CHESS

Cyber-security Excellence Hub in Estonia and South Moravia

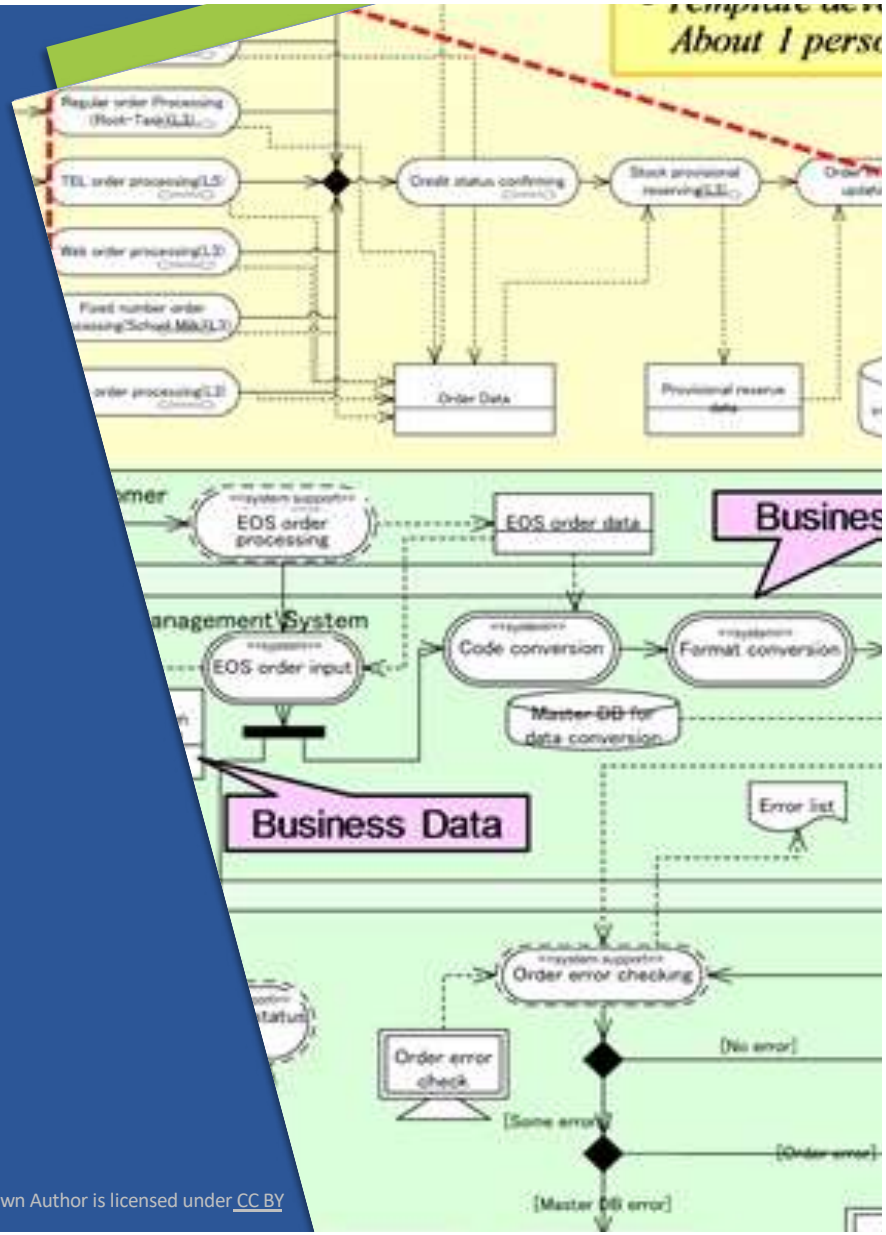
From Risk to Evidence: Cybersecurity Management and Forensic Readiness

Lukáš Daubner and **Raimundas Matulevičius**

Information Security Research Group
Institute of Computer Science
University of Tartu

Why is the Business Process Model useful?

- *System-oriented thinking*
- *Design solution*
- *Baseline for prototyping/ implementation*

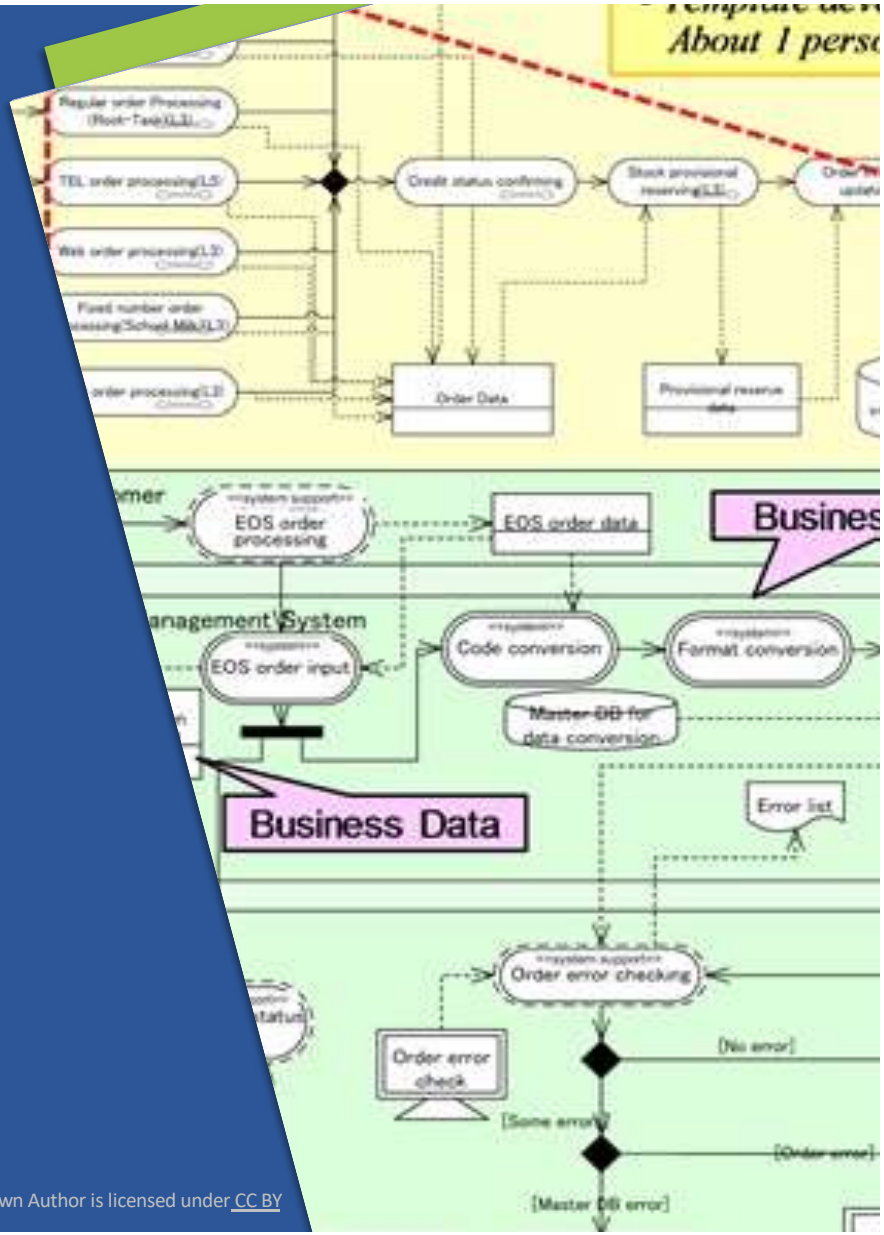


This Photo by Unknown Author is licensed under CC BY

How is the Business Process Model created?

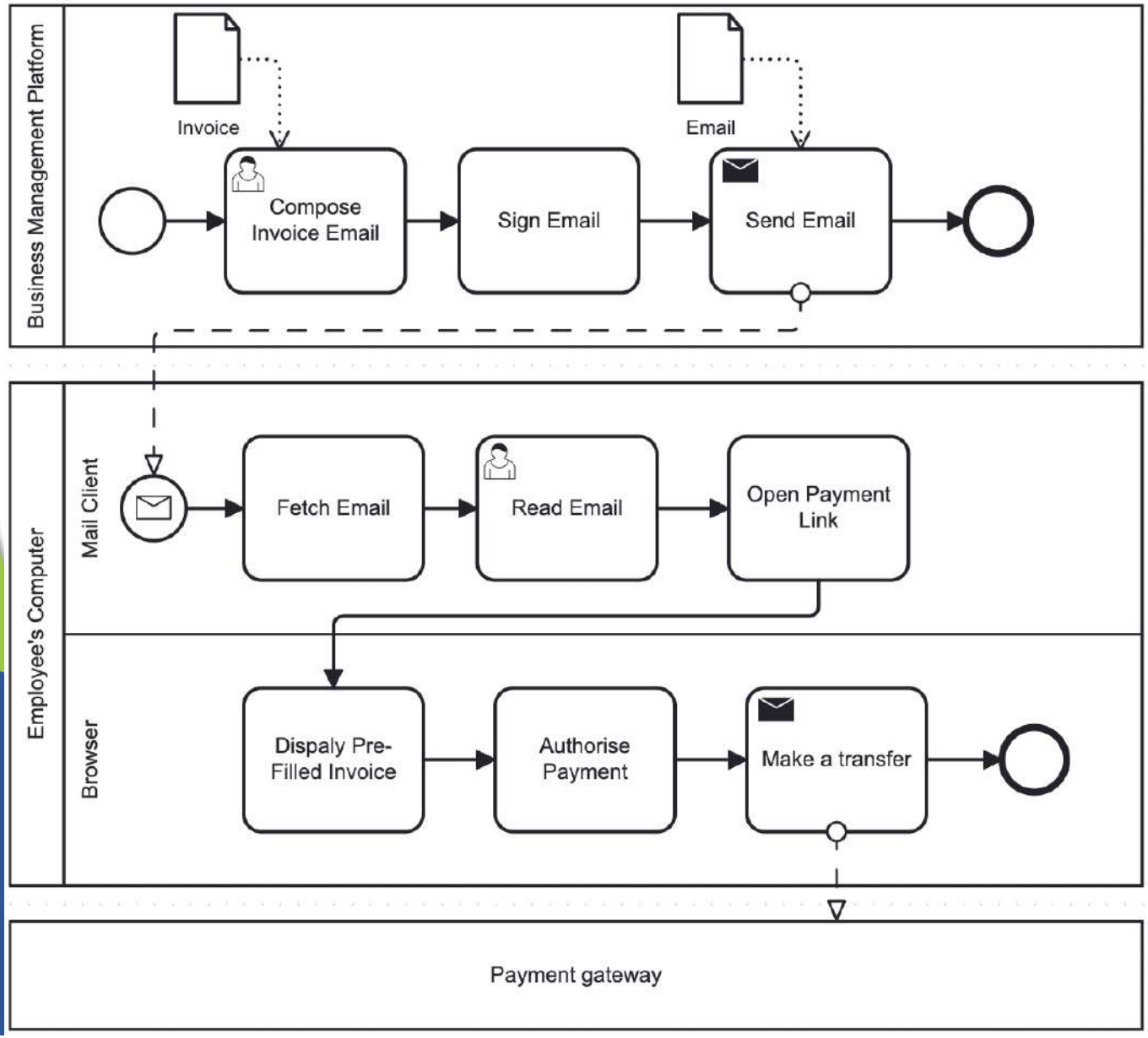
- *Brainstorming*
- *Elicitation*

- *BPMN*
- *Tools (e.g., bpmn.io, etc)*



This Photo by Unknown Author is licensed under CC BY

Running Scenario



What is

Security Engineering?

Security Engineering

Lowering the risk of intentional unauthorised harm to valuable assets to level that is acceptable to the system's stakeholders by preventing and reacting to malicious harm, misuse, threats, and security risks

Firesmith, D.: Engineering safety- and security-related requirements for software- intensive systems. Tutorial, 2007 Carnegie Mellon University (2007)

Security Engineering

Lowering the risk of **intentional unauthorised** harm to **valuable assets** to level that is **acceptable** to the system's stakeholders by preventing and reacting to **malicious harm**, **misuse**, **threats**, and **security risks**

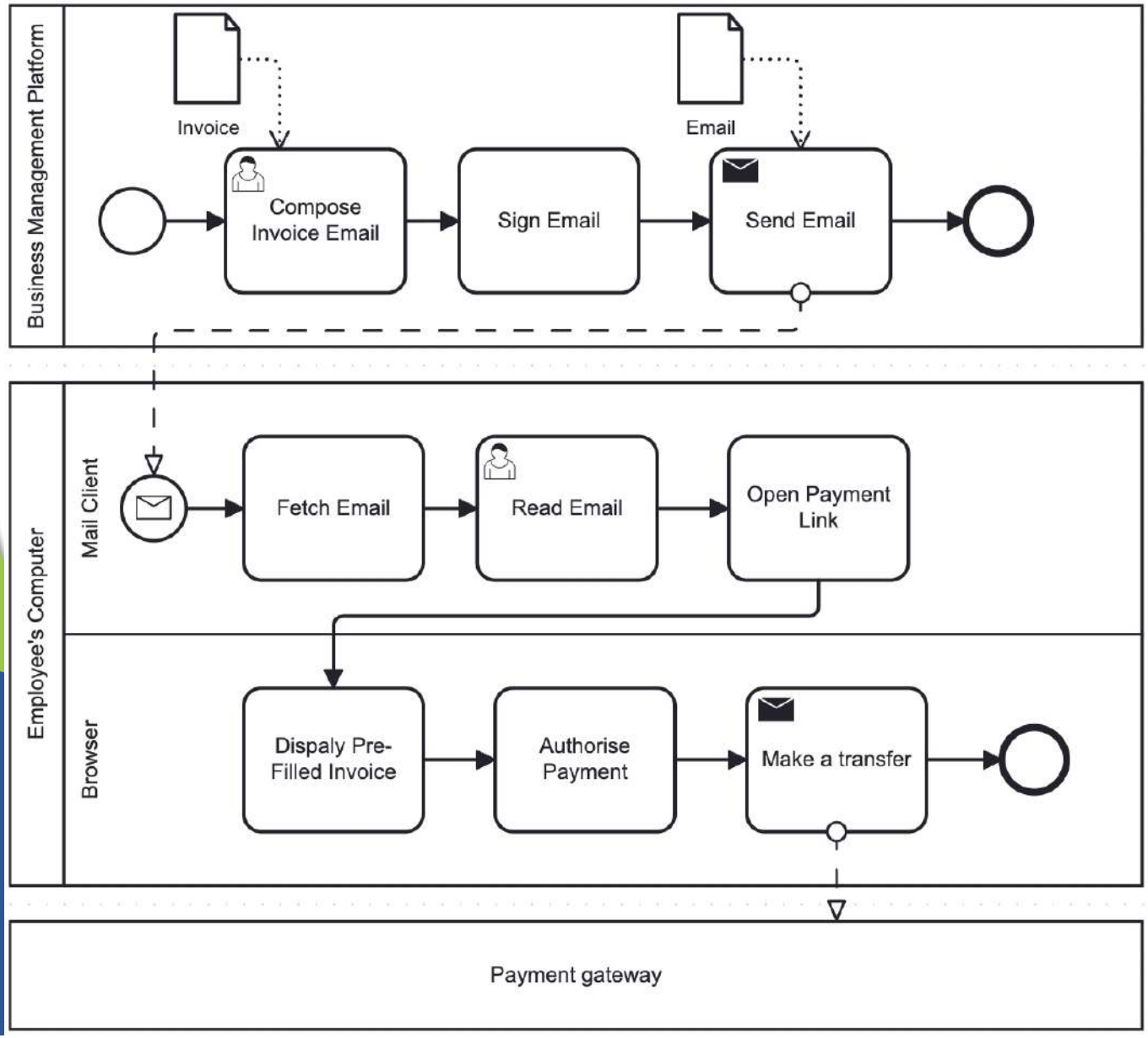
Firesmith, D.: Engineering safety- and security-related requirements for software- intensive systems. Tutorial, 2007 Carnegie Mellon University (2007)

The Quiz

https://liitu.ee/824550

What

do we protect?


