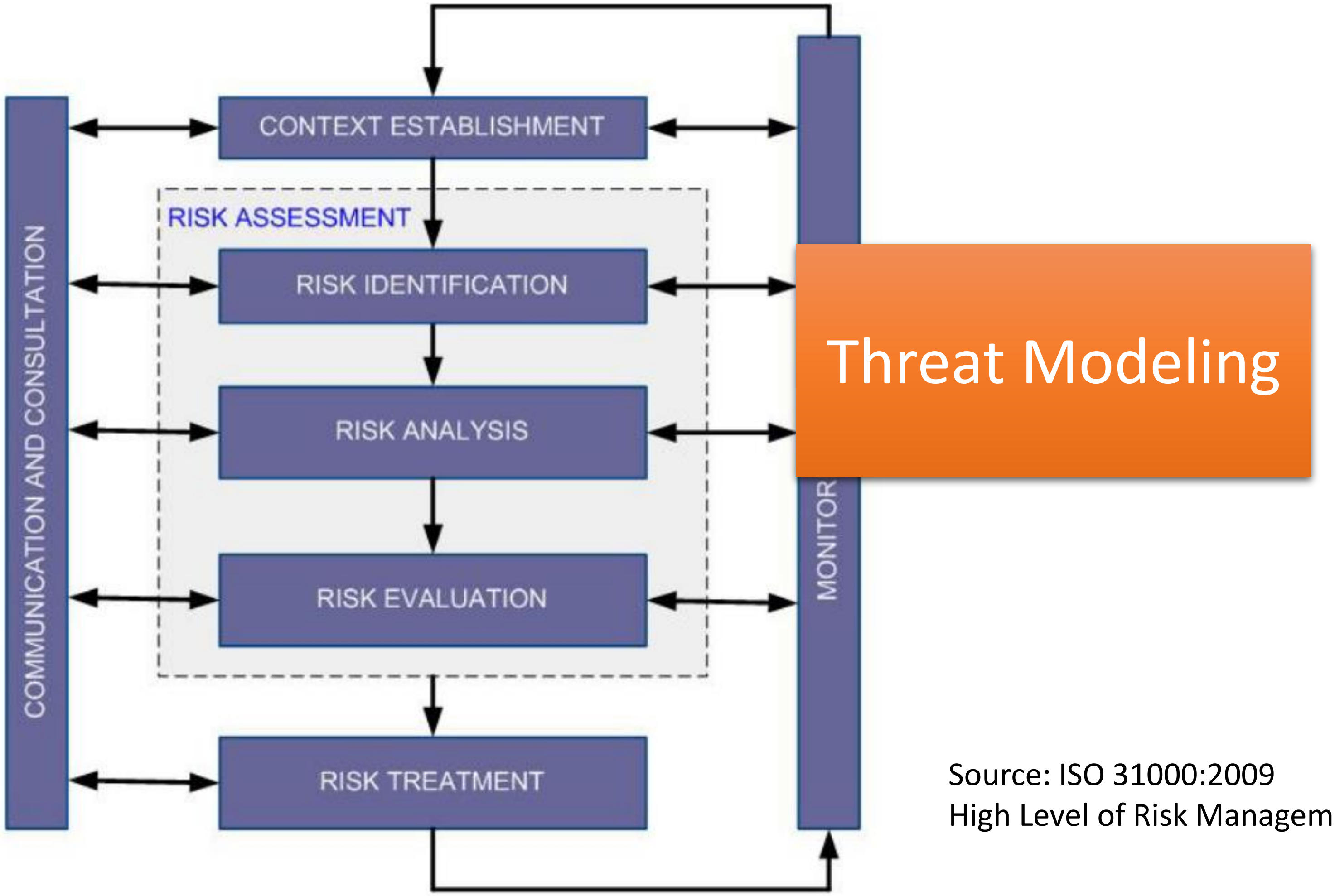
COSO

Information Security Risk Management



Source: ISO 31000:2009
High Level of Risk Management Process

Information Security Risk Management

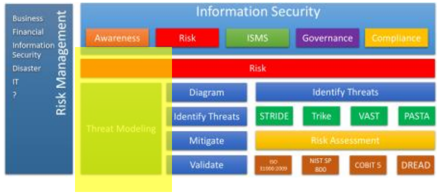


Source: ISO 31000:2009
High Level of Risk Management Process

Risk Management
Business
Financial
Information Security
Disaster
IT
?
Information Security
Awareness
Risk
ISMS
Governance
Compliance
Risk
Threat Modeling
Diagram
Identify Threats
Mitigate
Validate
Identify Threats
STRIDE
Trike
VAST
PASTA
Risk Assessment
ISO 31000:2009
NIST SP 800
COBIT 5
DREAD

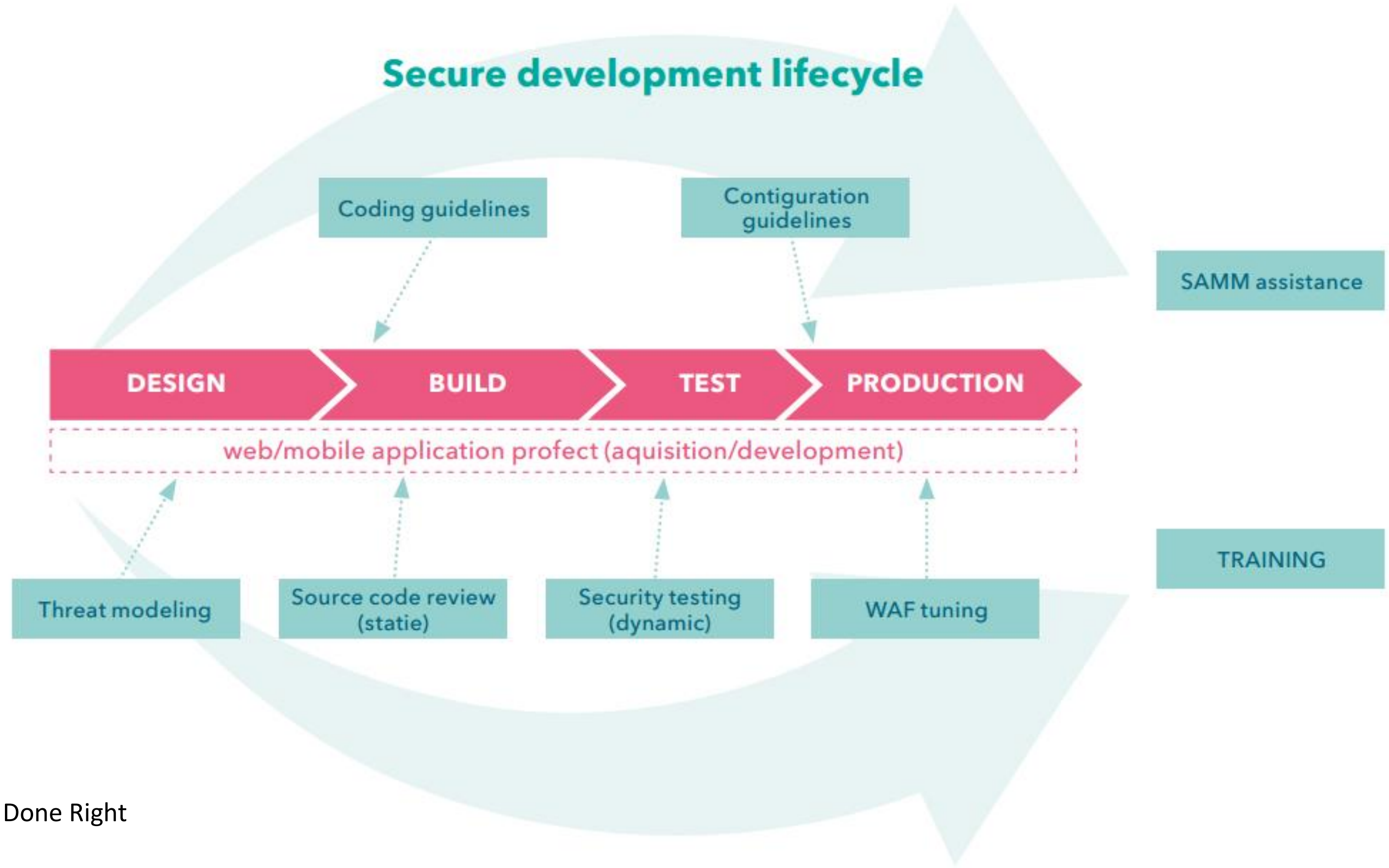
Introduction to Threat Modeling (TM)

- Threat Modeling as a structured activity for identifying and managing the objects (such as application) threats.
- Threat Modeling – also called Architectural Risk Analysis is an essential step in the development of your application.
- Without it, your protection is a shot in the dark



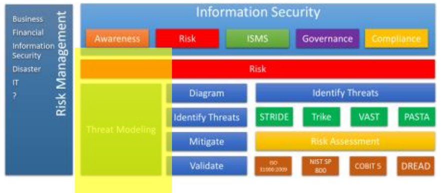
Introduction to Threat Modeling (TM)

Multiple security issues, a timely approach


Secure development lifecycle
Coding guidelines
Contiguration guidelines
SAMM assistance
DESIGN
BUILD
TEST
PRODUCTION
web/mobile application profect (aquisition/development)
Threat modeling
Source code review (statie)
Security testing (dynamic)
WAF tuning
TRAINING

Source: Toreon – Threat Modeling Done Right

Introduction to Threat Modeling (TM)



Risk Management

Business
Financial
Information Security
Disaster
IT
?

