

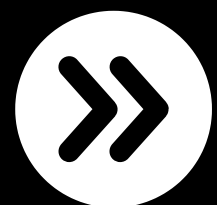
Corentin Ducottet

All



process steps

Let's Swipe Right



Quantitative Risk analysis

- 1** Single Loss Expectancy = Asset Value
x Exposure Factor
- 2** Annual Loss Expectancy = Single
Loss Expectancy x Annual Rate of
Occurrence
- 3** Value of safeguard = ALE
presafeguard - ALE postsafeguard -
Annual Cost of Safeguard

Let's Swipe Right



Risk Maturity Model

- 1** Ad hoc
- 2** Preliminary
- 3** Defined
- 4** Integrated
- 5** Optimized

Let's Swipe Right



NIST Risk Management Framework



Memo tech: People Can See I Am Always Monitoring

- | | |
|---------------------|--------------------|
| 1 Prepare | 5 Assess |
| 2 Categorize | 6 Authorize |
| 3 Select | 7 Monitor |
| 4 Implement | |

Let's Swipe Right



Business Continuity Planning

- 1** Project Scope & Planning
- 2** Business Impact Analysis
- 3** Continuity planning
- 4** Plan approval & implementation

Let's Swipe Right



Business Impact Analysis

- 1** Identify Priorities, Business Units & Data gathering techniques
- 2** Risk Identification (Asset Value)
- 3** Likelihood Assessment (ARO)
- 4** Impact Assessment (SLE & ALE)
- 5** Resources Prioritization

Let's Swipe Right



Data classification process (1/2)

- 1** Criterias are set for classifying data
- 2** Data owners are established for each type of data
- 3** Data is classified
- 4** Required controls are selected for each classification

Let's Swipe Right



Data classification process (2/2)

- 5** Baseline security standards are selected for the organization
- 6** Controls are scoped and tailored
- 7** Controls are applied and enforced
- 8** Access is granted and managed

Let's Swipe Right



Data classification for Public companies

- 1** Public
- 2** Sensitive
- 3** Private
- 4** Confidential

Let's Swipe Right



Data classification for Government

- 1 Unclassified
- 2 Confidential
- 3 Secret
- 4 Top Secret

Let's Swipe Right



Digital signature

- 1 Sender hash plaintext
- 2 Sender encrypts hash with its private key
- 3 Sender adds encrypted hash to plaintext (signature)
- 4 Receiver decrypts the encrypted hash with sender's public key
- 5 Receiver generates a hash of the plaintext using the same function as the sender
- 6 Receiver compares if the two hashes are similar

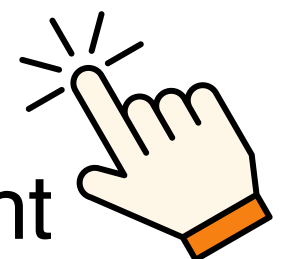
Let's Swipe Right



Public Key Infrastructure

- 1 Sender obtains the recipient's certificate
- 2 Sender verifies the authenticity of the certificate by using the Certificate Authority's public key to validate the digital signature contained in the certificate
- 3 Sender reach out to Certificate Revocation List to check if certificate is still valid
- 4 Sender encrypts and sends message using the recipient's public key contained in the certificate

Let's Swipe Right



Common Criteria

- 1** Functionality Tested
- 2** Structurally Tested
- 3** Methodically tested and checked
- 4** Methodically designed, tested and reviewed
- 5** Semi-formally designed and tested
- 6** Semi-formally verified design and tested
- 7** Formally verified design and tested

Let's Swipe Right



Perimeter Protection

- 1** Deter
- 2** Deny
- 3** Detect
- 4** Delay
- 5** Determine
- 6** Decide

Let's Swipe Right



OSI layers



Memo tech: Please Do Not
Throw Sausage Pizza Away



- 1** Physical
- 2** Data Link
- 3** Network
- 4** Transport
- 5** Session
- 6** Presentation
- 7** Application

Let's Swipe Right



TCP/IP Layers

- 1** Network access
- 2** Internet
- 3** Transport
- 4** Application

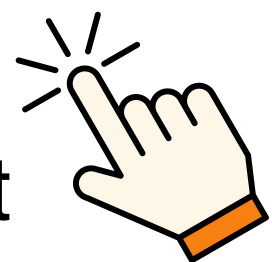
Let's Swipe Right



Keberos Authentication

- 1** The user types a username and password into the client.
- 2** The client encrypts the username with AES for transmission to the KDC.
- 3** The KDC verifies the username against a database of known credentials.
- 4** The KDC generates a symmetric key that will be used by the client and the Kerberos server. It encrypts this with a hash of the user's password.
The KDC also generates an encrypted timestamped TGT.
- 5** The KDC then transmits the encrypted symmetric key and the encrypted timestamped TGT to the client.
- 6** The client installs the TGT for use until it expires. The client also decrypts the symmetric key using a hash of the user's password.