Business Management Platform
Invoice
Email
Compose Invoice Email
Sign Email
Send Email
Employee's Computer
Mail Client
Fetch Email
Read Email
Open Payment Link
Browser
Dispaly Pre-Filled Invoice
Authorise Payment
Make a transfer
Payment gateway

Security Objectives

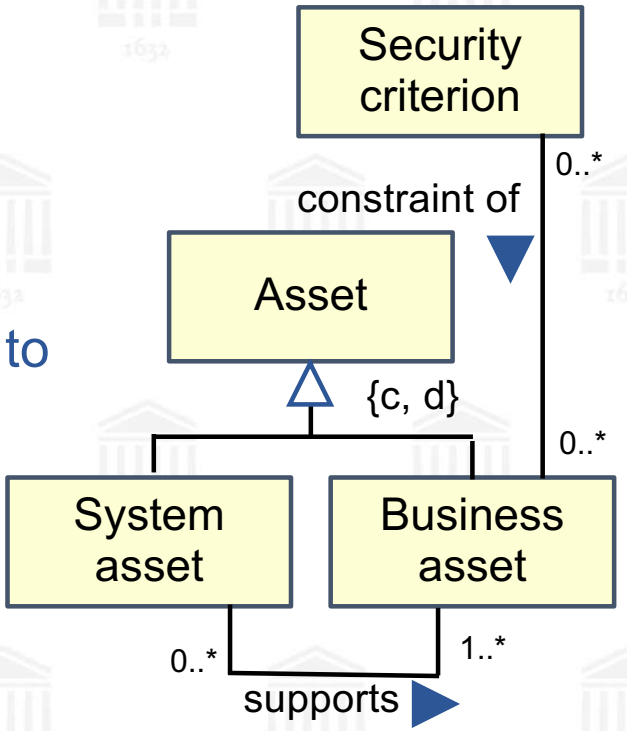
- **Confidentiality** – a property of being made not available or disclosed to unauthorized individuals, entities or processes

- **Integrity** – a property of safeguarding the accuracy and completeness of assets
  - ***Accuracy*** could be threatened by (unauthorised or undesirable) update or tampering
  - ***Completeness*** could be threatened using altering or deletion

- **Availability** – a property of being accessible and usable upon demand by an authorised entity

Asset-related concepts

- **Business assets**: Information, process, skill inherent to the business of the organisation
- **System assets:** a component or part of the system that is necessary for achieving its objectives and supporting business assets



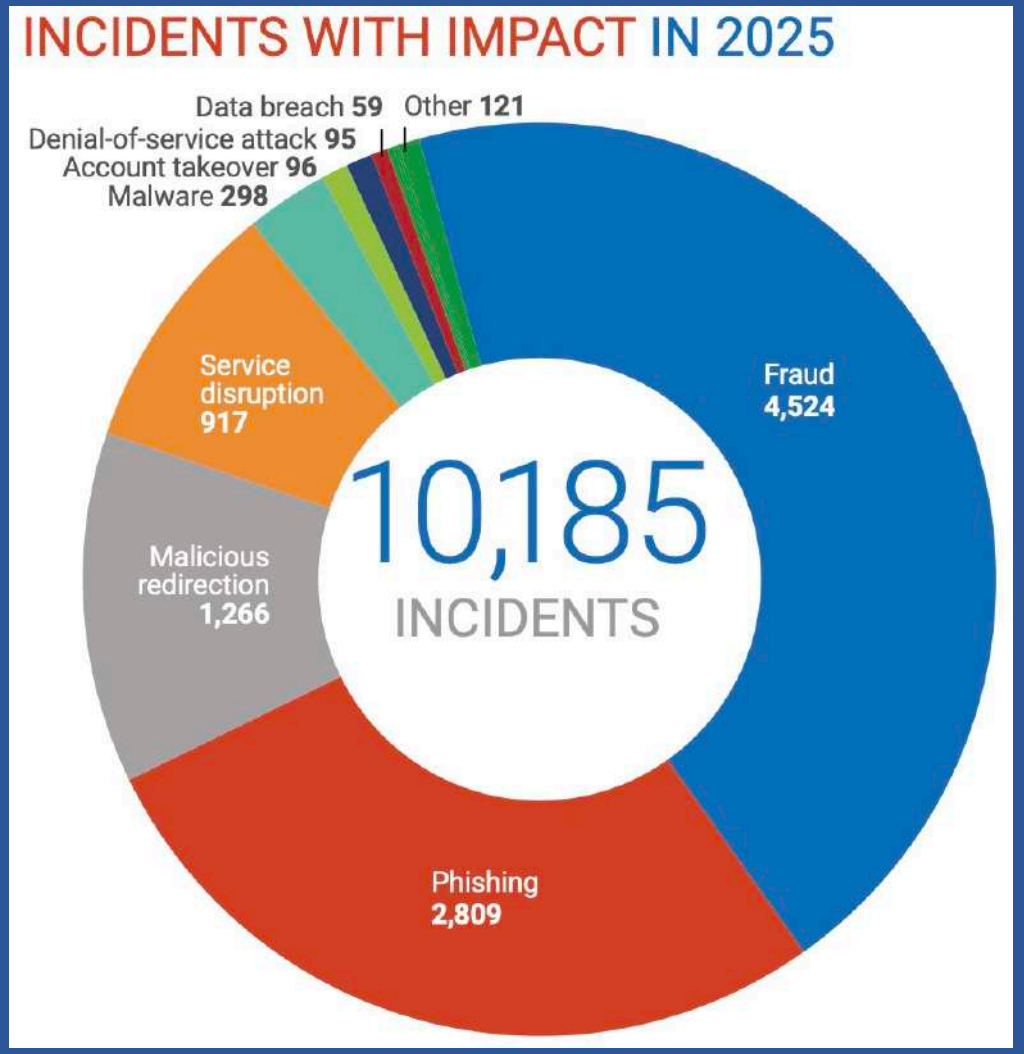
Against what

do we protect?

Security Threat

Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself

https://csrc.nist.gov/glossary/term/



RIA: Cyber Security in Estonia 2026

A denial-of-service:
prevention of authorized access to resources or the delaying of time-critical operations

Ransomware:
an attack where threat actors take control of a target's assets and demand a ransom in exchange for the return of the assets' availability

https://csrc.nist.gov/glossary/term/

Malware:
hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose

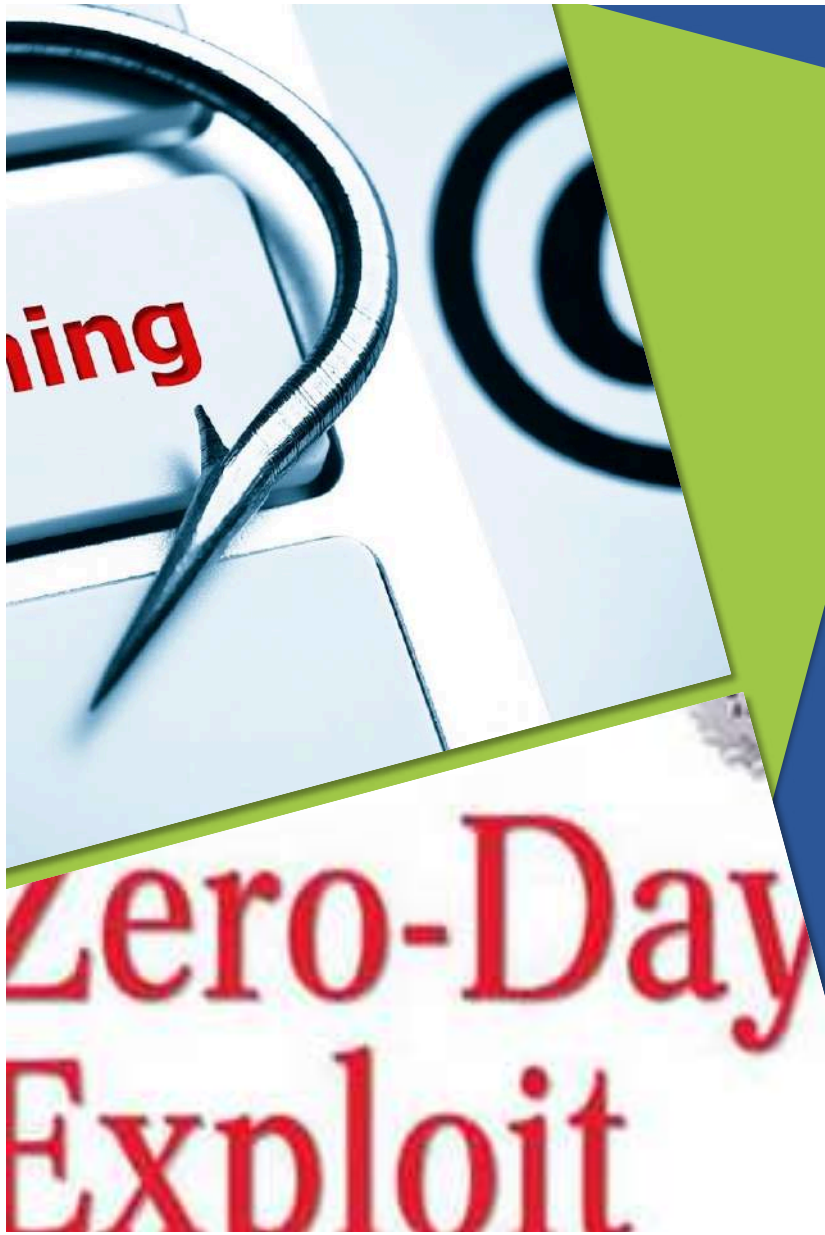
Man-in-the-middle (MitM): an attack where the adversary positions himself in between the user and the system so that he can intercept and alter data traveling between them

https://csrc.nist.gov/glossary/term/

Data spoofing:
Introduction of incorrect digital data to the target receiver for its use in processing of signals and the calculation

SQL injection:
an attacks that look for web sites that pass insufficiently-processed user input to database back-ends

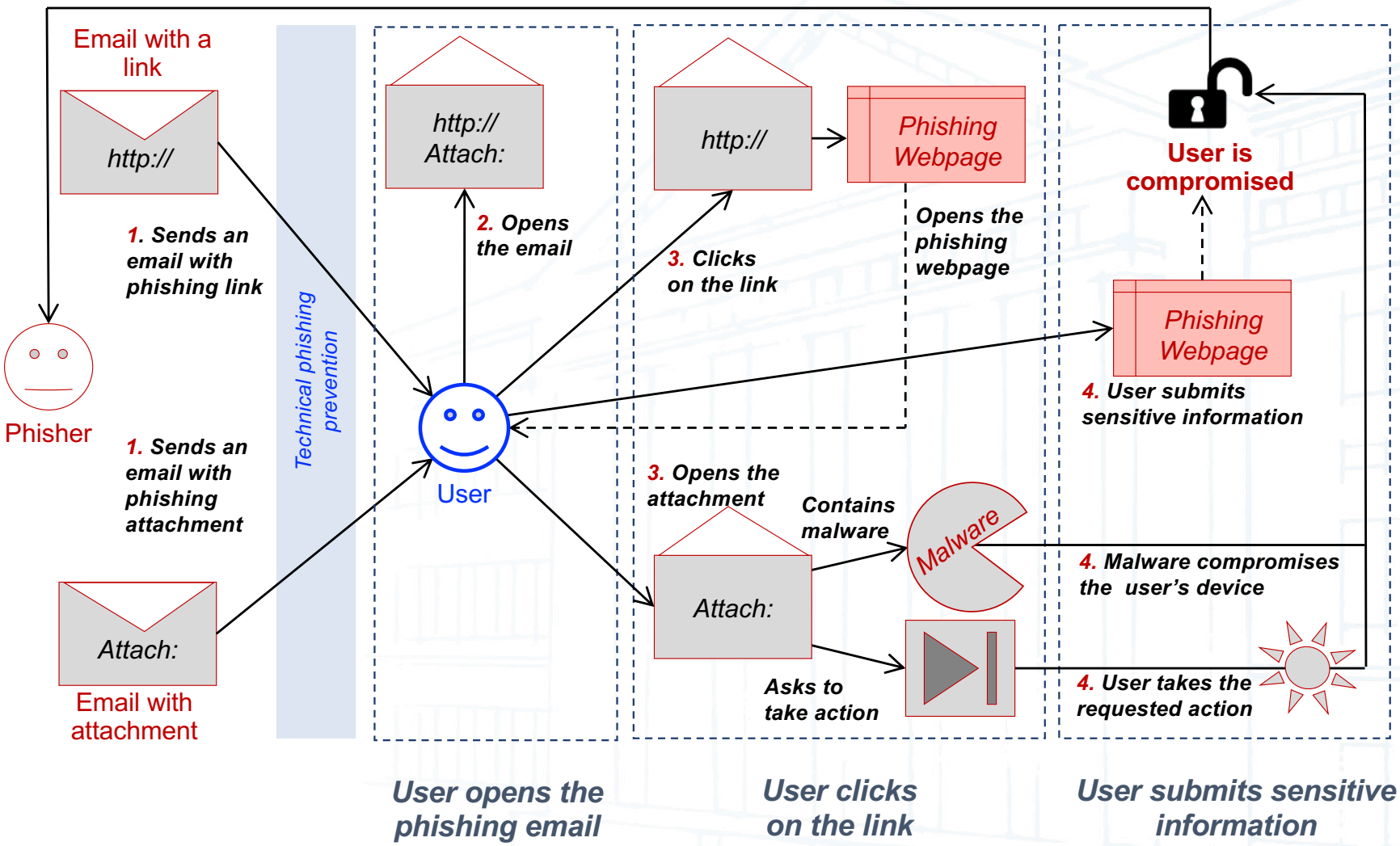
https://csrc.nist.gov/glossary/term/

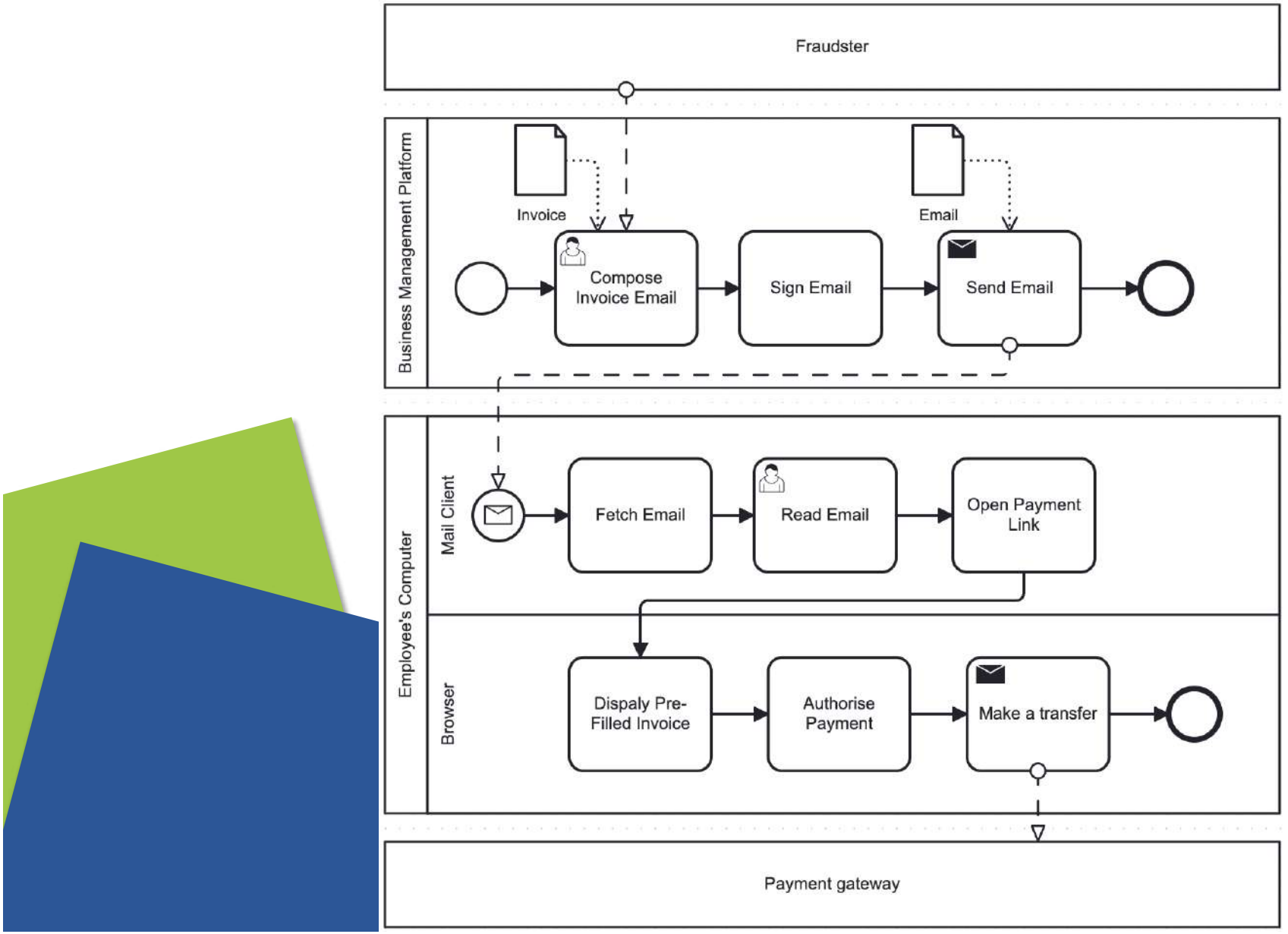


Phishing:
tricking individuals into disclosing sensitive personal information by claiming to be a trustworthy entity in an electronic communication