Information Security

Awareness
Risk
ISMS
Governance
Compliance

Risk

Threat Modeling

Diagram
Identify Threats
Mitigate
Validate

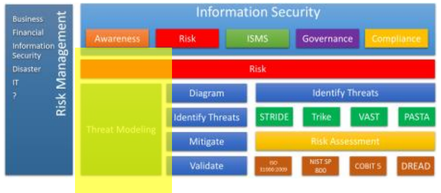
Identify Threats

STRIDE
Trike
VAST
PASTA

Risk Assessment

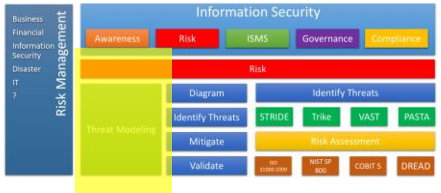
ISO 31000:2009
NIST SP 800
COBIT 5
DREAD

- Threat Modeling is a process by which potential threats can be identified, enumerated, and prioritized.
- The purpose of threat modeling is to provide defenders with a systematic analysis of the probable attacker’s profile, the most likely attack vectors, and the assets most desired by an attacker.
- Threat modeling answers the questions such as:
  - ✓ Diagram
    - What are we building?
    - Where are the high-value assets?
  - ✓ Identify Threats
    - What can go wrong?
    - Where am I most vulnerable to attack?
    - What are the most relevant threats?
  - ✓ Mitigate
    - What are we doing to defend against threats?
  - ✓ Validate
    - Validation of the previous steps and act upon them
    - Is there an attack vector that might go unnoticed?



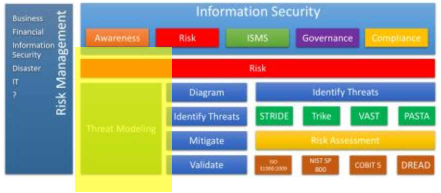
Threat Modeling Basics

- **Who?**
  - The bad guys will do a good job of it
- **What?**
  - A repeatable process to find and address all threats to your product
- **When?**
  - The earlier you start, the more time to plan and fix
- **Why?**
  - Find problems when there’s time to fix them
  - Security Development Lifecycle (SDL) requirement
  - Deliver more secure products
- **How?**



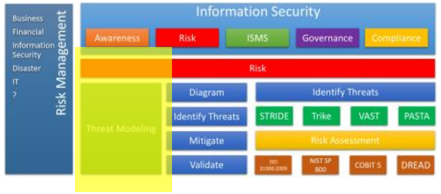
Threat Modeling Basics – Who?

- Building a threat model
  - Program manager (PM) owns overall process
  - Testers
    - Identify threats in analyze phase
    - Use threat models to drive test plans
  - Developers create diagrams
- Customer for threat models
  - Your team
  - Other features, product teams
  - Customers, via use education
  - ‘External’ quality assurance resources, such as pentesters
- You’ll need to decide what fits to your organization



Threat Modeling Basics – What?

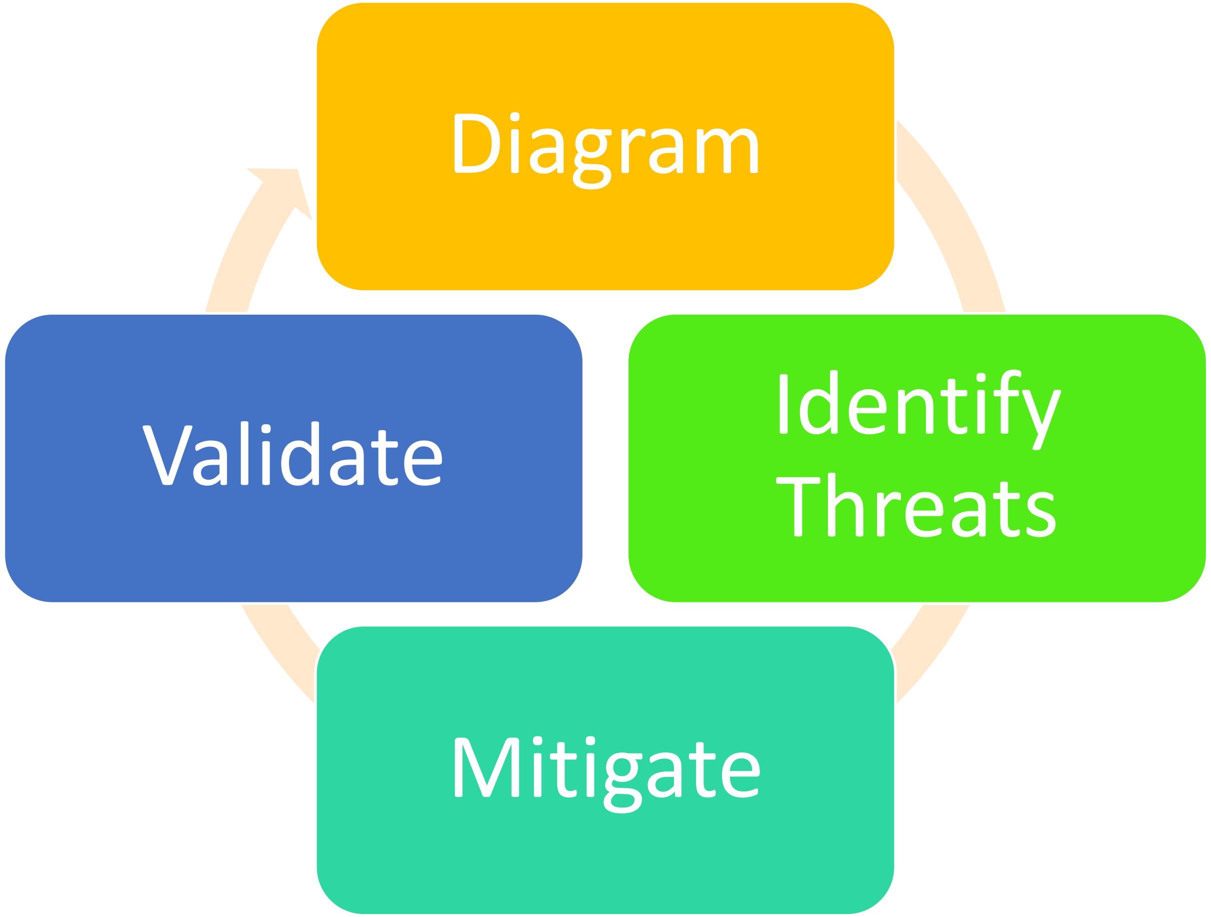
- Consider, document, and discuss security in a structured way
- Threat model and document
  - The product as a whole
  - The security-relevant features
  - The attack surfaces
- Assurance that threat modelling has been done well



Threat Modeling Basics – Why?

- Produce software that’s secure by design – not by incident
  - Improve designs the same way we’ve improved code
- Because attackers think differently
  - Creator blindness / new perspective
- Allow you to predictably and effectively find security problems early in the process

The Process



Diagram

Identify Threats

Mitigate

Validate

Risk Management

Business

Financial

Information Security

Disaster

IT

?