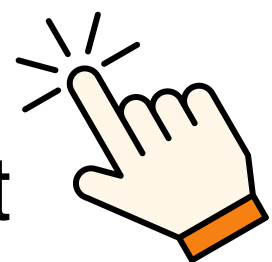
Let's Swipe Right



Kerberos Object Access

- 1** The client sends its TGT back to the KDC with a request for access to the resource.
- 2** The KDC verifies that the TGT is valid and checks its access control matrix to verify that the user has sufficient privileges to access the requested resource.
- 3** The KDC generates a service ticket and sends it to the client.
- 4** The client sends the ticket to the server or service hosting the resource.
- 5** The server or service hosting the resource verifies the validity of the ticket with the KDC.
- 6** Once identity and authorization are verified, Kerberos activity is complete. The server or service host then opens a session with the client and begins communications or data transmission.

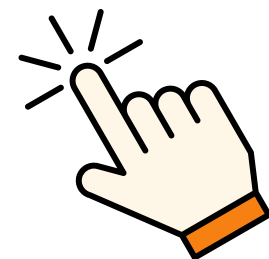
Let's Swipe Right



Pentest phases

- 1** Planning
- 2** Information gathering & discovery
- 3** Attack
- 4** Reporting

Let's Swipe Right





Incident management

Memo tech: DRMRRL



- 1** Detection
- 2** Response
- 3** Mitigation
- 4** Reporting
- 5** Recovery
- 6** Remediation
- 7** Lesson Learned

Let's Swipe Right



Kill Chain

- 1** Reconnaissance
- 2** Weaponization
- 3** Delivery
- 4** Exploitation
- 5** Installation
- 6** Command & control
- 7** Actions & objectives

Let's Swipe Right



Change management

- 1** Request the change
- 2** Review the change
- 3** Approve/reject the change
- 4** Test the change
- 5** Schedule and implement the change
- 6** Document the change

Let's Swipe Right



Patch Management

- 1** Evaluate
- 2** Test
- 3** Approve
- 4** Deploy
- 5** Verify

Let's Swipe Right



Disaster Recovery Planning

- 1** Prioritizing business units (use BIA)
- 2** Crisis management
- 3** Emergency communications
- 4** Workgroup recovery (cold sites, warm sites or hot sites)

Let's Swipe Right



Electronic Discovery (1/2)

- 1** Information governance
- 2** Identification
- 3** Preservation
- 4** Collection
- 5** Processing

Let's Swipe Right



Electronic Discovery (2/2)

- 6** Review
- 7** Analysis
- 8** Production
- 9** Presentation

Let's Swipe Right



ISC2 Code of Ethics

- 1** Protect society, the common good, necessary public trust and confidence, and the infrastructure
- 2** Act honorably, honestly, justly, responsibly, and legally
- 3** Provide diligent and competent service to principals
- 4** Advance and protect the profession

Let's Swipe Right



Software Development Life Cycle

- 1** Requirement Gathering
- 2** Design
- 3** Development
- 4** Test
- 5** Deployment
- 6** Operation & Maintenance

Let's Swipe Right



System Development Life Cycle



Same steps as Software
Development Lifecycle +
Retirement/ Disposal

5

Let's Swipe Right



Information System Lifecycle (1/2)

- 1** Stakeholders needs and requirements
- 2** Requirements analysis
- 3** Architectural design
- 4** Development/ Implement
- 5** Integration

Let's Swipe Right



Information System Lifecycle (2/2)

- 6** Verification & validation
- 7** Transition/ Deployment
- 8** Operations & maintenance/
sustainment
- 9** Retirement/ Disposal

Let's Swipe Right



Capability Maturity Model

- 1** Initial
- 2** Repeatable
- 3** Defined
- 4** Managed
- 5** Optimized

Let's Swipe Right



Capability Maturity Model Integrated

- 1** Initial
- 2** Managed
- 3** Defined
- 4** Quantitatively Managed
- 5** Optimized

Let's Swipe Right



IDEAL Model

- 1** Initiating
- 2** Diagnosing
- 3** Establishing
- 4** Acting
- 5** Learning

Let's Swipe Right



Software Assurance Maturity Model (1/2)

- 1** Governance (Strategy & Metrics, Policy & Compliance, Education & Guidance)
- 2** Design (Threat Assessment, Security Requirement, Secure Architecture)
- 3** Implementation (Secure Build/Deployment, Defect Management)

Let's Swipe Right



Software Assurance Maturity Model (2/2)

- 4** Verification (Architecture Analysis/
Requirement-driven/ Security
Testing)
- 5** Operations (Incident /Environment/
Operational Management)

Let's Swipe Right



Corentin Ducottet

All CISSP Process Steps

Change management (Software)

1 Request Control

2 Change Control

3 Release Control

Let's Swipe Right



Software configuration management

- 1** Configuration Identification
- 2** Configuration Control
- 3** Configuration Status Accounting
- 4** Configuration Audit

Let's Swipe Right



ACID Model

- 1 Atomicity
- 2 Consistency
- 3 Isolation
- 4 Durability

Let's Swipe Right



Corentin Ducottet

All CISSP Process Steps

**Follow me for
more content to
help you in your
CISSP journey !**

Save  & Share  if these tips
helped you !

Corentin Ducottet