Zero-day attack:
an attack that exploits a previously unknown hardware, firmware, or software vulnerability

https://csrc.nist.gov/glossary/term/

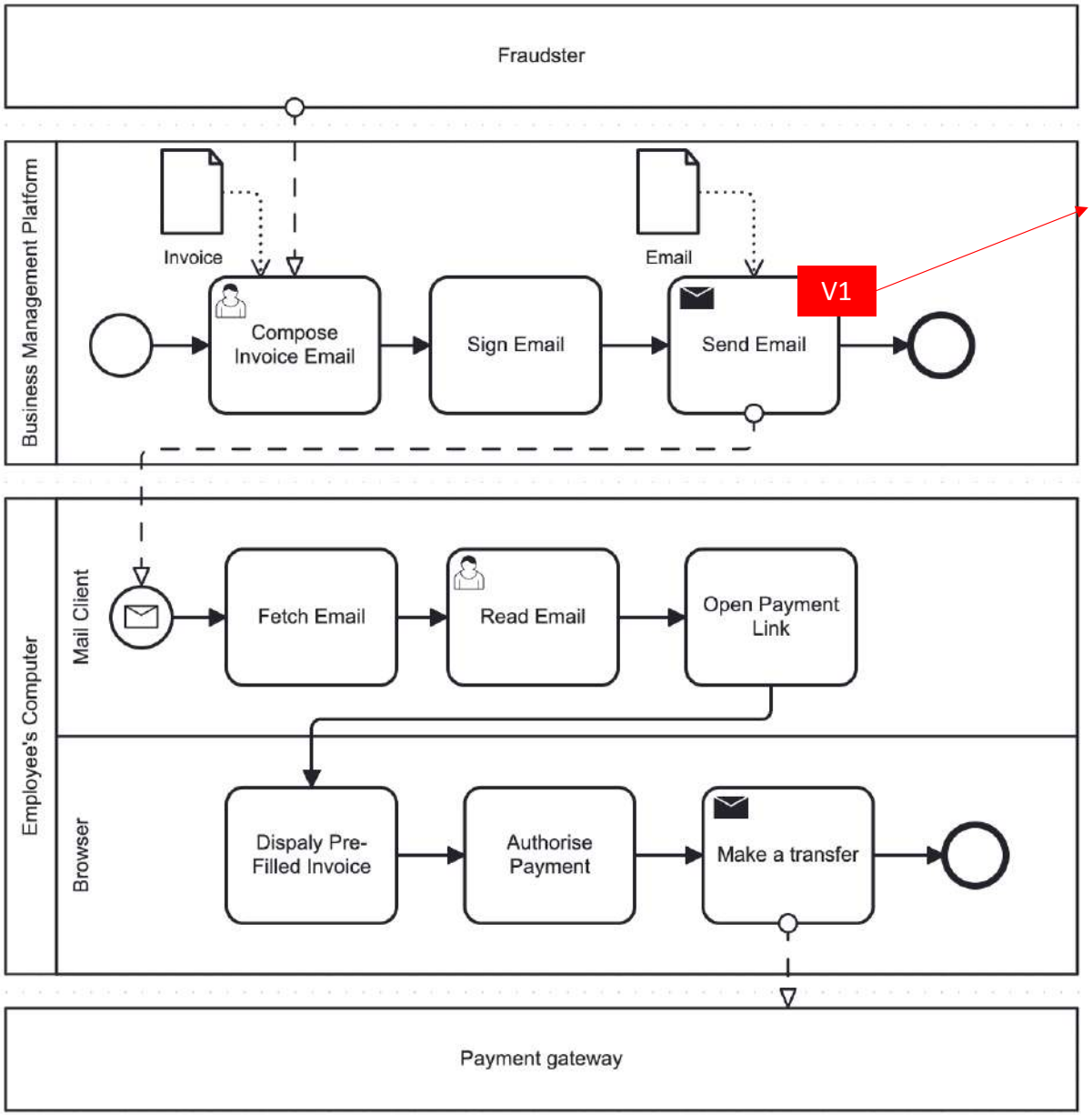

Email with a link
http://
1. Sends an email with phishing link
Phisher
1. Sends an email with phishing attachment
Attach:
Email with attachment
Technical phishing prevention
http:// Attach:
2. Opens the email
User
http://
Phishing Webpage
3. Clicks on the link
Opens the phishing webpage
3. Opens the attachment
Contains malware
Malware
Attach:
Asks to take action
User is compromised
Phishing Webpage
4. User submits sensitive information
4. Malware compromises the user's device
4. User takes the requested action
User opens the phishing email
User clicks on the link
User submits sensitive information


Fraudster
Business Management Platform
Invoice
Email
Compose Invoice Email
Sign Email
Send Email
Employee's Computer
Mail Client
Fetch Email
Read Email
Open Payment Link
Browser
Dispaly Pre-Filled Invoice
Authorise Payment
Make a transfer
Payment gateway

Vulnerability

Vulnerability *constitutes a weakness or a flaw in terms of system security*

- **V1:** A legitimate business management platform can be used to send fraudulent emails

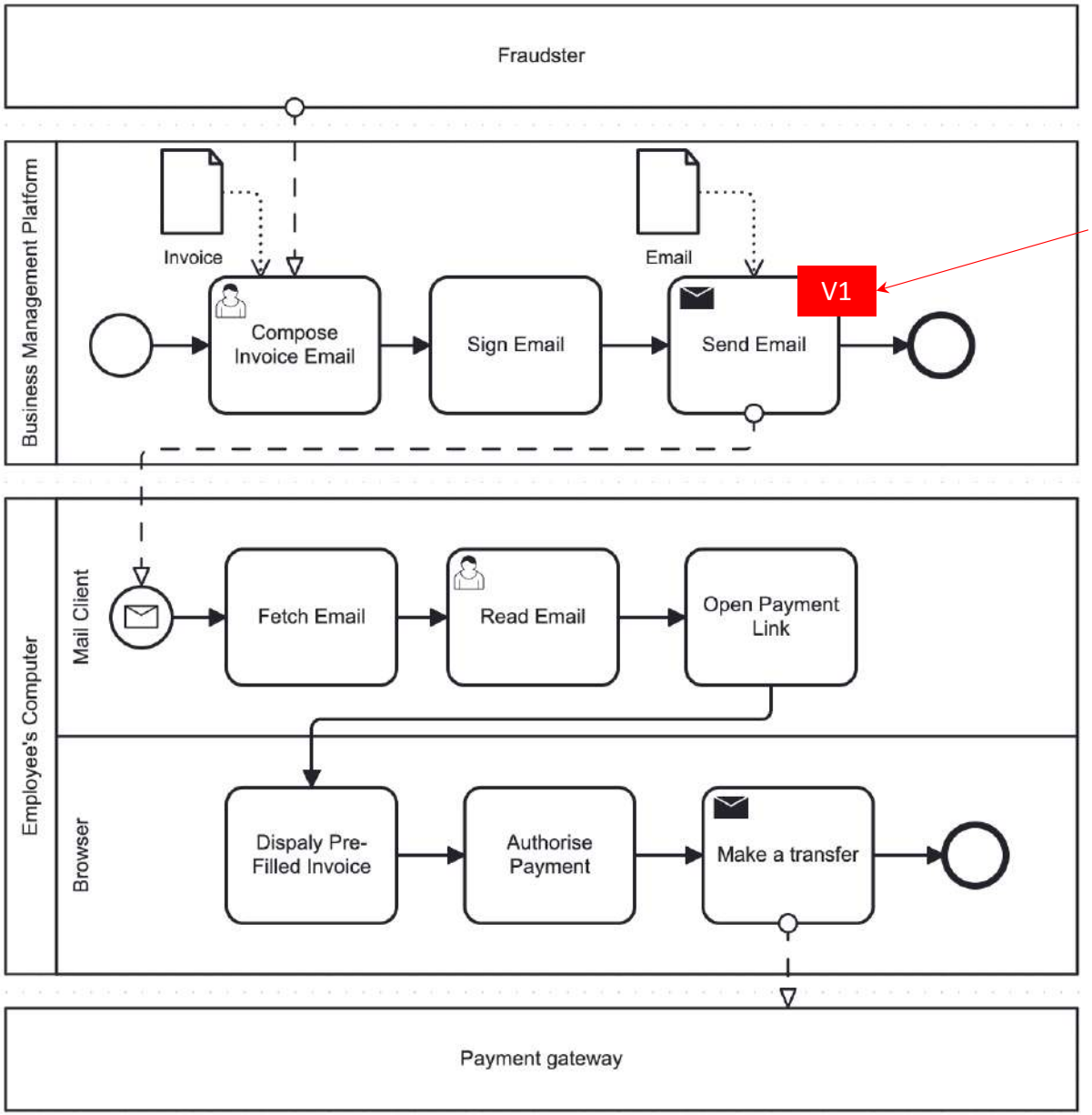


A legitimate business management platform can be used to send fraudulent emails

Threat

A threat *is an incident initiated by a threat agent using an attack method to target one or more IS assets by exploiting their vulnerabilities.*

- **Th1:** A threat actor sends a fraudulent invoice via the legitimate business management platform

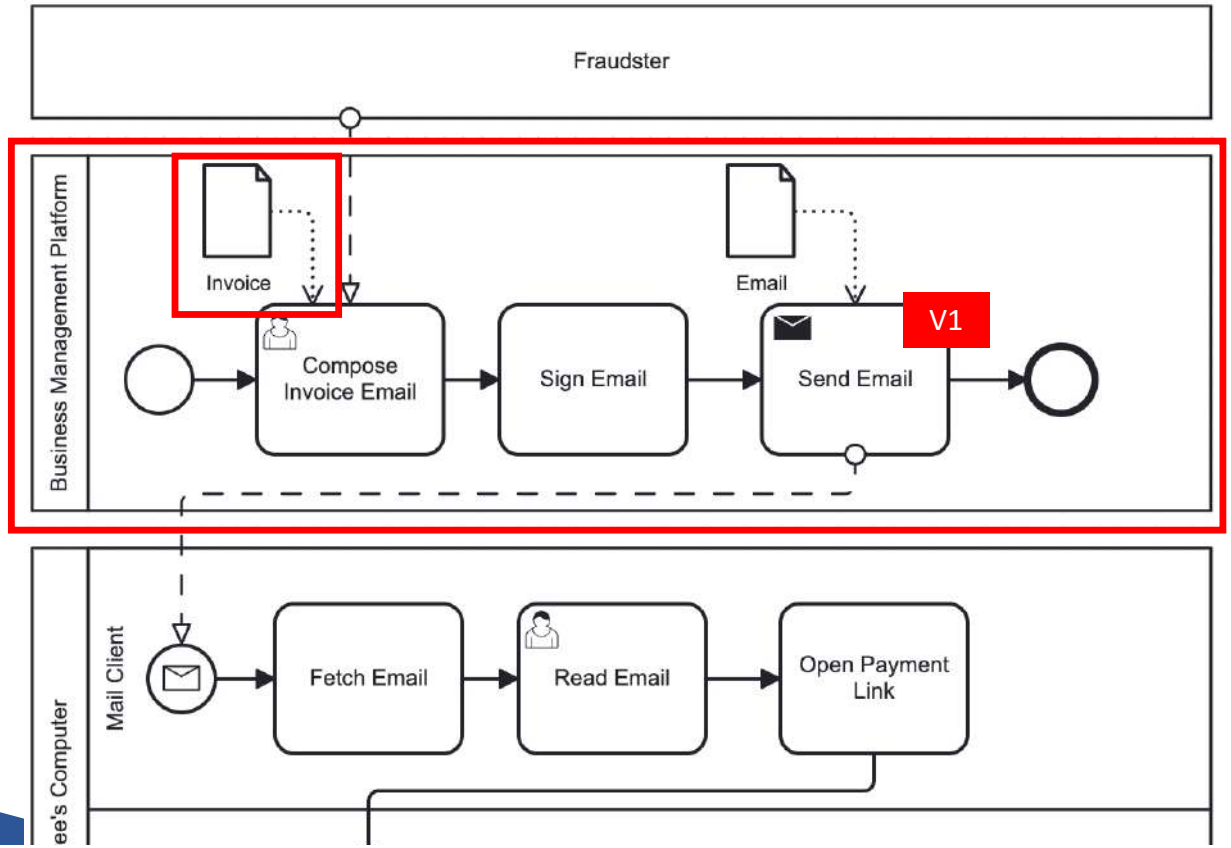


Th1: A threat agent sends a fraudulent invoice via the legitimate business management platform

Impact

Impact is a potential negative consequence when a threat is accomplished

- The integrity of the invoice was negated
- The invoice is not real
- The Business Management platform is compromised

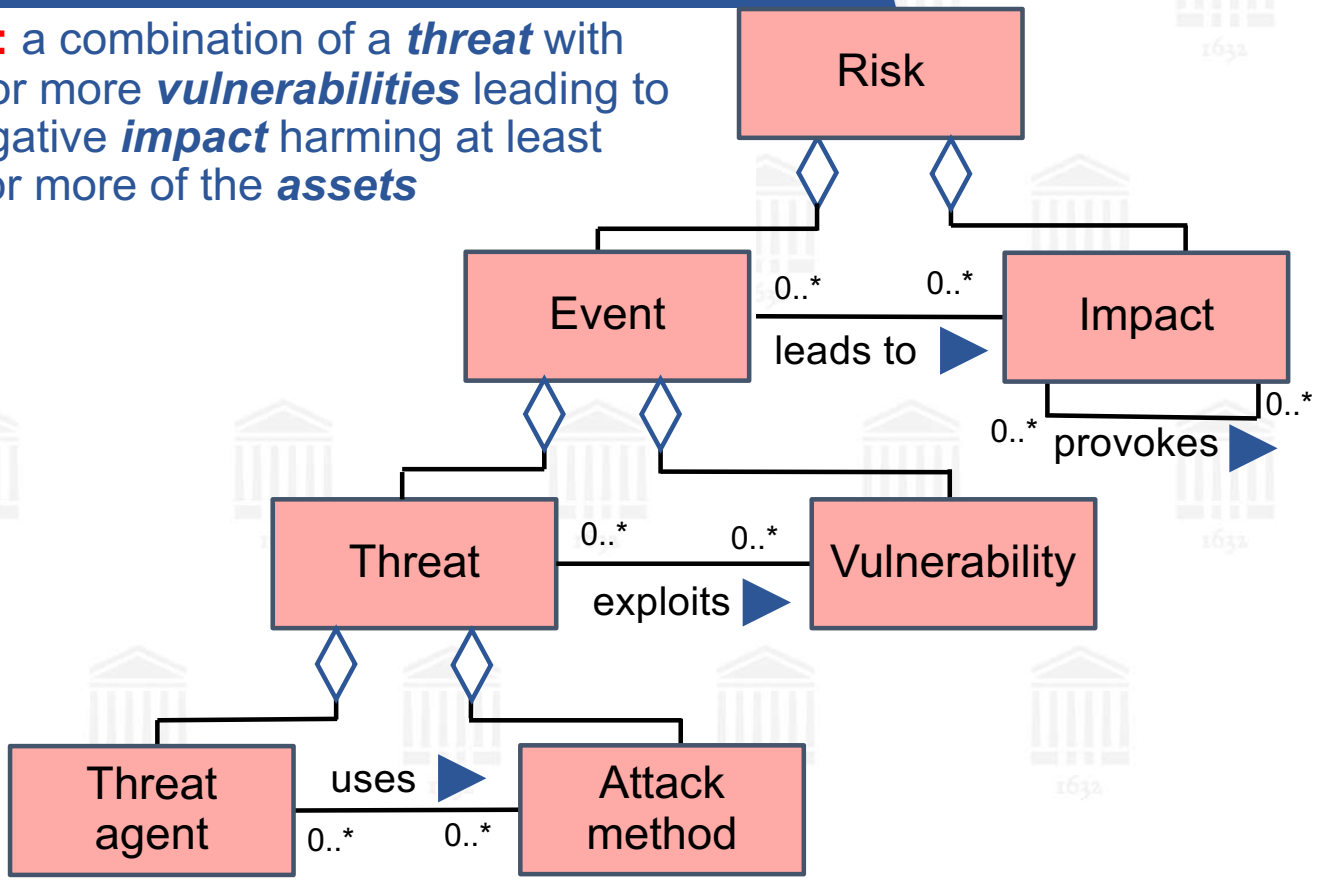


Example of data spoofing risk

- *A threat agent sends a fraudulent invoice via the legitimate business management platform because the legitimate business management platform can be used to send fraudulent emails leading to the negation of integrity of the invoice, the delivery of an illegitimate invoice and the compromise of the business management platform*