Information Security

Awareness

Risk

ISMS

Governance

Compliance

Risk

Threat Modeling

Diagram

Identify Threats

Mitigate

Validate

Identify Threats

STRIDE

Trike

VAST

PASTA

Risk Assessment

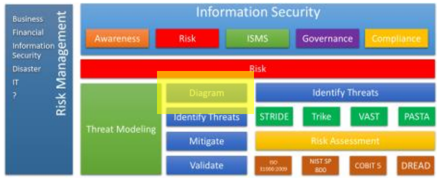
ISO 31000:2009

NIST SP 800

COBIT 5

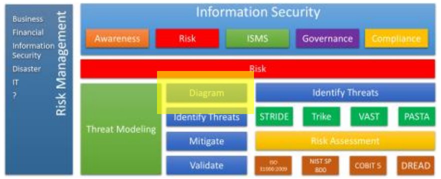
DREAD

Threat Modeling Diagram



How to create diagrams

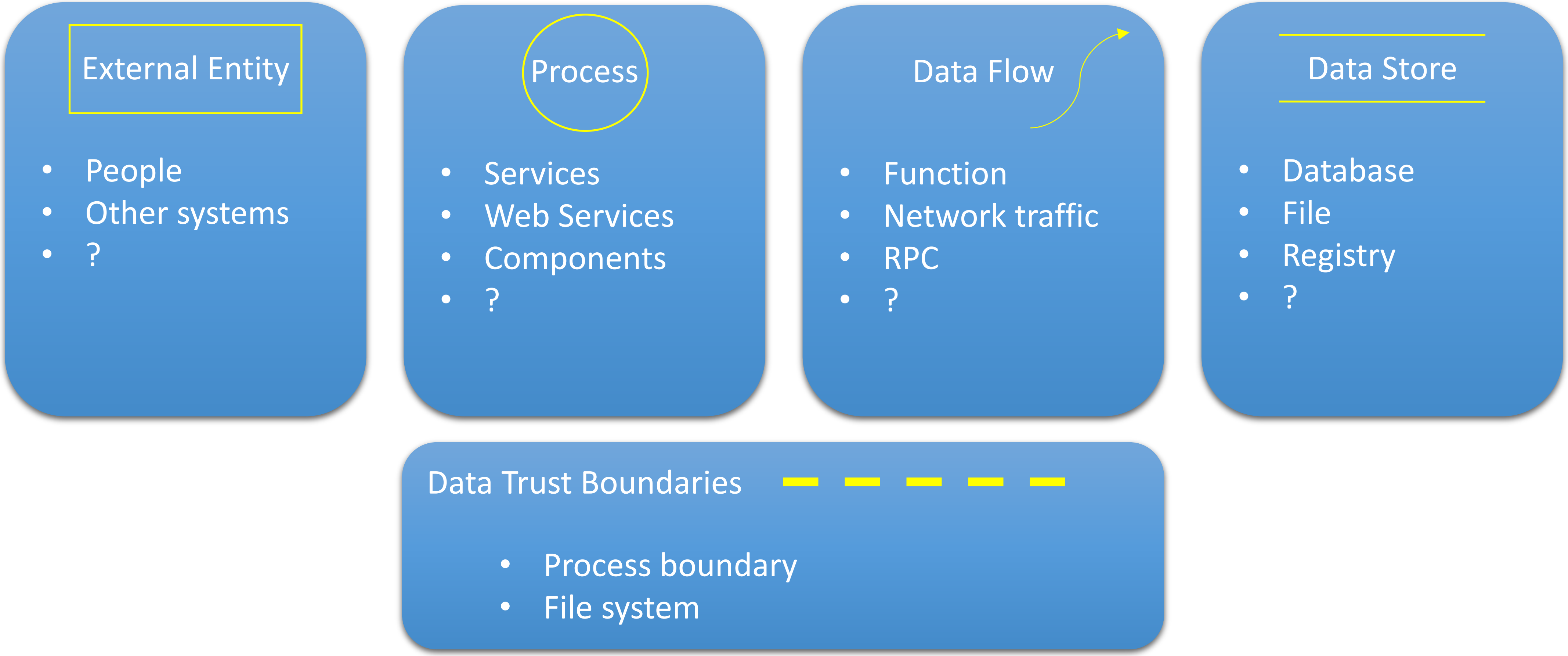
- Go to the whiteboard
- Start with an overview which has:
  - A few external interactors
  - One or two processes
  - One or two data stores (if applicable)
  - Data flows to connect them
- Check your work
  - Can you tell a story without edits?
  - Does it match reality?



Diagramming

- Use DFDs (Data Flow Diagrams)
- Update diagrams as product changes
- Enumerate assumptions, dependencies

Diagram Elements: Examples



External Entity

- People
- Other systems
- ?

Process

- Services
- Web Services
- Components
- ?

Data Flow

- Function
- Network traffic
- RPC
- ?

Data Store

- Database
- File
- Registry
- ?

Data Trust Boundaries

- Process boundary
- File system

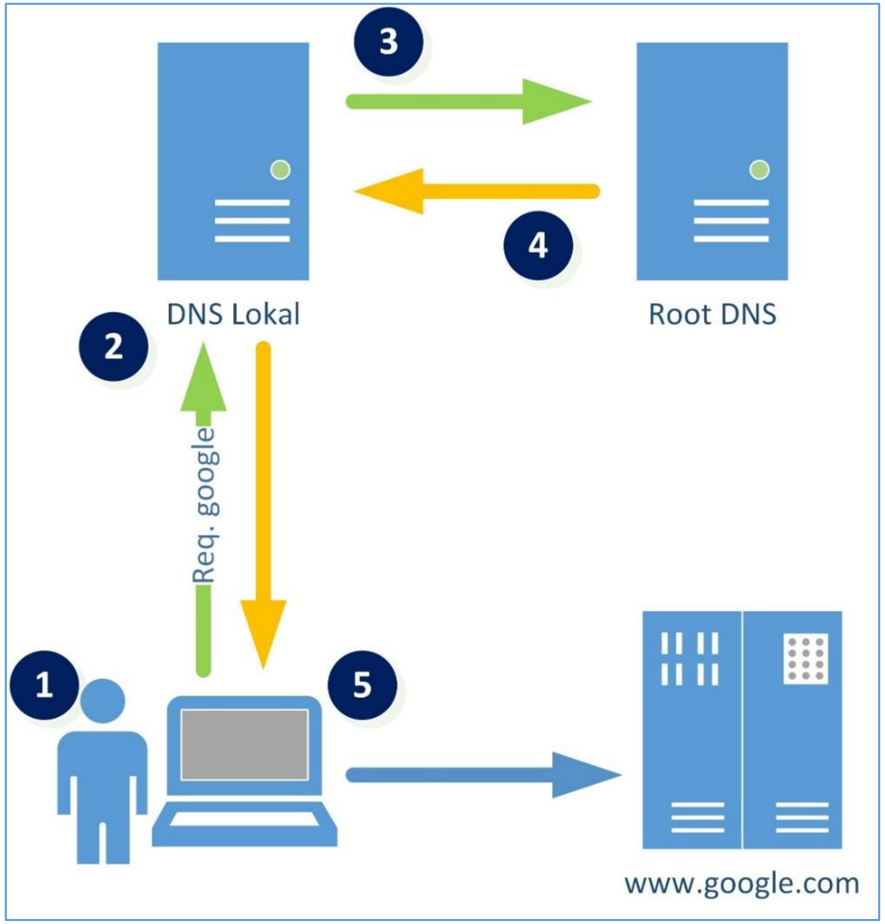
Diagramming: Trust Boundaries

- Add trust boundaries that intersect data flows
- Points where an attacker can interject
  - Machine boundaries, privileges boundaries, integrity boundaries are example of trust boundaries
- Process talking across a network always have a trust boundary
  - They make may create a secure channel, but they’re still distinct entities

Diagramming: Iteration

- Iterate over processes, data stores, and see where they need to be broken down
- How to know it ‘needs to be broken down?’
  - More detail is needed to explain security impact of the design
  - Words like ‘sometimes’ and ‘also’ indicate you have a combination of things that can be broken out
    - ‘sometimes this data store is used for X’ – probably add a second datastore to the diagra,