Risk-related concepts

Risk: a combination of a ***threat*** with one or more ***vulnerabilities*** leading to a negative ***impact*** harming at least two or more of the ***assets***



Impact: a potential negative consequence when a threat is accomplished

Vulnerability: constitute a weakness or a flaw in terms of system security

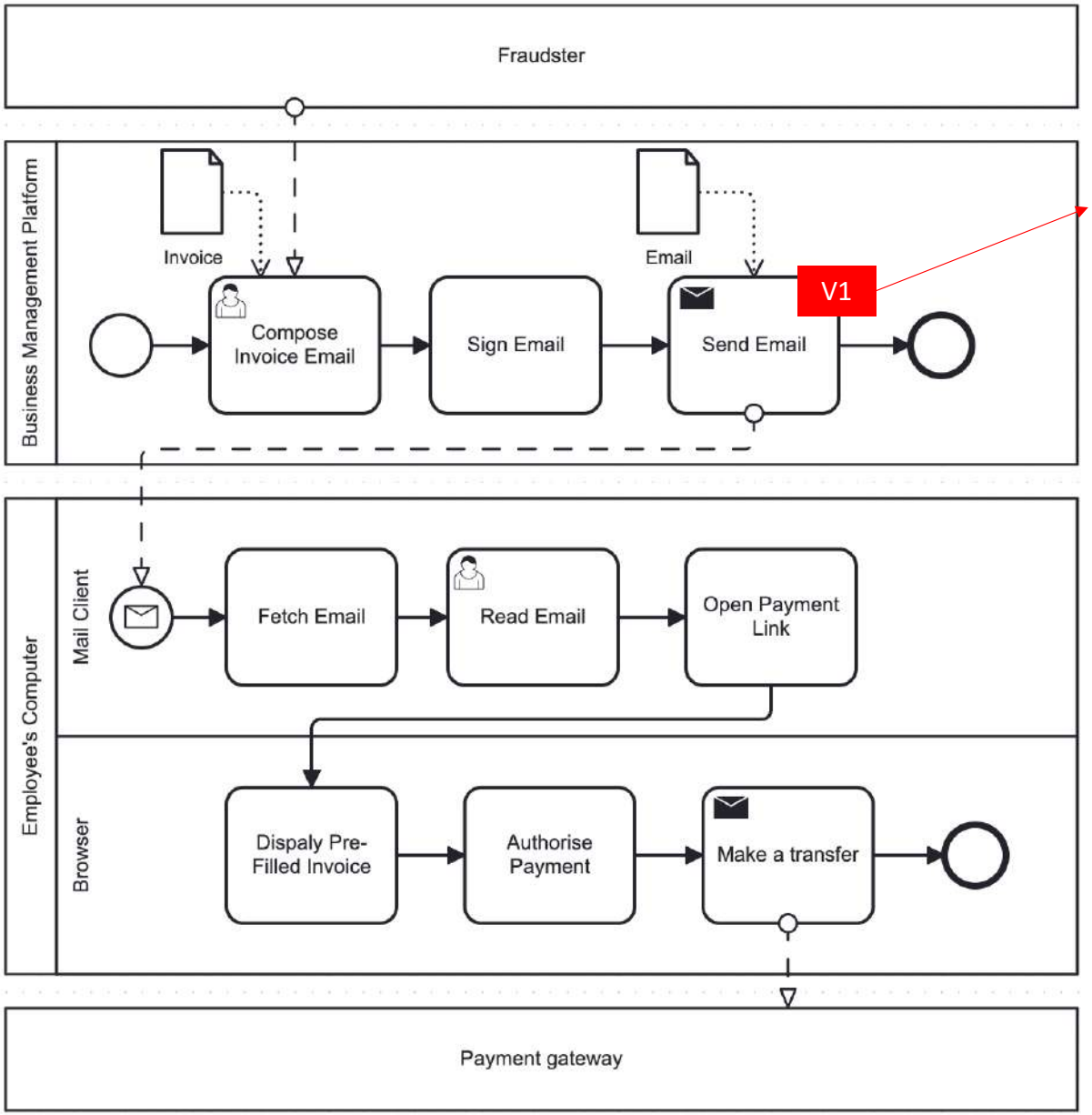
Attack method: means by which a threat agent carries out a threat

Threat agent: an agent that can potentially cause harm to system assets

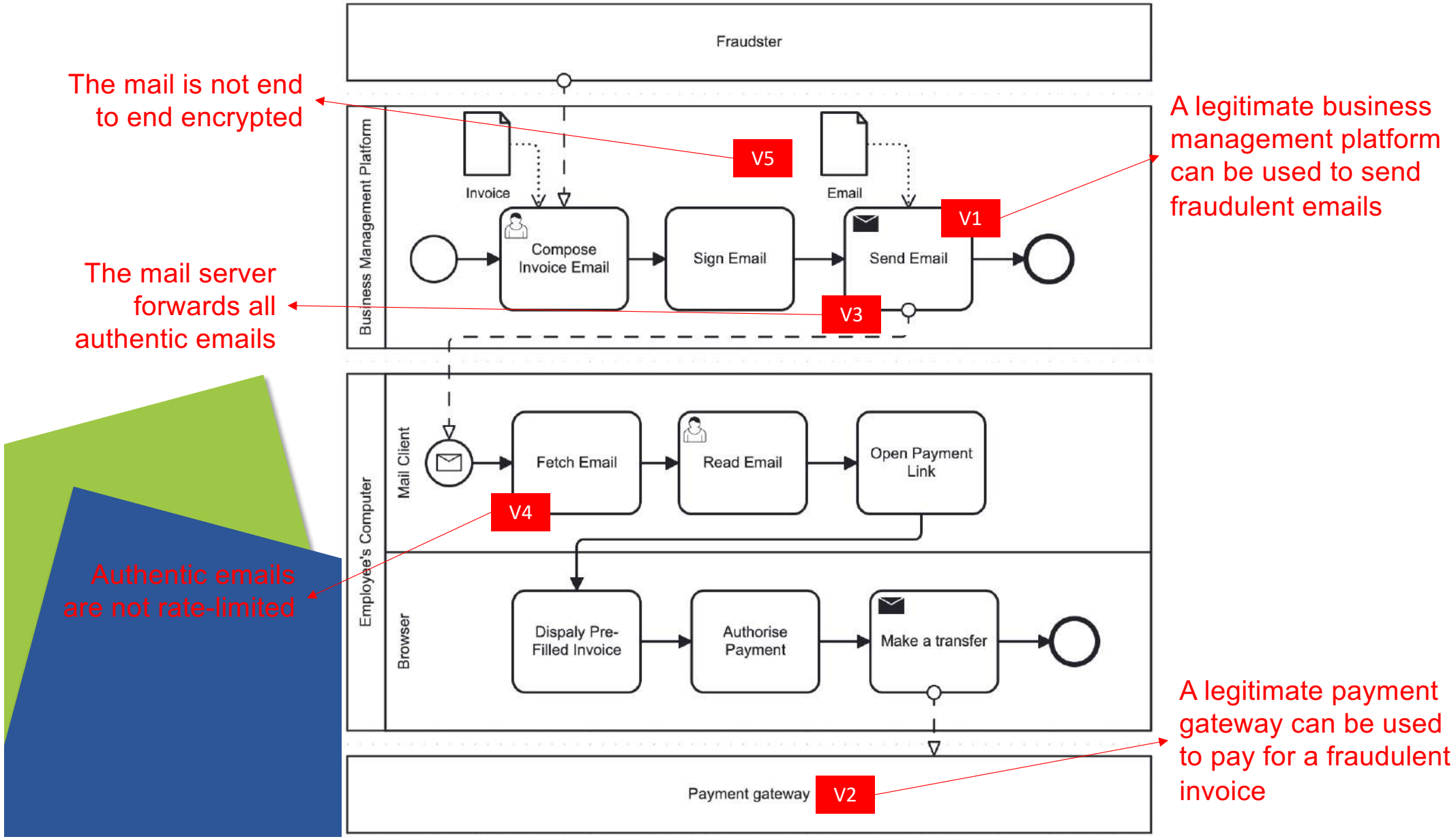
Vulnerability

Vulnerability *constitutes a weakness or a flaw in terms of system security*

- **V1:** A legitimate business management platform can be used to send fraudulent emails
- **V2:** A legitimate payment gateway can be used to pay for a fraudulent invoice
- **V3:** The mail server forwards all authentic emails
- **V4:** Authentic emails are not rate-limited
- **V5:** The email is not end-to-end encrypted



A legitimate business management platform can be used to send fraudulent emails


Fraudster
Business Management Platform
Invoice
Email
Compose Invoice Email
Sign Email
Send Email
Employee's Computer
Mail Client
Fetch Email
Read Email
Open Payment Link
Browser
Dispaly Pre-Filled Invoice
Authorise Payment
Make a transfer
Payment gateway
V1
V2
V3
V4
V5
The mail is not end to end encrypted
The mail server forwards all authentic emails
Authentic emails are not rate-limited
A legitimate business management platform can be used to send fraudulent emails
A legitimate payment gateway can be used to pay for a fraudulent invoice

Threat

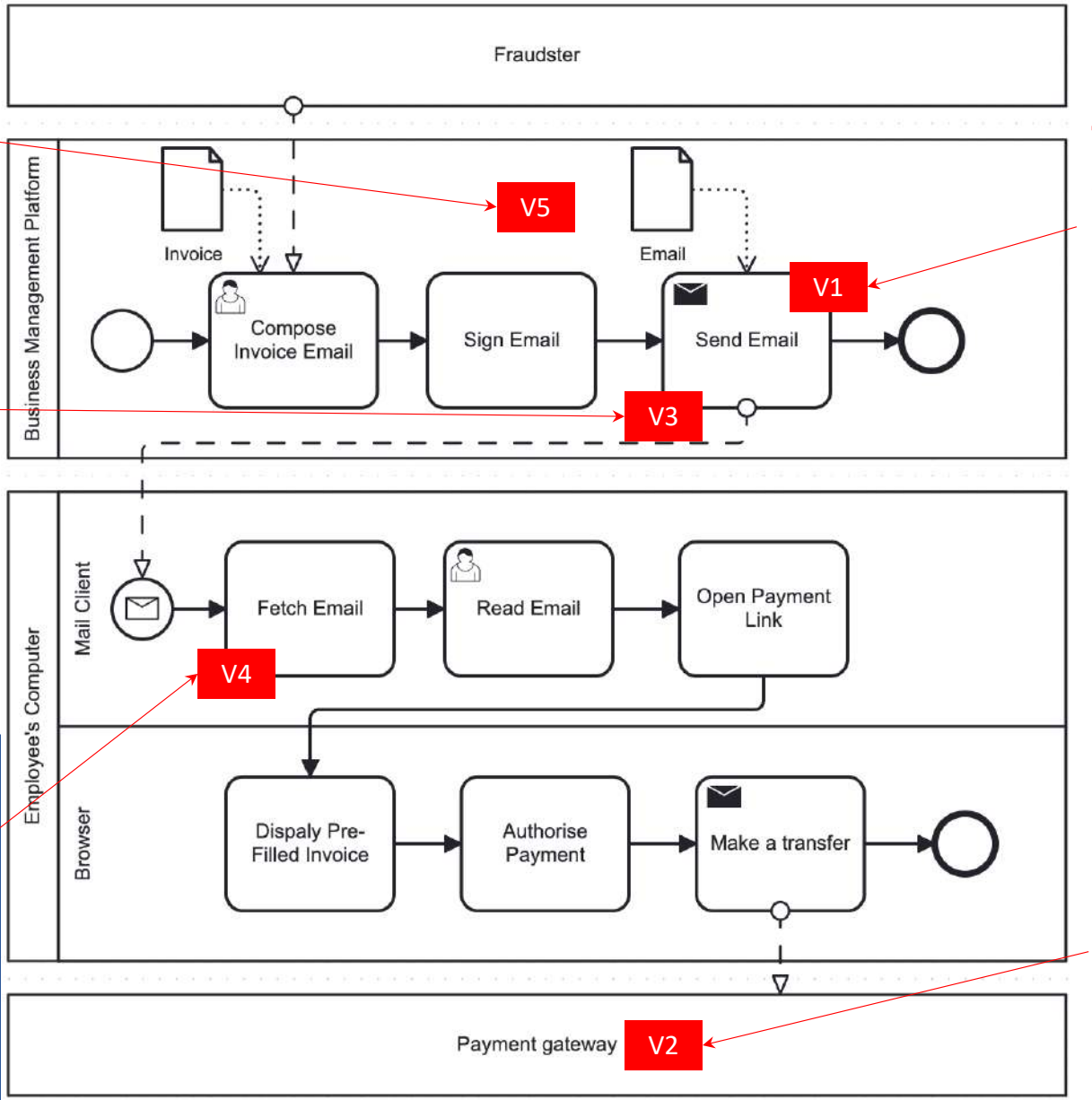
***A threat** is an incident initiated by a threat agent using an attack method to target one or more IS assets by exploiting their vulnerabilities.*

- **Th1:** A threat agent sends a fraudulent invoice via the legitimate business management platform
- **Th2:** A threat agent sets up a fraudulent invoice payment
- **Th3:** A threat agent sends a phishing email to the employee
- **Th4:** A threat agent floods the employee's inbox with subscription emails
- **Th5:** A threat agent exfiltrates email through an MCP server (LLM connector) backdoor

Th5: A threat agent exfiltrates email through an MCP server (LLM connector) backdoor

Th3: A threat agent sends a phishing email to the employee

Th4: A threat agent floods the employee's inbox with subscription emails

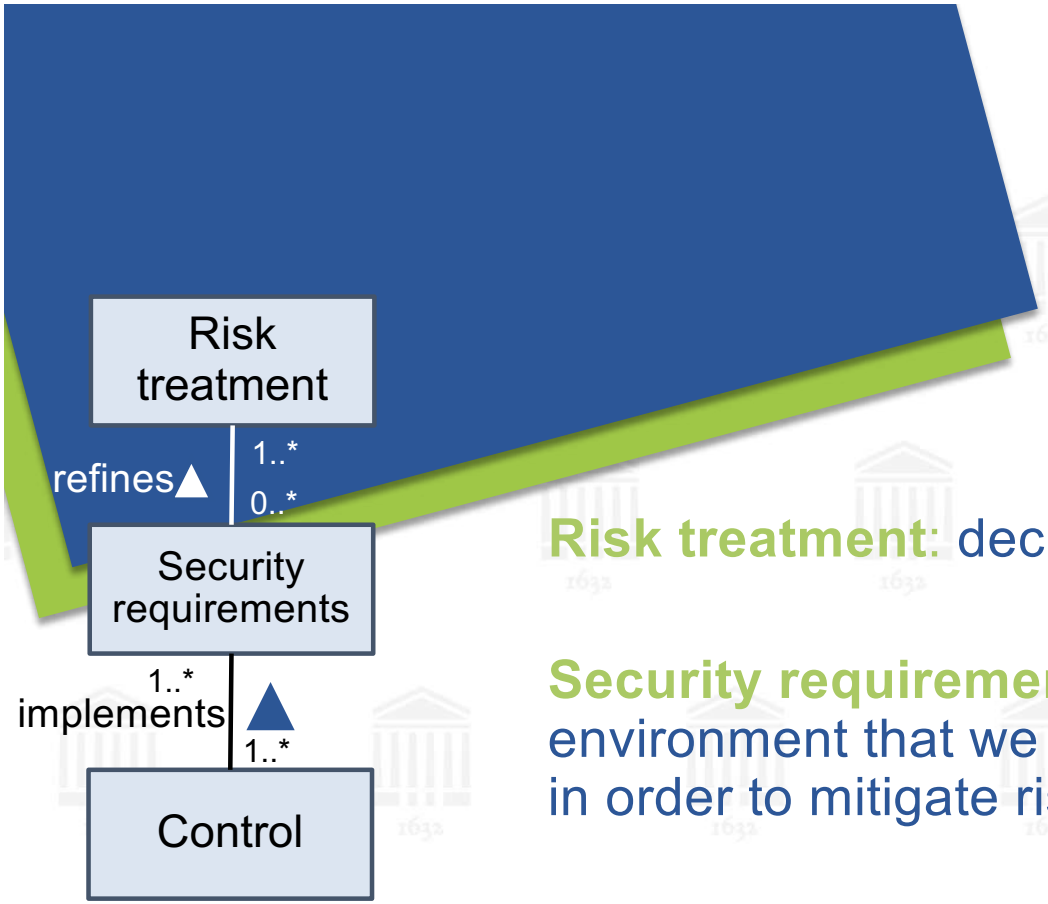


Th1: A threat agent sends a fraudulent invoice via the legitimate business management platform

Th2: A threat agent sets up a fraudulent invoice payment

What are the security countermeasures?

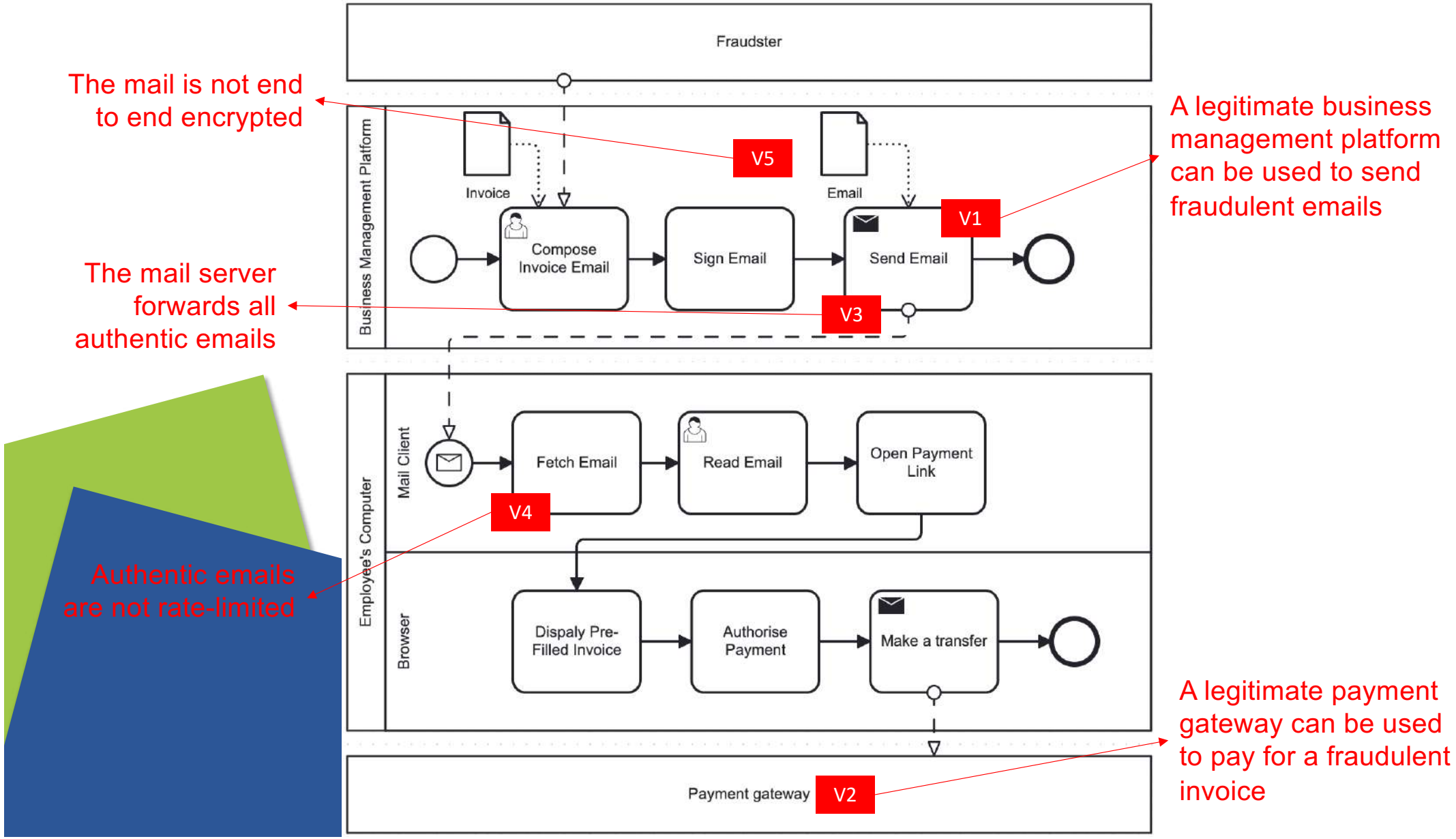
Risk treatment-related concepts



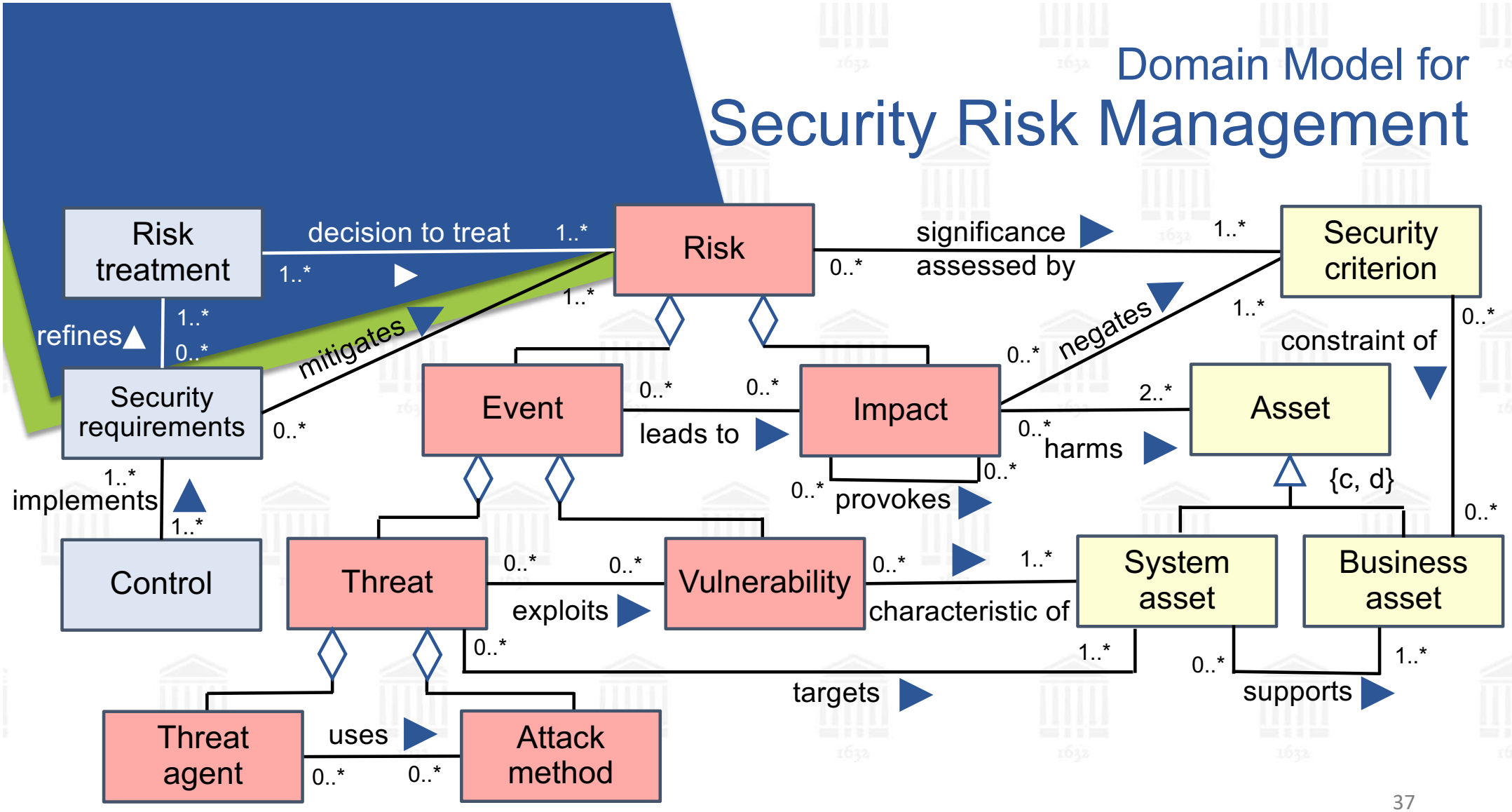
Risk treatment: decision of how to treat the identified risks

Security requirement: condition over the phenomena of the environment that we wish to make true by installing the system, in order to mitigate risks

Control: designed means to improve security, specified by a security requirement, and implemented to comply with it


Fraudster
Business Management Platform
Invoice
Email
Compose Invoice Email
Sign Email
Send Email
Employee's Computer
Mail Client
Fetch Email
Read Email
Open Payment Link
Browser
Dispaly Pre-Filled Invoice
Authorise Payment
Make a transfer
Payment gateway
V1
V2
V3
V4
V5
The mail is not end to end encrypted
The mail server forwards all authentic emails
Authentic emails are not rate-limited
A legitimate business management platform can be used to send fraudulent emails
A legitimate payment gateway can be used to pay for a fraudulent invoice

Domain Model for Security Risk Management



The next step:

Forensic Readiness

Forensic Readiness

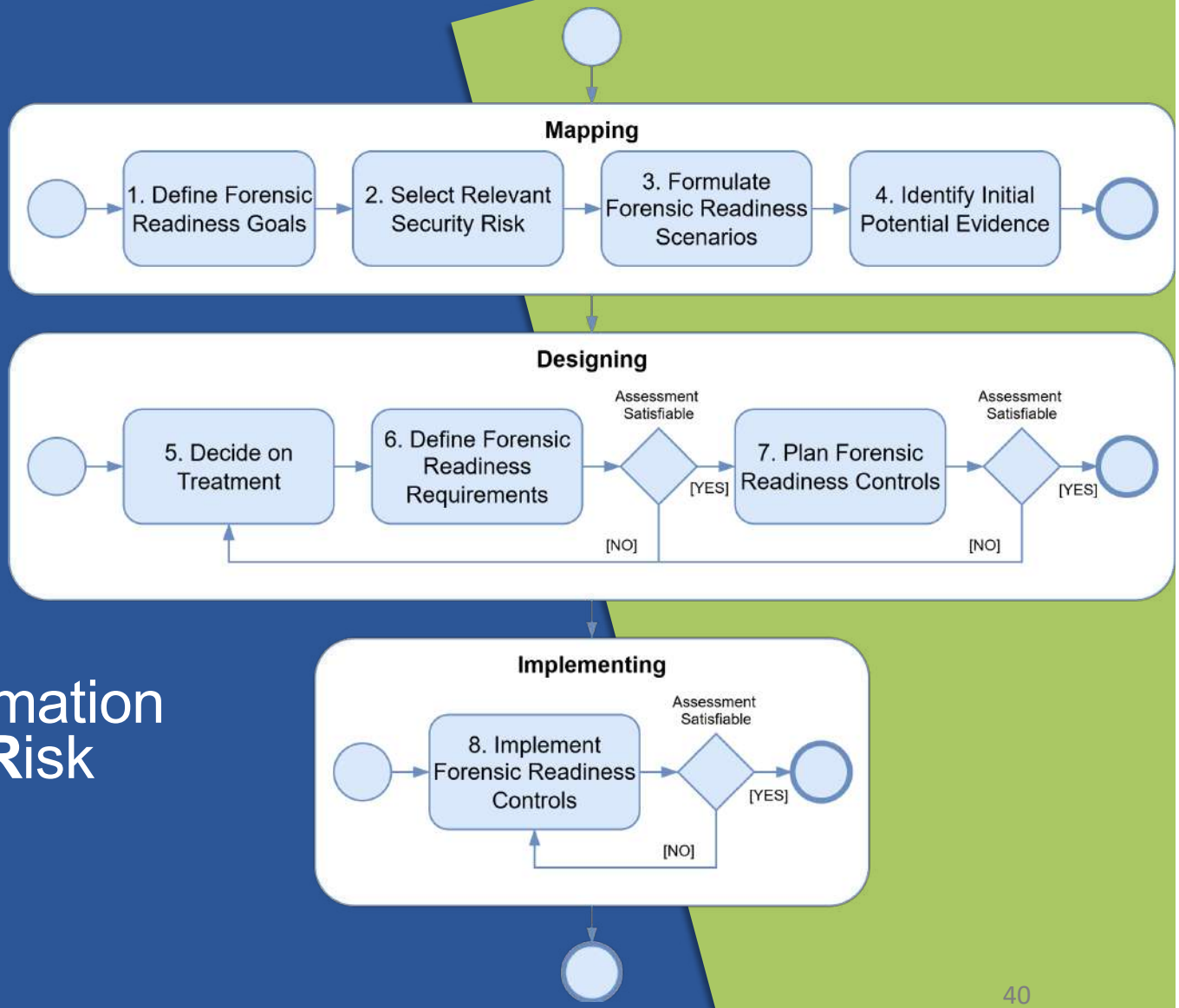
Proactive steps towards incident investigation

Forensic-ready systems (forensic-by-design)

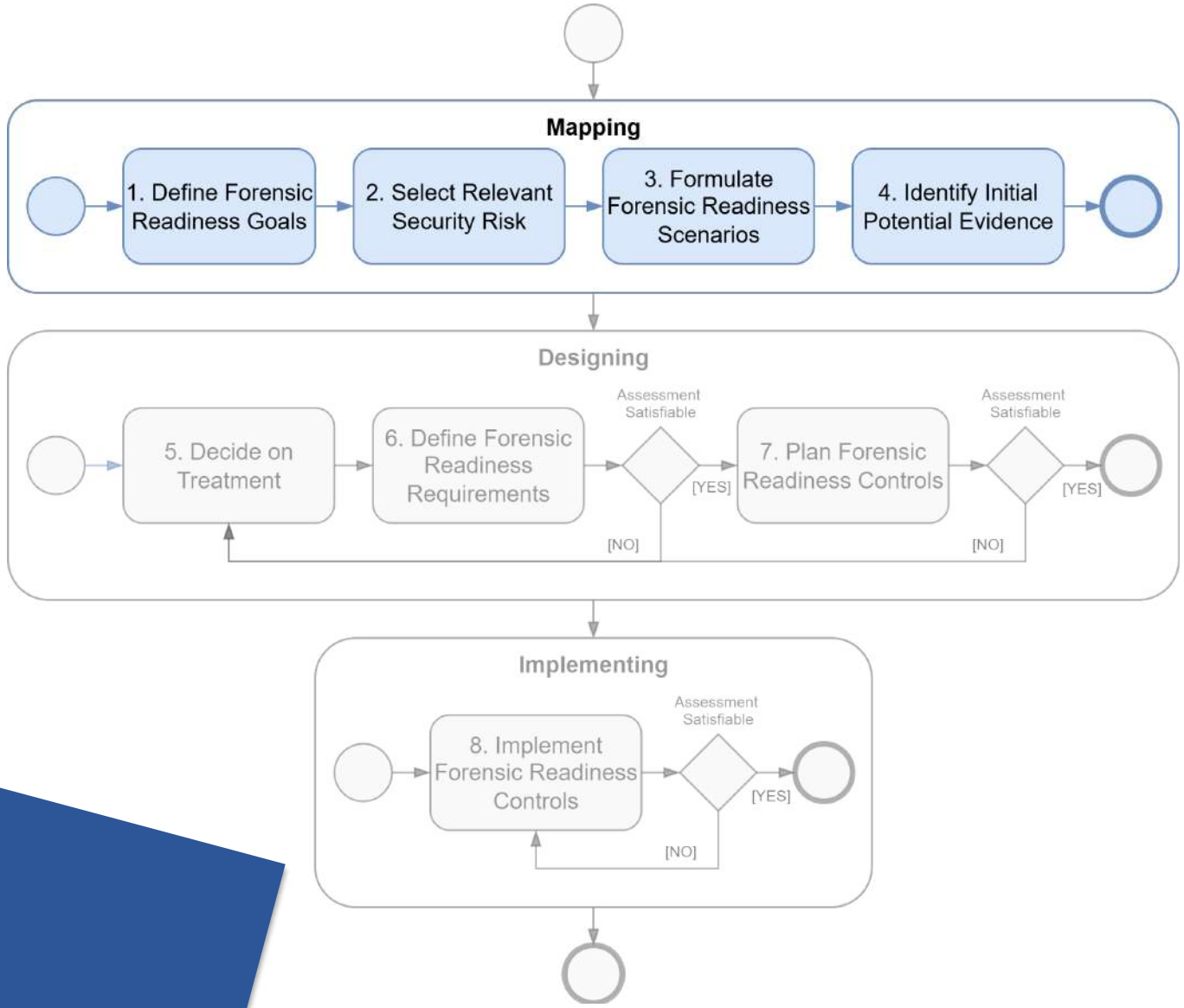
- *Prepare systems during development*
- *Ensure rich and forensically sound evidence for future use*