Context Diagram: Example



Level 1 Diagram: Example

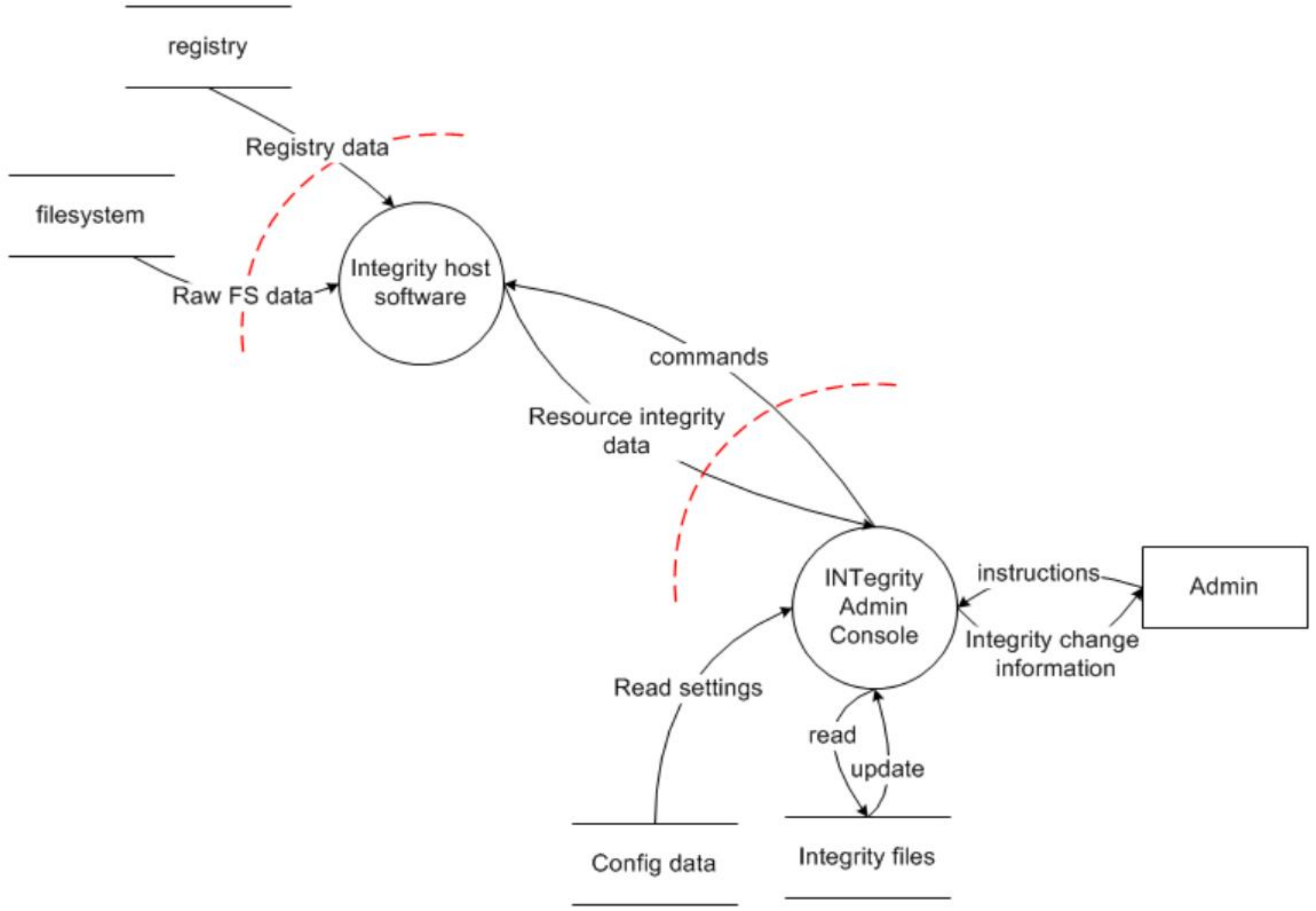


Diagram Layers

- Context Diagram
  - Very high-level; entire component / product / system
- Level 1 Diagram
  - High level; single feature / scenario
- Level 2 Diagram
  - Low level; detailed sub-components of features
- Level 3 Diagram
  - More detailed
  - Rare to need more layers, except in huge projects or when you’re drawing more trust boundaries

The Process: Identify Threats

Business
Financial
Information Security
Disaster
IT
?
Risk Management
Information Security
Awareness
Risk
ISMS
Governance
Compliance
Risk
Threat Modeling
Diagram
Identify Threats
Mitigate
Validate
Identify Threats
STRIDE
Trike
VAST
PASTA
Risk Assessment
ISO 31000:2009
NIST SP 800
COBIT 5
DREAD

Identify Threats

- Experts can brainstorm
- Use STRIDE to step through the diagram elements
- Consider related standards such as ISO 27001 series, NIST SP 800, Cobit 5 Series, OWASP, etc

Risk Management

Business

Financial

Information Security

Disaster

IT

?

Information Security

Awareness

Risk

ISMS

Governance

Compliance

Risk

Threat Modeling

Diagram

Identify Threats

Mitigate

Validate

Identify Threats

STRIDE

Trike

VAST

PASTA

Risk Assessment

ISO 31000:2009

NIST SP 800

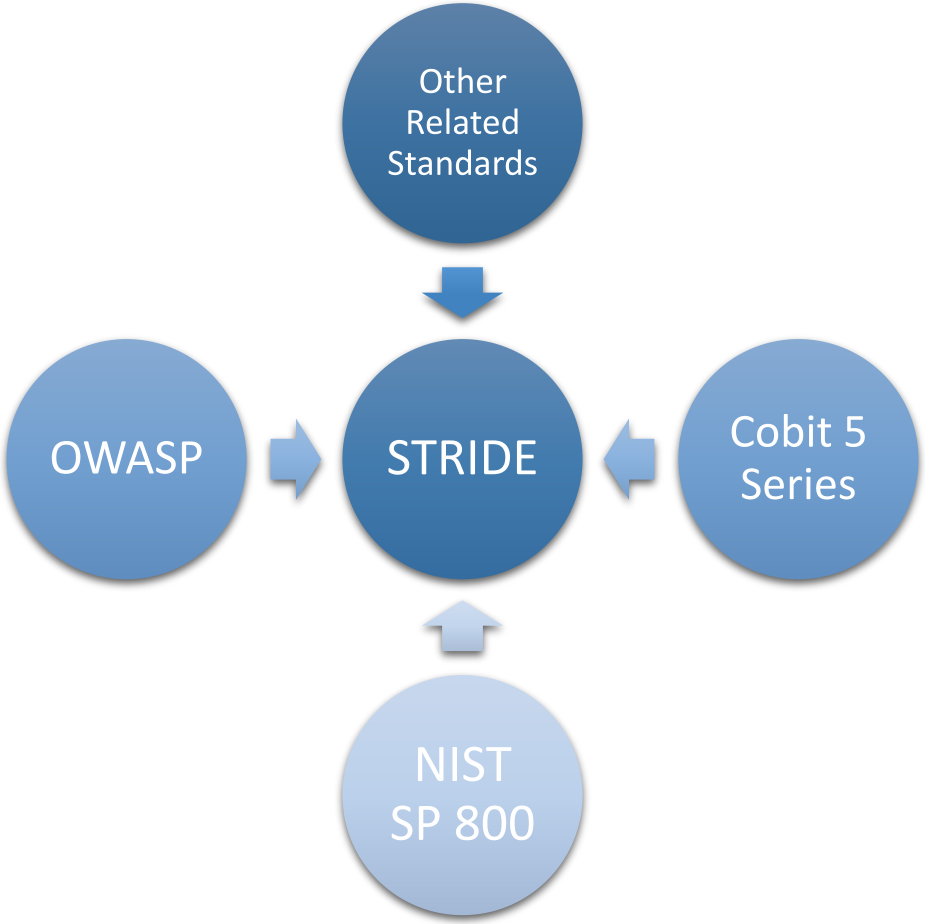
COBIT 5

DREAD

Identify Threats: STRIDE

Threats	Property we want
Spoofing	Authentication
Tampering	Integrity
Repudiation	Nonrepudiation
Information Disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorization

Identify Threats: Considered Inputs



Other Related Standards

OWASP

STRIDE

Cobit 5 Series

NIST SP 800

Threat: Spoofing

Threat	Spoofing
Property	Authentication
Definition	Impersonating something or someone else
Example	Pretending to be any cleaner staff

Threat: Tampering

Threat	Tampering
Property	Integrity
Definition	Modifying data or code
Example	Modifying PHP on disk or a packet as it traverse the LAN

Threat: Repudiation

Threat	Repudiation
Property	Non-repudiation
Definition	Claiming to have not performed in action
Example	“I didn’t send that email,” “I didn’t modify that file”

Threat: Information Disclosure

Threat	Information Disclosure
Property	Confidentiality
Definition	Exposing information to someone not authorized to see it
Example	Allowing someone to read the database, publishing a list of customers to a website