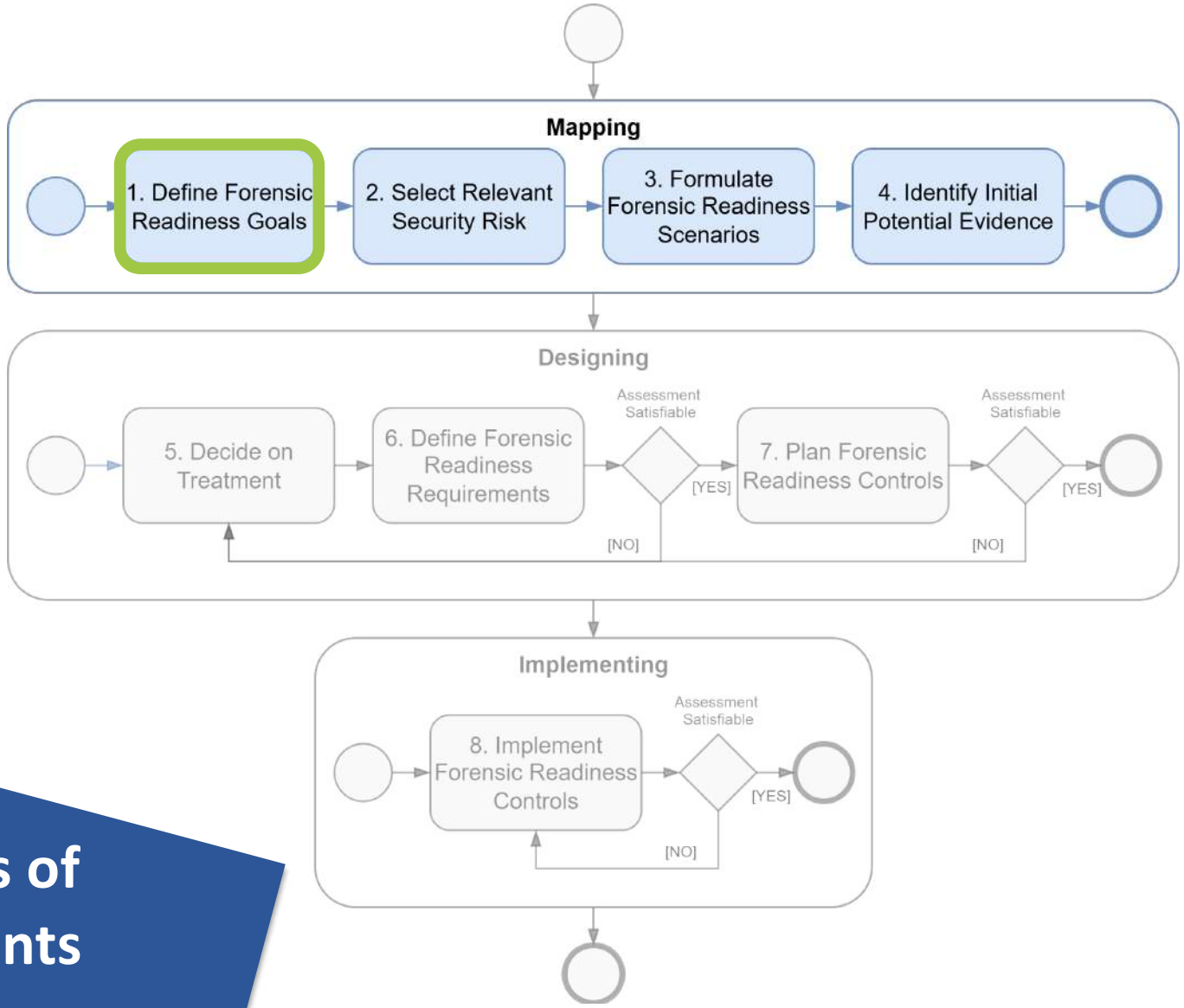
Rowlingson, Robert. "A ten step process for forensic readiness." International Journal of Digital Evidence 2.3 (2004)

FR-ISSRM Process

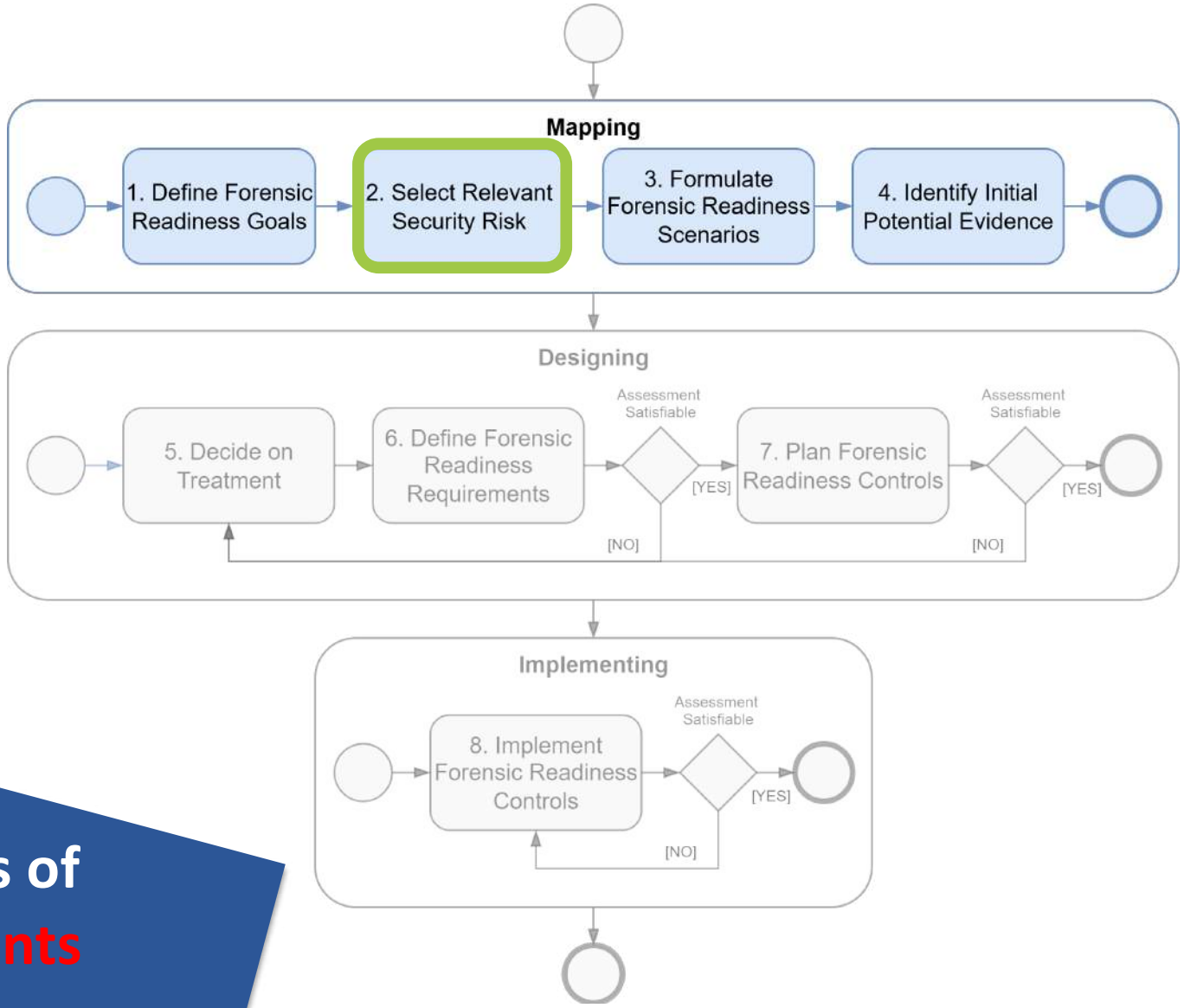


Forensic-**R**eady **I**nformation **S**ystems **S**ecurity **R**isk **M**anagement

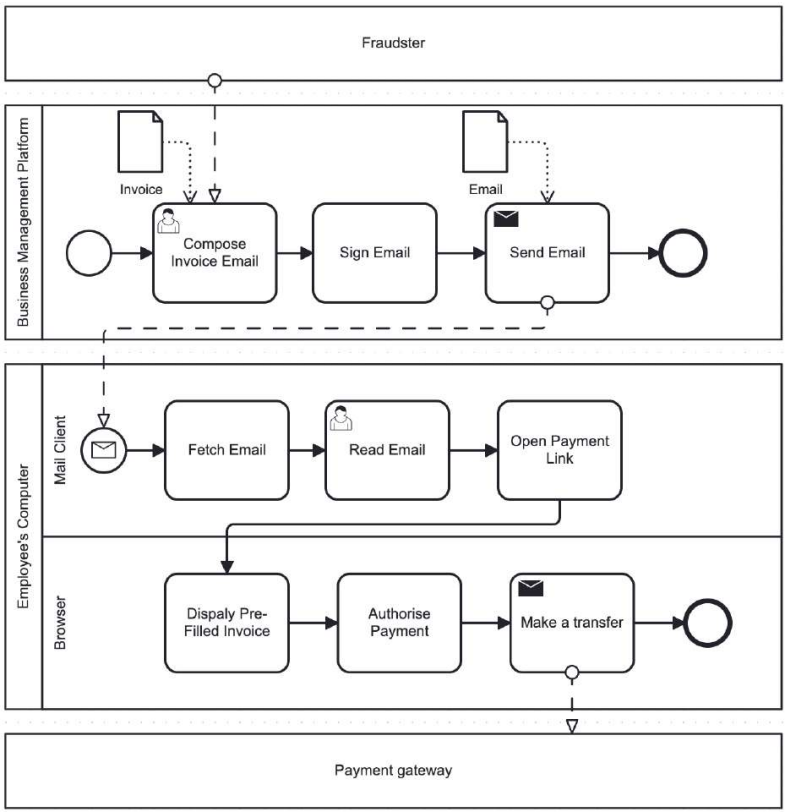

Mapping
1. Define Forensic Readiness Goals
2. Select Relevant Security Risk
3. Formulate Forensic Readiness Scenarios
4. Identify Initial Potential Evidence
Designing
5. Decide on Treatment
6. Define Forensic Readiness Requirements
Assessment Satisfiable
[YES]
[NO]
7. Plan Forensic Readiness Controls
Assessment Satisfiable
[YES]
[NO]
Implementing
8. Implement Forensic Readiness Controls
Assessment Satisfiable
[YES]
[NO]

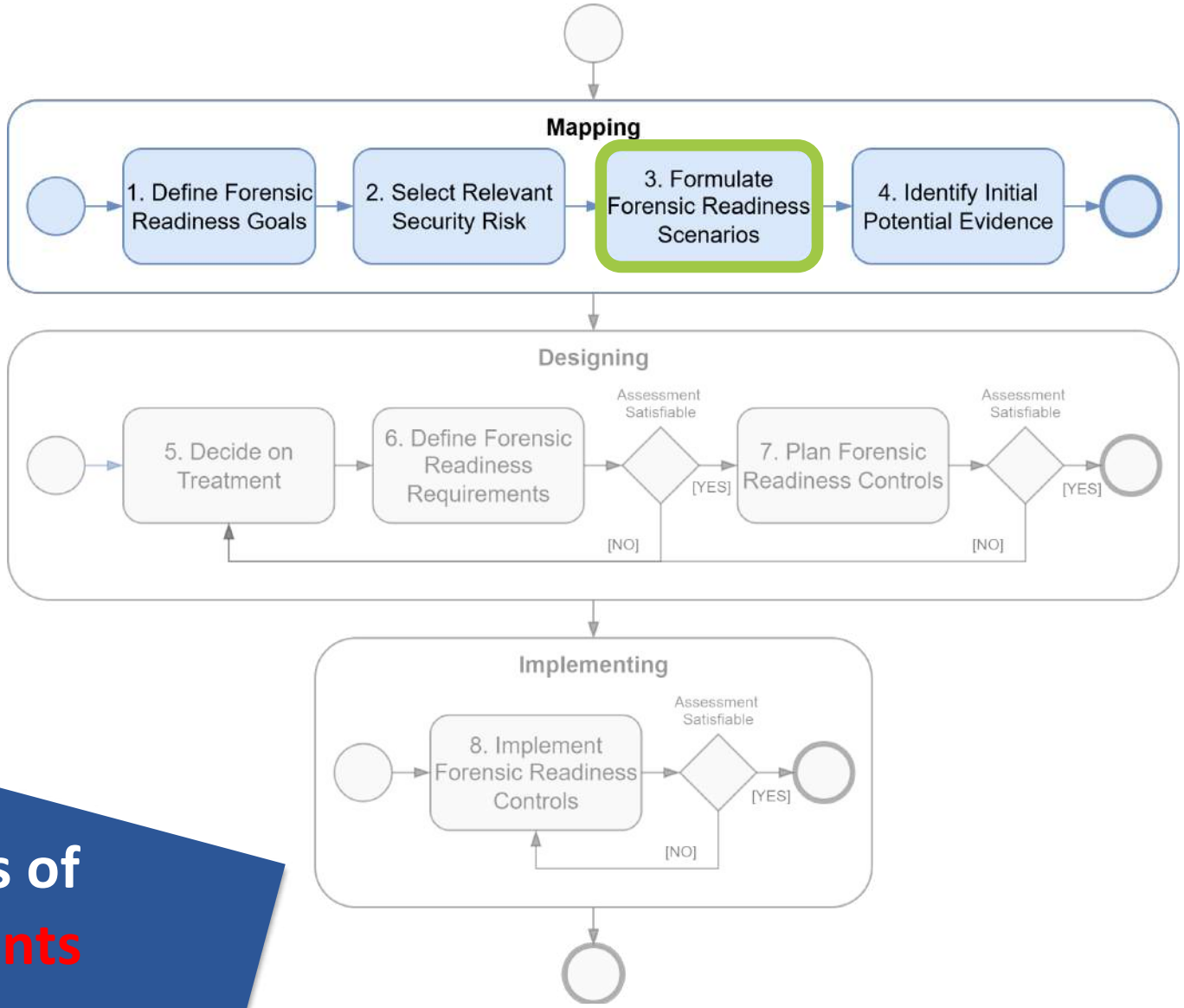


Ensure that investigations of fraudulent invoice payments are possible.

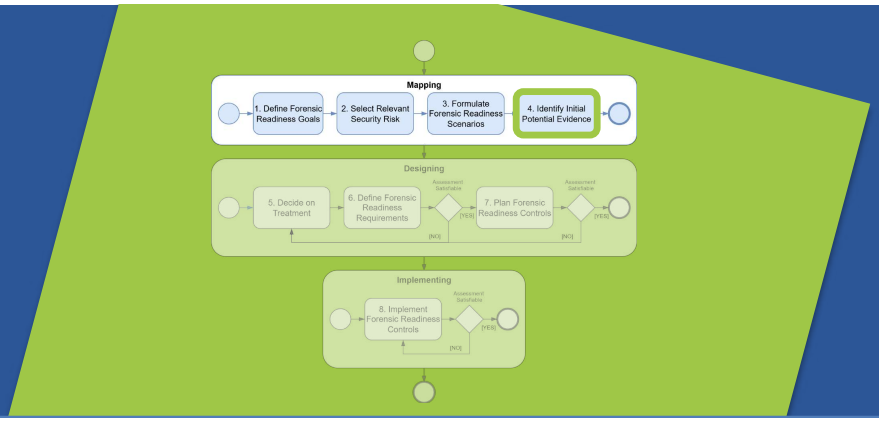


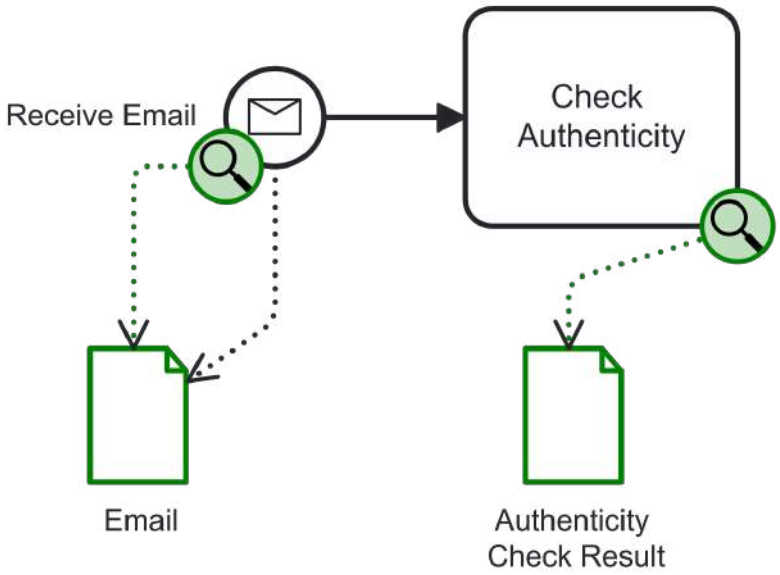
Ensure that investigations of fraudulent invoice payments are possible.





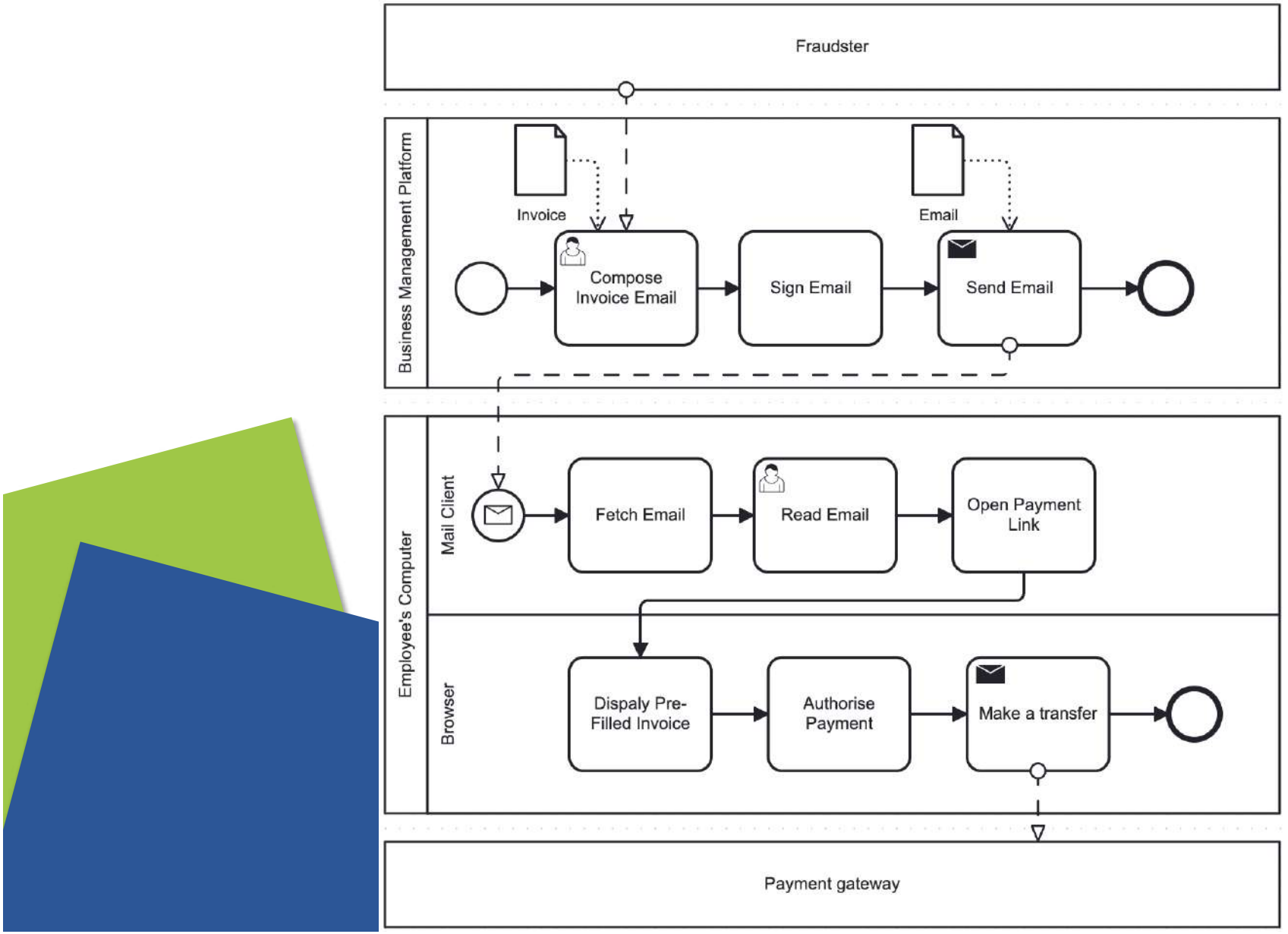
Ensure that investigations of fraudulent invoice payments are possible.

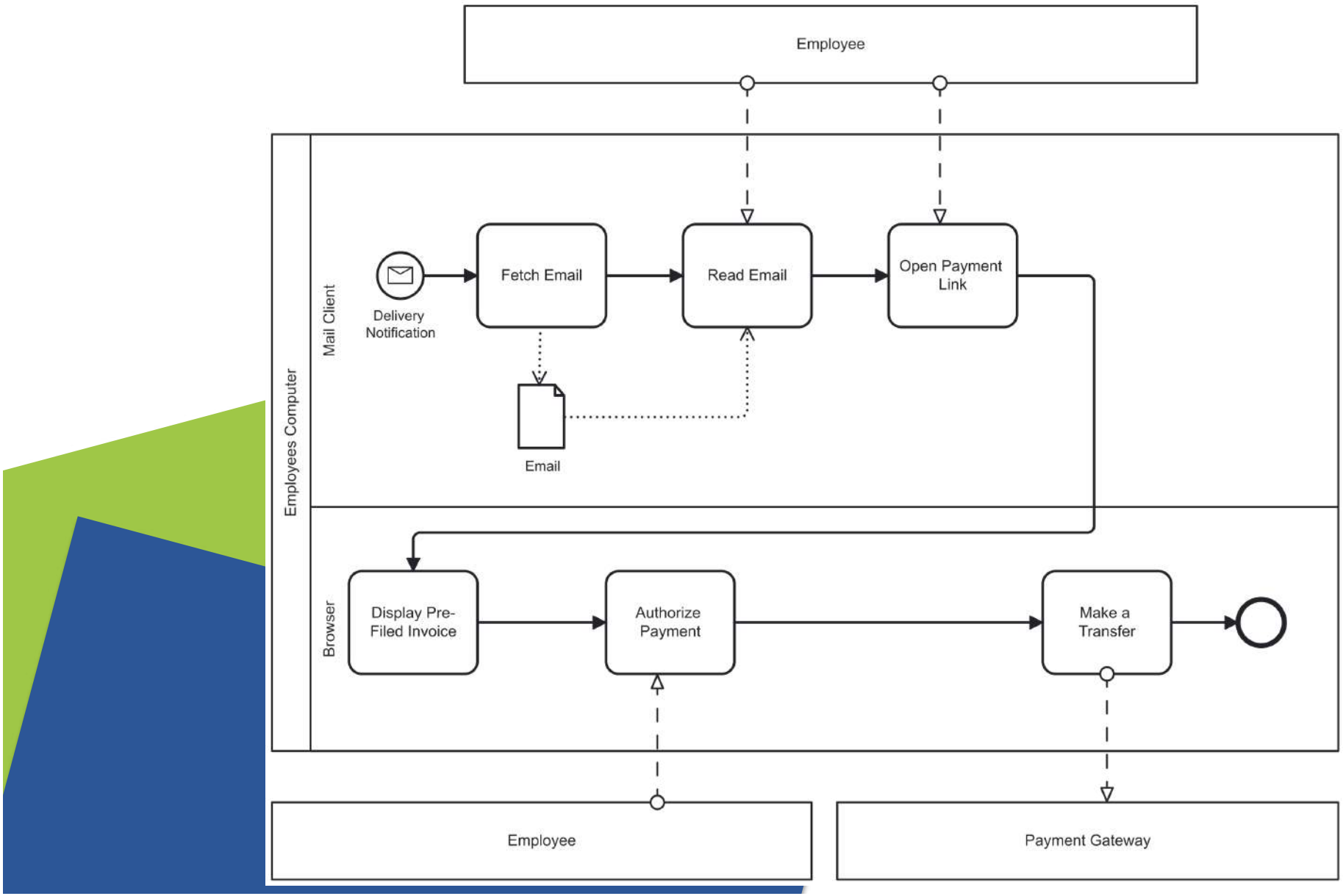




Task: Evidence

- *Given the modelled risks, is there evidence in the system?*
  - *To show what happened*
  - *Allowing to investigate the risk*
- *Mark the existing*
- *Discover new and model them*


Fraudster
Business Management Platform
Invoice
Email
Compose Invoice Email
Sign Email
Send Email
Employee's Computer
Mail Client
Fetch Email
Read Email
Open Payment Link
Browser
Dispaly Pre-Filled Invoice
Authorise Payment
Make a transfer
Payment gateway

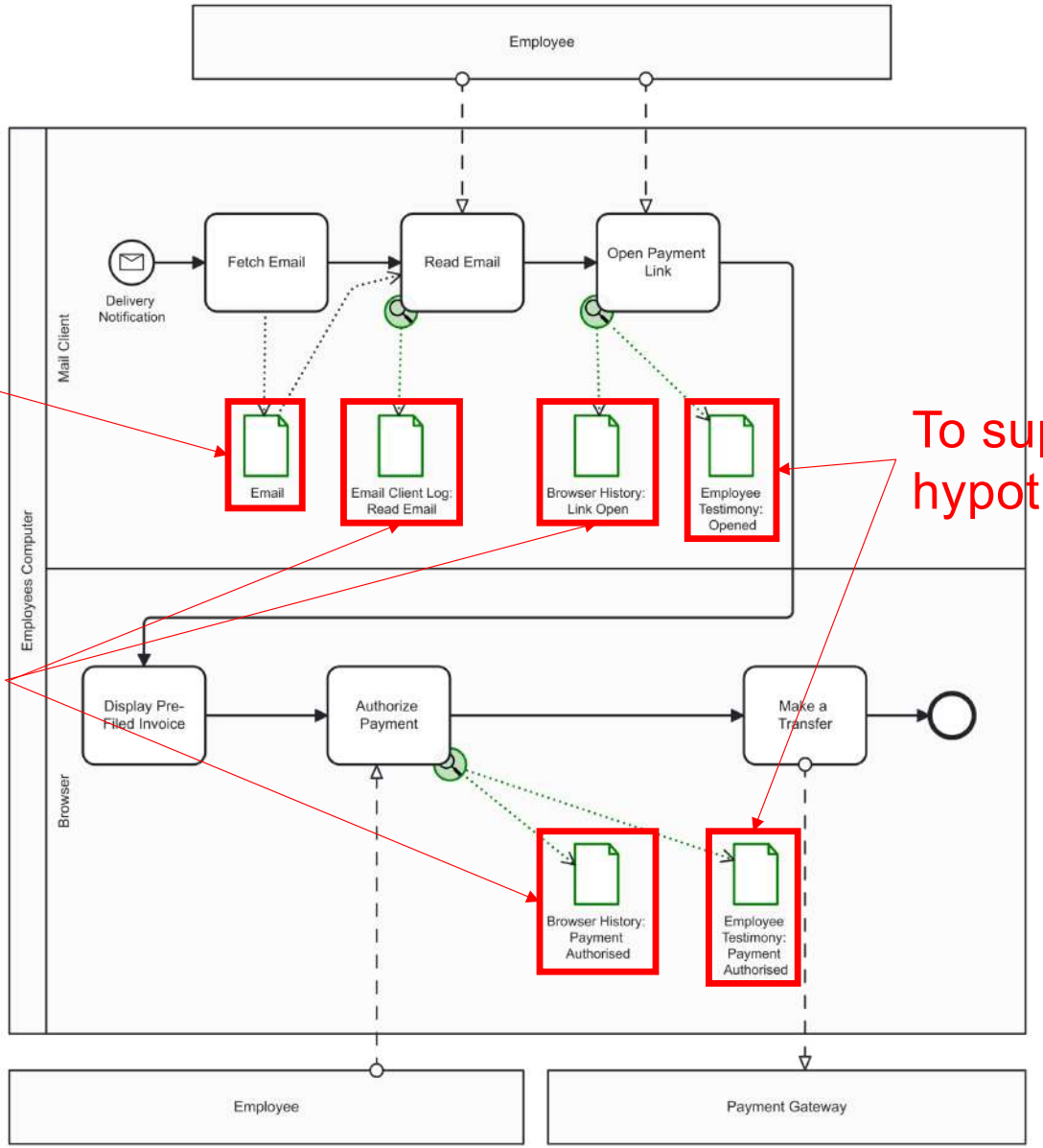

Employee
Employees Computer
Mail Client
Delivery Notification
Fetch Email
Read Email
Open Payment Link
Email
Browser
Display Pre-Filed Invoice
Authorize Payment
Make a Transfer
Employee
Payment Gateway