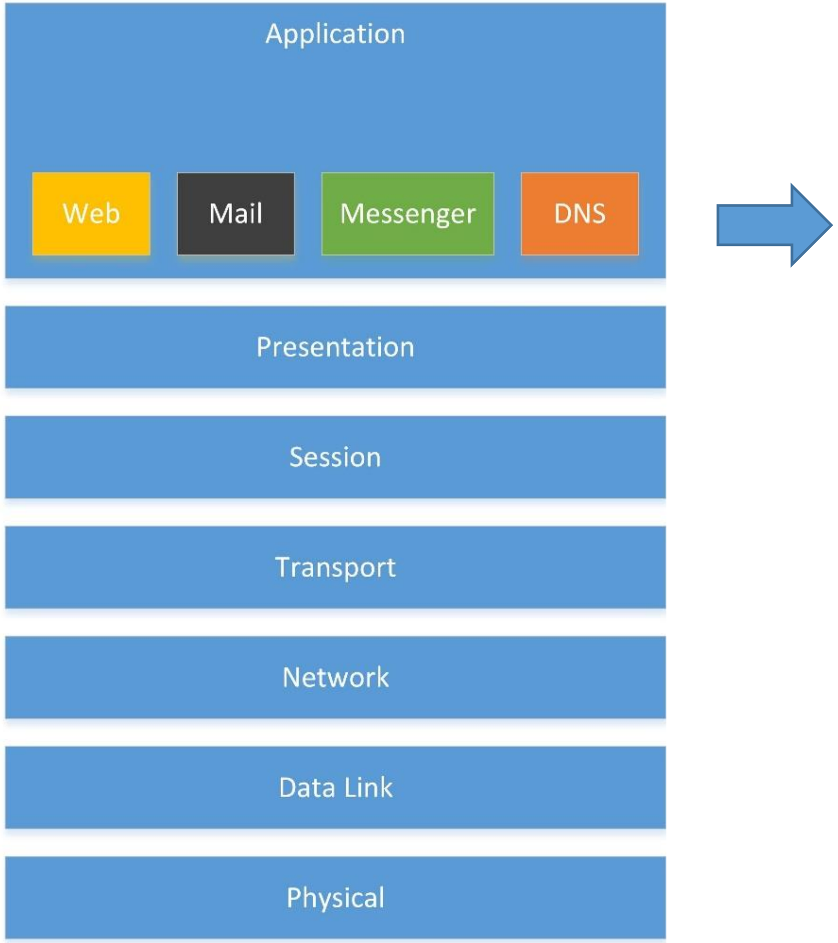
Threat: Denial of Service

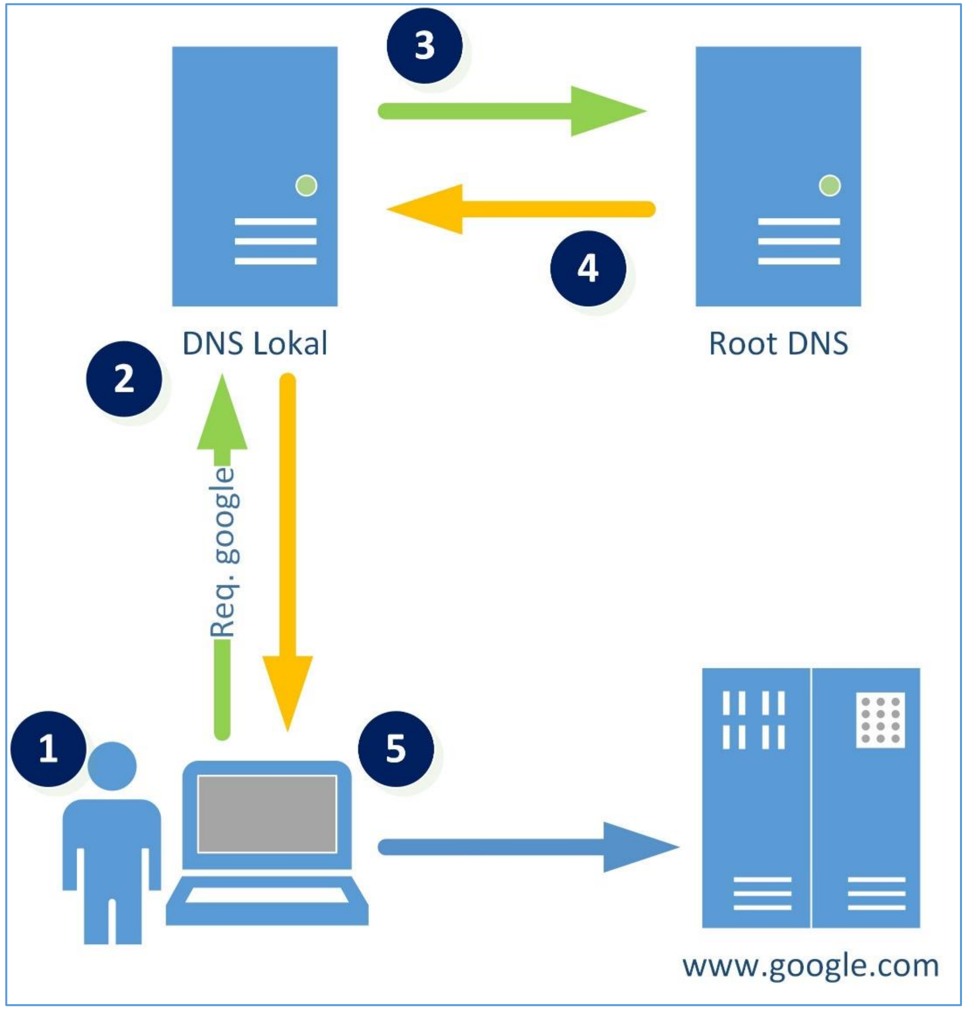
Threat	Denial of Service
Property	Availability
Definition	Deny or degrade or interruption service to users
Example	Crashing OS or website, sending a packet and absorbing seconds of CPU time

Threat: Elevation of Privelege

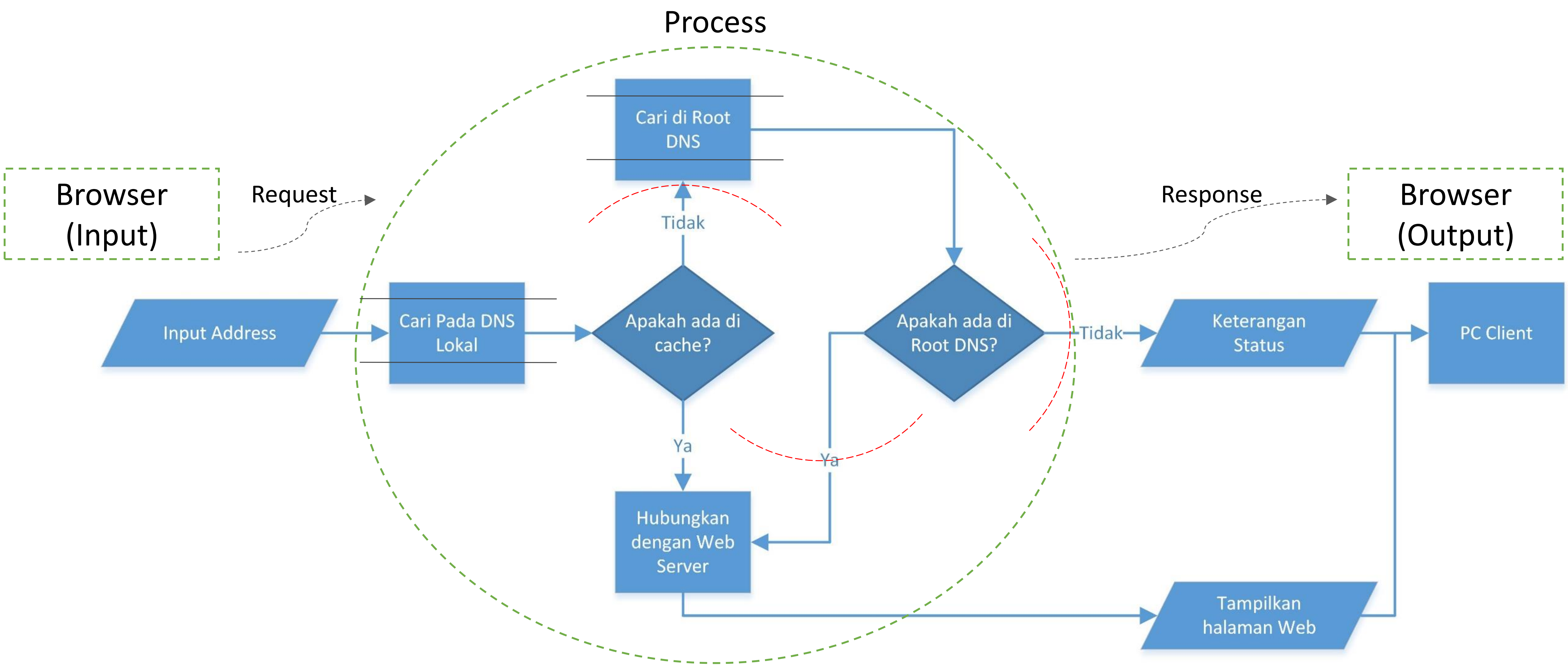
Threat	Elevation of Privilege
Property	Authorization
Definition	Gain capabilities without proper authorization
Example	User with a privilege set of "read only" permissions somehow elevates the set to include "read and write”.

Application Overview: Flow System Identification





Application Overview: Flow System Identification



Identify Threats per Interaction

#	Elements	Interactions	S	T	R	I	D	E
1	Local DNS	Received data from browser		x				
2		Data out to obtain data to database (Root DNS)	x					
3		Received data from database (Root DNS)	x	x			x	x
4		Data flow to browser	x		x	x		
5	Data Flow (request / response)	*Crosses machine boundary*		x		x	x	
6	Database (Root DNS)	Data flow to database		x	x	x	x	
7		Data out from database			x	x	x	
8	Browser	Data flow to Local DNS	x		x	x		
9		Received data from Local DNS	x					

Identify Threats per Interaction

Element: Local DNS	
Interaction: Received data from browser	
Tampering	• Local DNS changed • Data flow source changed

Element: Local DNS	
Interaction: Data out to obtain data to database (Root DNS)	
Spoofing	Database (Root DNS) spoofed and local DNS request to wrong resource.

Identify Threats per Interaction

Risk Management

Business
Financial
Information Security
Disaster
IT
?

Information Security

Awareness
Risk
ISMS
Governance
Compliance

Risk

Threat Modeling

Diagram
Identify Threats
Mitigate
Validate

Identify Threats

STRIDE
Trike
VAST
PASTA

Risk Assessment

ISO 31000:2009
NIST SP 800
COBIT 5
DREAD

Element: Local DNS	
Interaction: Received data from database (Root DNS)	
Spoofing	Database (Root DNS) spoofed and local DNS read from wrong resource
Tampering	Data corrupted when data read from database
Denial of Service (DoS)	Process corrupted by data that received from database
Elevation of Privilege	Process corrupted due wrong data read and caused code execution

Identify Threats per Interaction

Element: Local DNS	
Interaction: Data flow to browser	
Spoofing	Process is confuse toward browser identity
Repudiation	Browser deny toward the given output
Information Disclosure	Browser obtain information disclosure

Identify Threats per Interaction

Element: Data Flow	
Interaction: *Crosses machine boundary*	
Tampering	Data Flow modified by MITM attack
Information Disclosure	Data flow sniffed
Denial of Service	Data flow interrupted by external entity (i.e.: mixed by TCP sequence numbers)

Identify Threats per Interaction

Element: Database (Root DNS)	
Interaction: Data flow to database(Root DNS)	
Tampering	Database corrupted
Repudiation	Local DNS claim not doing the request to Database (Root DNS)
Information Disclosure	Database information disclosure
Denial of Service	Database can’t accessed

Identify Threats per Interaction

Element: Database (Root DNS)	
Interaction: Data out from database	
Repudiation	Local DNS claim can’t read data from Database (Root DNS)
Information Disclosure	Database information disclosure
Denial of Service	Database can’t read

Identify Threats per Interaction

Element: Browser	
Interaction: Data flow to Local DNS	
Spoofing	Process is confuse toward browser identity
Repudiation	Browser deny toward the given output

Element: Browser	
Interaction: Received data from Local DNS	
Spoofing	Process is confuse toward browser identity
Repudiation	Browser deny toward the given output

Identify Threats per Element

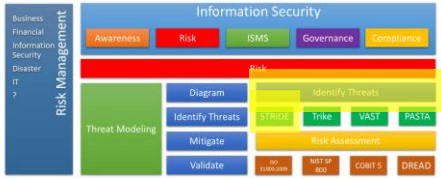
Element	Sub Element	Sub Element Code	Threats	S	T	R	I	D	E
1 DNS Hosting Environment	1.1 Host platform (OS, file system)	1.1.1	Threat 1: The OS, any system software, or any other application software on the DNS host could be vulnerable to attacks such as integrity attack, resulting lost of trust.	X	X		X		
		1.1.2	Threat 2: A malicious insider who has access to local area network (LAN) segments where DNS hosts reside could launch an Address Resolution Protocol (ARP) spoofing attack that disrupts DNS message flows	X			X	X	
		1.1.3	Threat 3: The platform-level configuration file that enables communication (e.g., resolv.conf and host.conf in Unix platforms) can be corrupted by viruses and worms or subject to unauthorized modifications due to inadequate file-level protections, resulting in breakdown of communication among DNS hosts (e.g., between a stub resolver and a resolving name server, between a resolving name server and an authoritative name server).		X			X	
		1.1.4	Threat 4: The DNS-specific configuration files (named.conf, root.hints, etc.), data files (zone file), and files containing cryptographic keys could be corrupted by viruses and worms or subjected to unauthorized modifications due to inadequate file-level protections, resulting in improper functioning of name resolution service		X			X	
		1.1.5	Threat 5: A malicious host on the same LAN as a DNS client may be able to intercept and/or alter DNS responses. This would allow an attacker to redirect a client to a different site. This could be the first action in an attack on a client host.	X	X		X	X	
	1.2 DNS Software (name server, resolver)	1.2.1	Threat 6: DNS software (name server or resolver) could have vulnerabilities such as buffer overflows that result in denial of service.					X	
		1.2.2	Threat 7: DNS software does not provide adequate access control capabilities for its configuration files (e.g., named.conf), its data files (e.g., zone file) and files containing signing keys (e.g., TSIG, DNSKEY) to prevent unauthorized read/update of these files				X	X	X
	1.3 DNS Data (zone file, configuration file)	1.3.1	Threat 8: Lame Delegation: This error occurs when FQDN and/or IP addresses of name servers have been changed in the child zone but the parent zone has not updated the delegation information (NS RRs and glue records). In this situation, the child zone becomes unreachable (denial of service).					X	
		1.3.2	Threat 9: RRs such as HINFO and TXT provide information about software name and versions (e.g., for resources such as Web servers and mail servers) that will enable the well-equipped attacker to exploit the known vulnerabilities in those software versions and launch attacks against those resources.				X		

Identify Threats per Element

Element	Sub Element	Sub Element Code	Threats	S	T	R	I	D	E
2 DNS Transactions	2.1 DNS query/response	2.1.1	Threat 10: Forged or bogus response	X					
		2.1.2	Threat 11: Removal of some RRs from the response		X			X	
	2.2 Zone transfers	2.2.1	Threat 12: Denial of Service: Because zone transfers involve the transfer of entire zones, they place substantial demands on network resources relative to normal DNS queries. Errant or malicious frequent zone transfer requests on the name servers of the enterprise can overload the master zone server and result in denial of service to legitimate users.					X	
		2.2.2	Threat 13: The zone transfer response message could be tampered		X				
	2.3 Dynamic updates	2.3.1	Threat 14: Unauthorized Updates: Unauthorized updates could have several harmful consequences for the content of zone data. Some harmful data operations include: (a) adding illegitimate resources (new FQDN and new RRs to a valid zone file), (b) deleting legitimate resources (entire FQDN or specific RRs), and (c) altering delegation information (NS RRs pointing to child zones)		X	X	X	X	X
		2.3.2	Threat 15: The data in a dynamic update request could be tampered.		X			X	
		2.3.3	Threat 16: Replay Attacks: Update request messages could be captured and resubmitted later, thus causing inappropriate updates.		X			X	

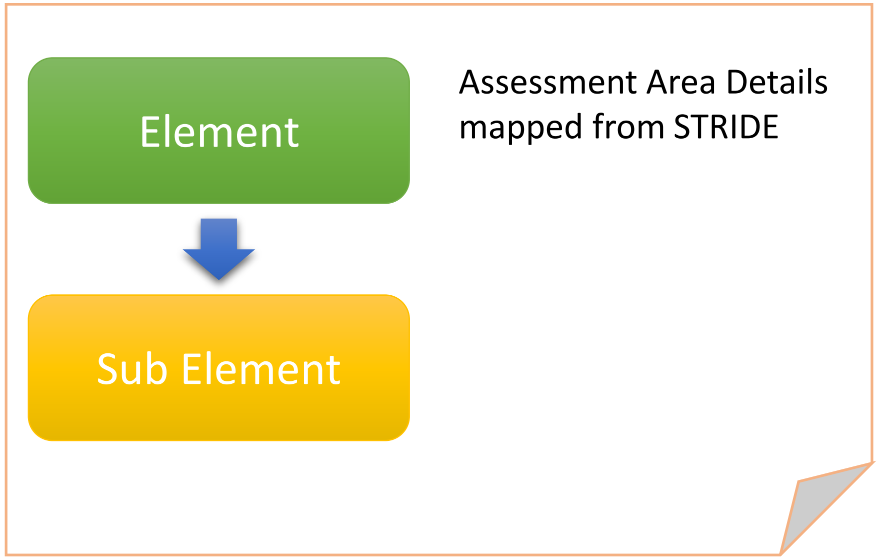
Business
Financial
Information Security
Disaster
IT
?
Risk Management
Information Security
Awareness
Risk
ISMS
Governance
Compliance
Risk
Threat Modeling
Diagram
Identify Threats
Mitigate
Validate
Identify Threats
STRIDE
Trike
VAST
PASTA
Risk Assessment
ISO 31000:2009
NIST SP 800
COBIT 5
DREAD

STRIDE Mapping



Assessment Area Details

AREA	DETAIL AREA	
	ELEMENT	SUB ELEMENT
SPOOFING		
TAMPERING		
REPUDIATION		
INFORMATION DISCLOSURE		
DENIAL OF SERVICE		
ELEVATION OF PRIVILEGE		



Assessment Area Details mapped from STRIDE

Mapped Threats in Assessment Area Details

ASSESSMENT AREA	ASSESSMENT SUB ELEMENT CODE		
SPOOFING	**1.1.1**	**1.1.2**	**1.1.5**
	2.1.1		
	3.1.1		

Mapped Threats in Assessment Area Details

Business
Financial
Information Security
Disaster
IT
?
Risk Management

Information Security
Awareness
Risk
ISMS
Governance
Compliance

Risk

Threat Modeling
Diagram
Identify Threats
Mitigate
Validate

Identify Threats
STRIDE
Trike
VAST
PASTA

Risk Assessment
ISO 31000:2009
NIST SP 800
COBIT 5
DREAD

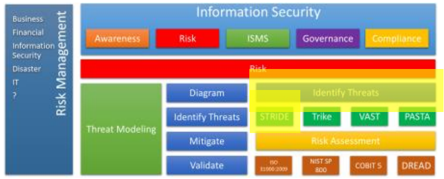
ASSESSMENT AREA	ASSESSMENT SUB ELEMENT CODE			
TAMPERING	1.1.1	1.1.3	1.1.4	1.1.5
	2.1.2			
	2.2.2			
	2.3.1	2.3.2	2.3.3	
	3.1.6			

Mapped Threats in Assessment Area Details

ASSESSMENT AREA	ASSESSMENT SUB ELEMENT CODE
REPUDIATION	**2.3.1**

Mapped Threats in Assessment Area Details

ASSESSMENT AREA	ASSESSMENT SUB ELEMENT CODE						
INFORMATION DISCLOSURE	1.1.1	1.1.2	1.1.5				
	1.2.2						
	1.3.2						
	2.3.1						
	3.1.1	3.1.2	3.1.3	3.1.4	3.1.5	3.1.6	3.1.7

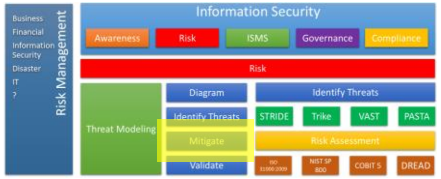


Mapped Threats in Assessment Area Details

ASSESSMENT AREA	ASSESSMENT SUB ELEMENT CODE				
DENIAL OF SERVICE	**1.1.1**	**1.1.2**	**1.1.3**	**1.1.4**	**1.1.5**
	1.2.1	**1.2.2**			
	1.3.1				
	2.1.2				
	2.2.1				
	2.3.1	**2.3.2**	**2.3.3**		

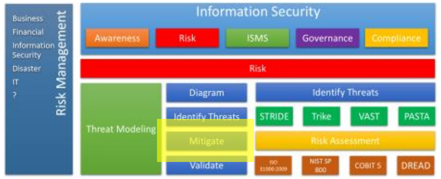
Mapped Threats in Assessment Area Details

ASSESSMENT AREA	ASSESSMENT SUB ELEMENT CODE
ELEVATION OF PRIVILEGE	**1.2.2**
	2.3.1
	3.1.6

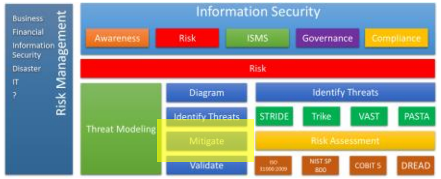


The Process: Mitigation

Mitigation is the point of Threat Modeling

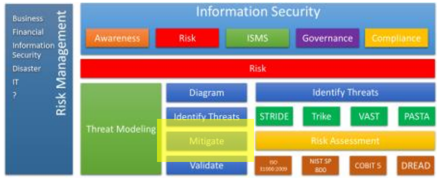


- Mitigation
  - To address or alleviate a problem
- Protect customers
- Design secure software
- Why bother if you:
  - Create a great model
  - Identify lots of threats
- So, find problems and fix them



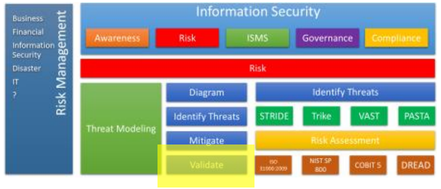
Mitigate

- Address each threat
- Ways to address threats:
  - Redesign to eliminate
  - Apply standard mitigations
  - Invent new mitigations (riskier)
  - Accept vulnerability in design
    - SDL rules about what you can accept

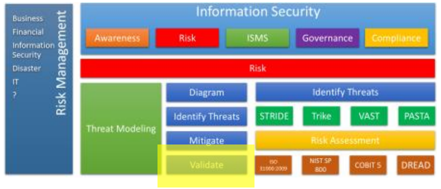


Standard Mitigations

Spoofing	Authentication	To authenticate principals: • Cookie Authentication • PKI systems such as SSL/TLS and certificates To authenticate code or data: • Digital Signatures
Tampering	Integrity	• Integrity Controls • ACLs • Digital Signatures
Repudiation	Nonrepudiation	• Secure logging and auditing • Digital Signatures
Information Disclosure	Confidentiality	• Encryption • ACLs
Denial of Service	Availability	• ACLs • Filtering • Quotas
Elevation of Privilege	Authorization	• ACLs • Group or role membership • Privilege ownership • Input Validation



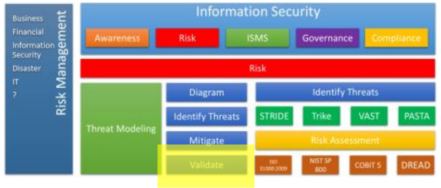
The Process: Validation



Validating Threats Models

- Validate the whole threat model
  - Does diagram match final code?
  - Are threats enumerated?
  - Has Test / QA reviewed the model?
  - Is each threat mitigated?
  - Are mitigations done right?
- Did you check these before Final Security Review?

Validate Quality of Threats and Mitigations



Business
Financial
Information Security
Disaster
IT
?
Risk Management

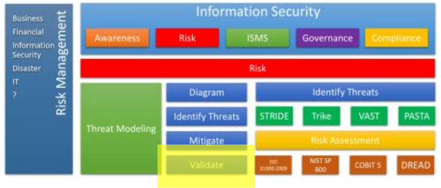
Information Security
Awareness
Risk
ISMS
Governance
Compliance

Risk

Threat Modeling
Diagram
Identify Threats
Mitigate
Validate

Identify Threats
STRIDE
Trike
VAST
PASTA
Risk Assessment
ISO 31000:2009
NIST SP 800
COBIT 5
DREAD

- Threats: Do They:
  - Describe the attack
  - Describe the context
  - Describe the impact
- Mitigations
  - Associate with threat
  - Describe mitigations



Risk Management

Business

Financial

Information Security

Disaster

IT

?

Information Security

Awareness

Risk

ISMS

Governance

Compliance

Risk

Threat Modeling

Diagram

Identify Threats

Mitigate

Validate

Identify Threats

STRIDE

Trike

VAST

PASTA

Risk Assessment

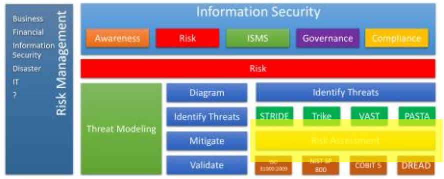
ISO 31000:2009

NIST SP 800

COBIT 5

DREAD

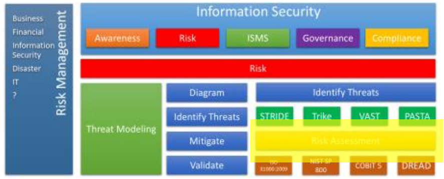
Overview: Risk Assessment



Risk Assessment

- “An approach to identifying and managing systemic risk for an organization and system”
- Enterprise Security Risk Assessments are performed to allow organizations to:
  - assess, identify and modify their overall security posture
  - and to enable security, operations, organizational management and other personnel to collaborate and view the entire organization from an attacker’s perspective.

Risk Assessment



Risk Management

Business

Financial

Information Security

Disaster

IT

?

Information Security

Awareness

Risk

ISMS

Governance

Compliance

Risk

Threat Modeling

Diagram

Identify Threats

Mitigate

Validate

Identify Threats

STRIDE

Trike

VAST

PASTA

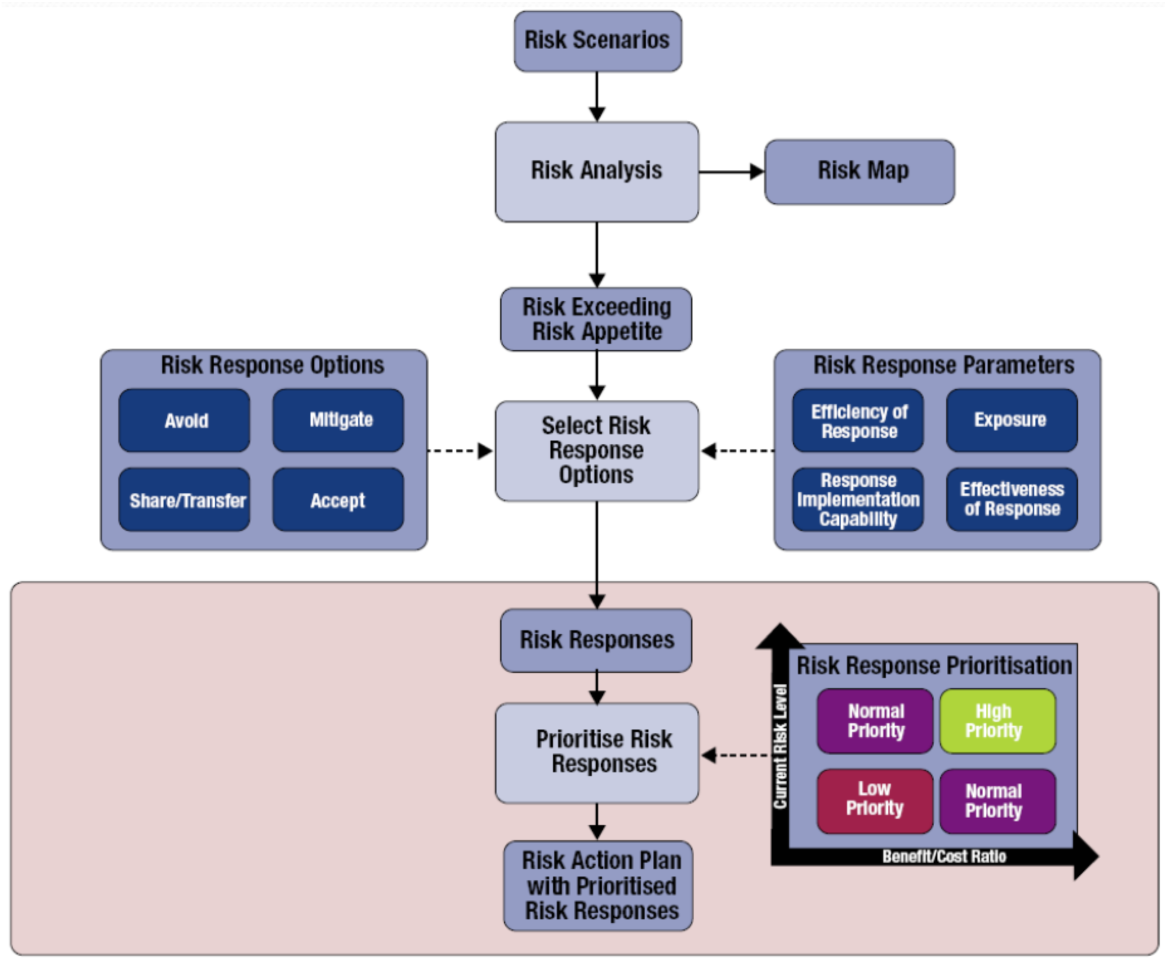
Risk Assessment

ISO 31000:2009

NIST SP 800

COBIT 5

DREAD



Risk Scenarios

Risk Analysis

Risk Map

Risk Exceeding Risk Appetite

Risk Response Options

Avoid

Mitigate

Share/Transfer

Accept

Select Risk Response Options

Risk Response Parameters

Efficiency of Response

Exposure

Response Implementation Capability

Effectiveness of Response

Risk Responses

Prioritise Risk Responses

Risk Action Plan with Prioritised Risk Responses

Risk Response Prioritisation

Current Risk Level

Normal Priority

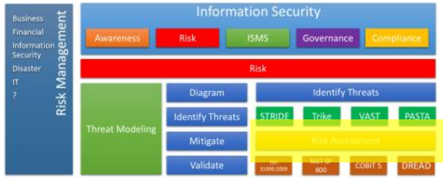
High Priority

Low Priority

Normal Priority

Benefit/Cost Ratio

Source:
Cobit 5 for Risk



Business
Financial
Information Security
Disaster
IT
?
Risk Management

Information Security
Awareness
Risk
ISMS
Governance
Compliance

Risk

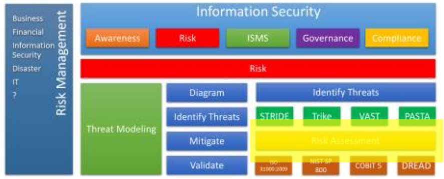
Threat Modeling
Diagram
Identify Threats
Mitigate
Validate

Identify Threats
STRIDE
Trike
VAST
PASTA
Risk Assessment
ISO 31000:2009
NIST SP 800
COBIT 5
DREAD

Risk Assessment: Risk Rating

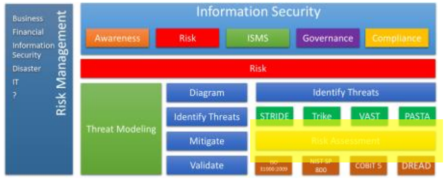
- Low / Very Low, the possibility of attacks and the impact if a successful attack is relatively low. Ratings for this category:
  - Very Low: < 1.5, Low: >= 1.5 &< 2.5
- Medium, the possibility of attacks and the impact if successful attacks are relatively moderate / medium. Ratings for this category:
  - Medium >=2.5 &< 3.5.
- High / Very High, the possibility of attacks and the impact if a successful attack is relatively high. Ratings for this category:
  - High: >= 3.5 &< 4.5, Very High : >= 4.5

Risk Assessment: Risk Level



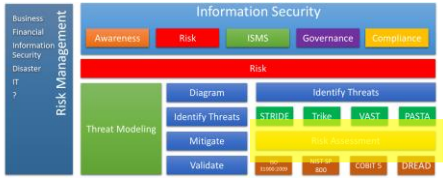
Risk Levels = (Impact + Possibility) / 2

- **Possibility** (P), the possibility of an attack is determined from a combination of factors such as:
  - the attacker motivation, opportunity and resources;
  - information security policies and procedures and the consistency of existing implementations;
  - network or system architecture and configuration details.
  - The highest value of the possibility (P) = 5 and the lowest value = 1
- **Impact** (I), impact is determined based on the risk to the organization, either directly or indirectly.
  - The highest value of the impact (D) = 5 and the lowest score = 1

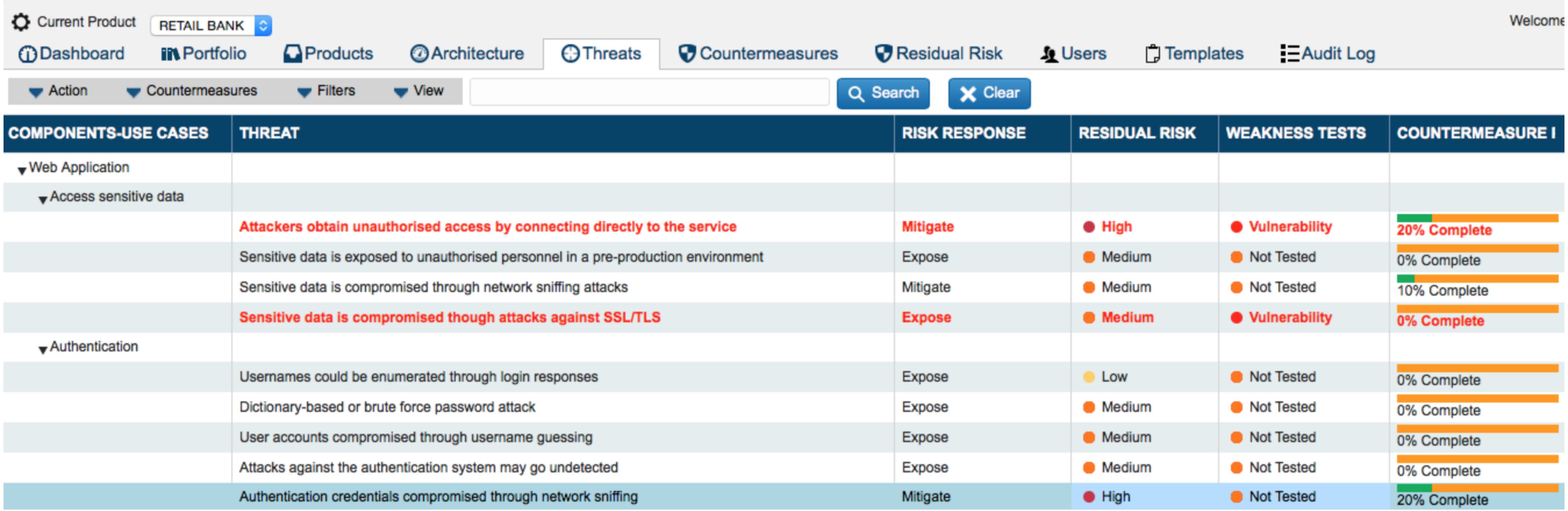


Risk Assessment: Sample Risk Summary

#	RISK				DETAILS	
	LEVEL	R	I	P	THREATS	MITIGATIONS
1	High	4	4	4	**System Vulnerable** The OS, any system software, or any other application software on the DNS host could be vulnerable to attacks such as integrity attack, resulting lost of trust.	Ensure that the system or software keep always updated and patched.



Sample of Threat Modeling Tools



COMPONENTS-USE CASES	THREAT	RISK RESPONSE	RESIDUAL RISK	WEAKNESS TESTS	COUNTERMEASURE I
▾Web Application					
▾Access sensitive data					
	Attackers obtain unauthorised access by connecting directly to the service	**Mitigate**	● **High**	● **Vulnerability**	**20% Complete**
	Sensitive data is exposed to unauthorised personnel in a pre-production environment	Expose	● Medium	● Not Tested	0% Complete
	Sensitive data is compromised through network sniffing attacks	Mitigate	● Medium	● Not Tested	10% Complete
	Sensitive data is compromised though attacks against SSL/TLS	**Expose**	● **Medium**	● **Vulnerability**	**0% Complete**
▾Authentication					
	Usernames could be enumerated through login responses	Expose	● Low	● Not Tested	0% Complete
	Dictionary-based or brute force password attack	Expose	● Medium	● Not Tested	0% Complete
	User accounts compromised through username guessing	Expose	● Medium	● Not Tested	0% Complete
	Attacks against the authentication system may go undetected	Expose	● Medium	● Not Tested	0% Complete
	Authentication credentials compromised through network sniffing	Mitigate	● High	● Not Tested	20% Complete

References

- Adam Shostack “Threat Modeling Designing for Security”
- Cobit 5 for Risk
- ISACA Journal 2010 Volume 1
- ISO 31000:2009
- Microsoft “Introduction to Microsoft Security Development Lifecycle (SDL) Threat Modeling”
- Toreon “Threat Modeling Done Right”

Thank You