Task: Evidence

Is evidence itself

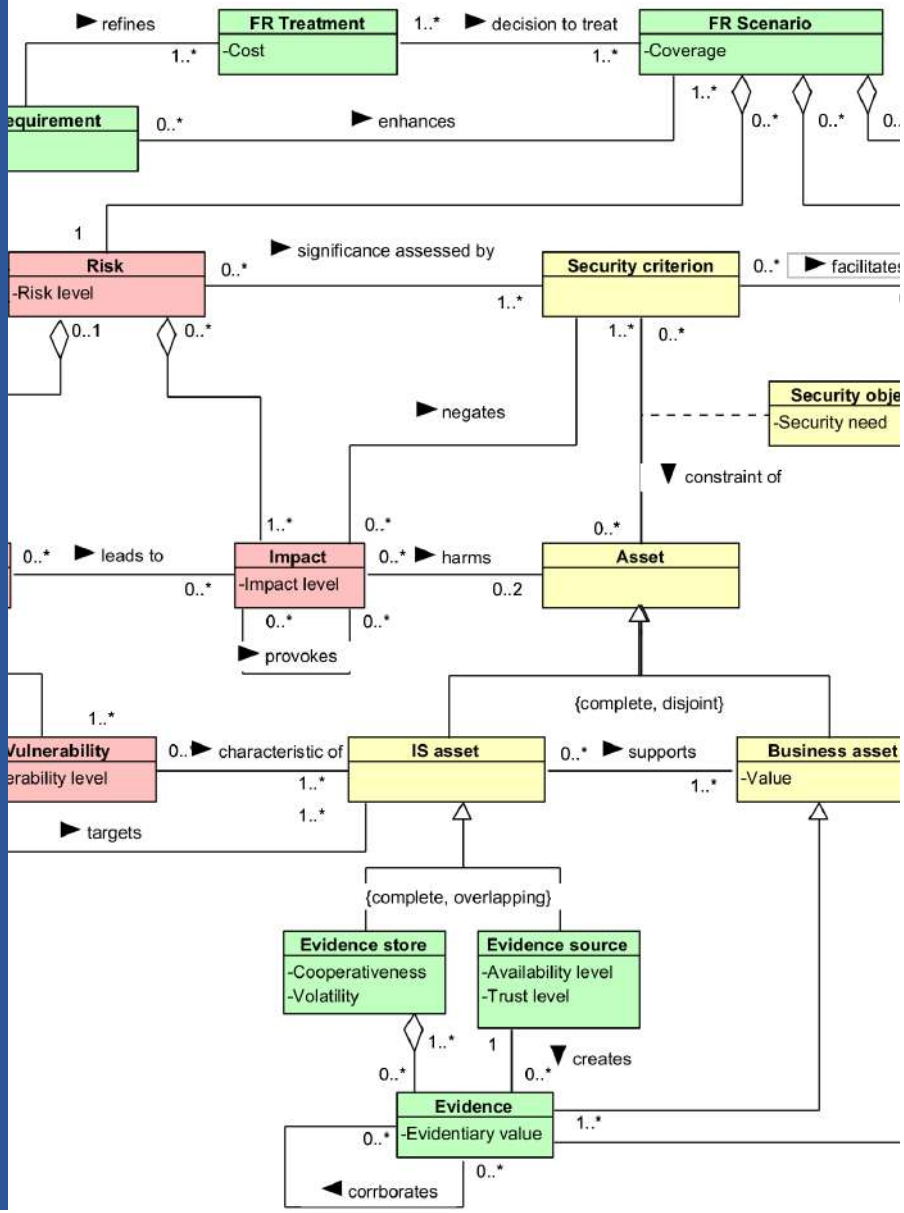
If the employee cooperates

To support a hypothesis



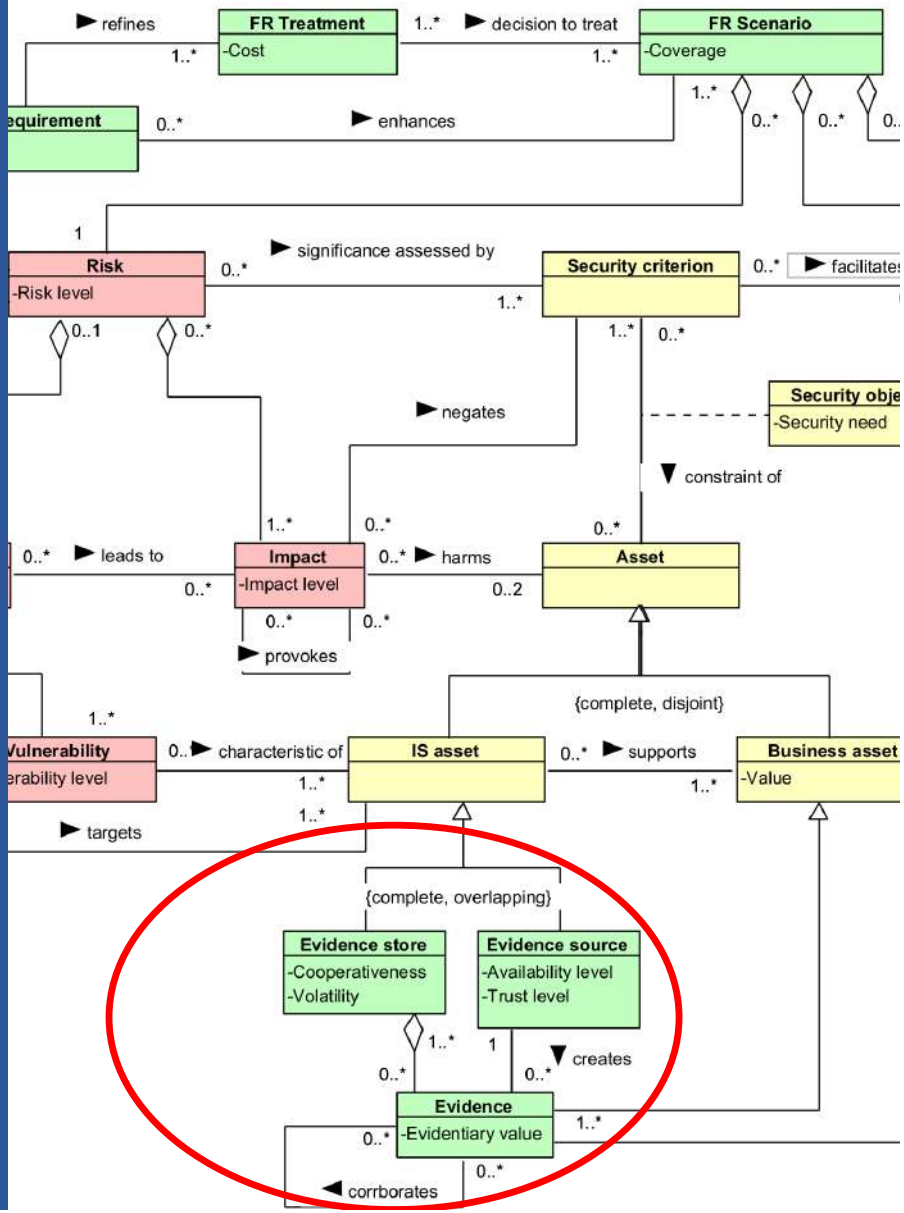
Formalised Evidence

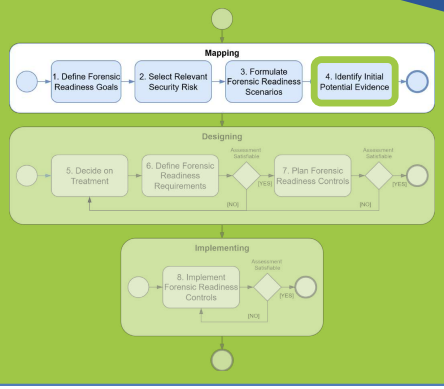
- *Potential Evidence*
  - *Specific and usable data*
- *Evidence Origin (Source)*
  - *Where and when it comes from*
- *Evidence Store*
  - *Where it ends up*
  - *Where it can be found during investigation*



Formalised Evidence

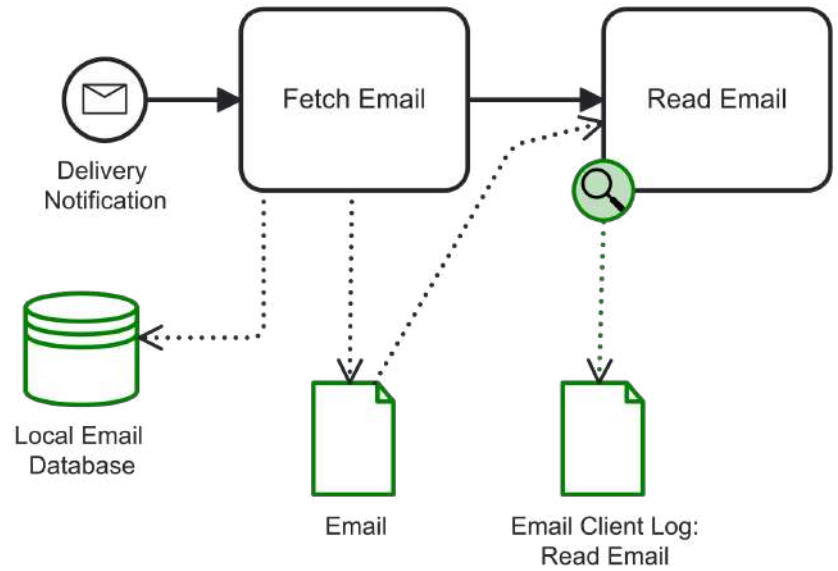
- *Potential Evidence*
  - *Specific and usable data*
- *Evidence Origin (Source)*
  - *Where and when it comes from*
- *Evidence Store*
  - *Where it ends up*
  - *Where it can be found during investigation*





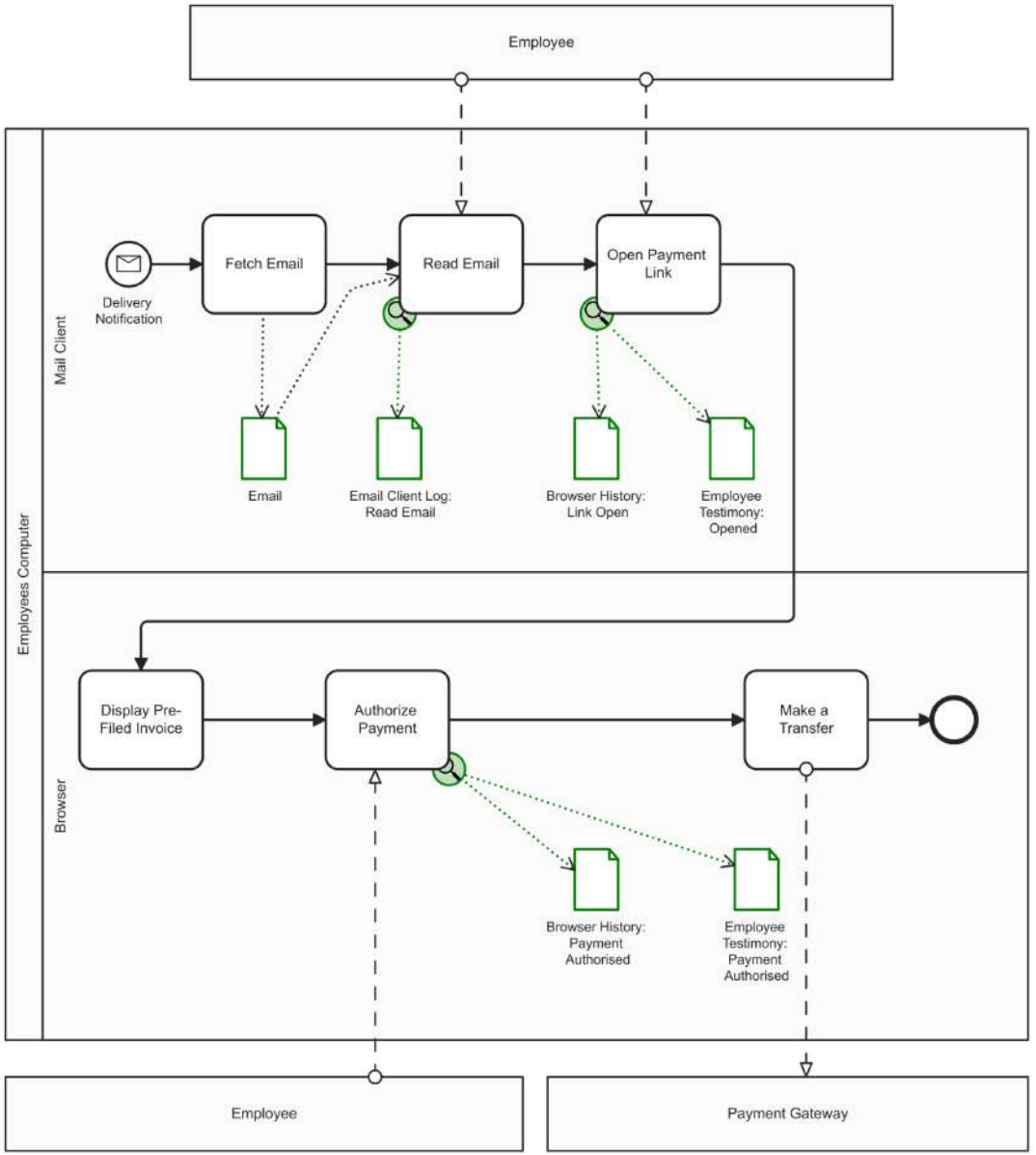
Task: Evidence Store

- *Where is the data stored*
  - *Within the process*
- *Where can it be found afterwards*
  - *Does not need to be connected*
- *Model the stores*

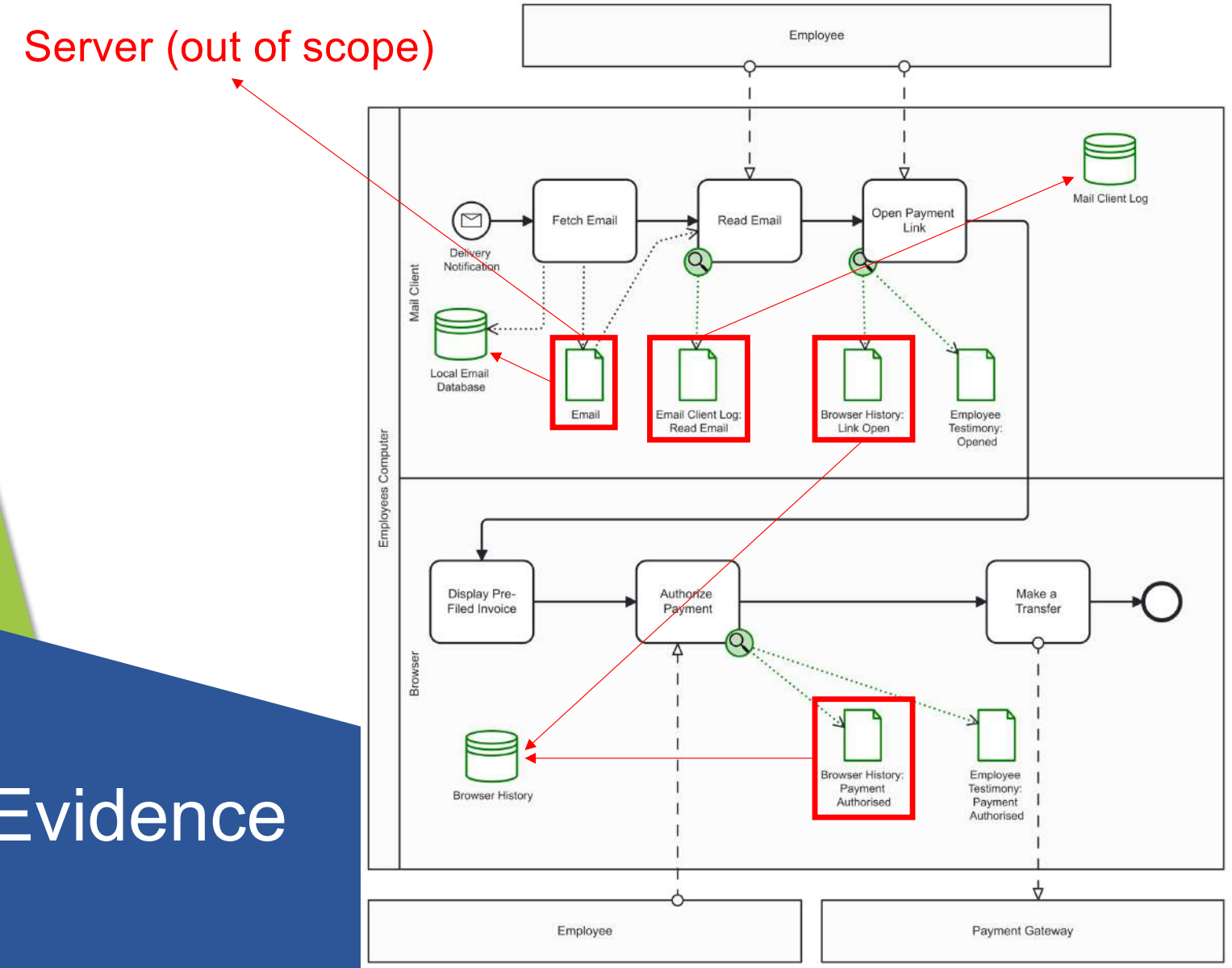


Hint: Click on the Data Store and the green button to mark it

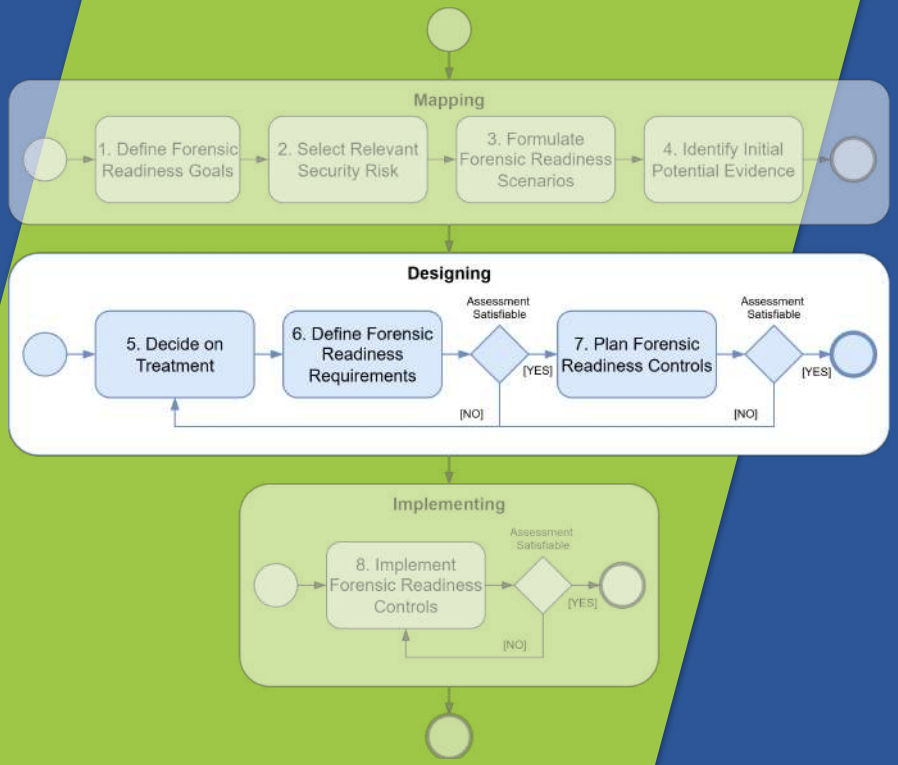
Task: Evidence Store



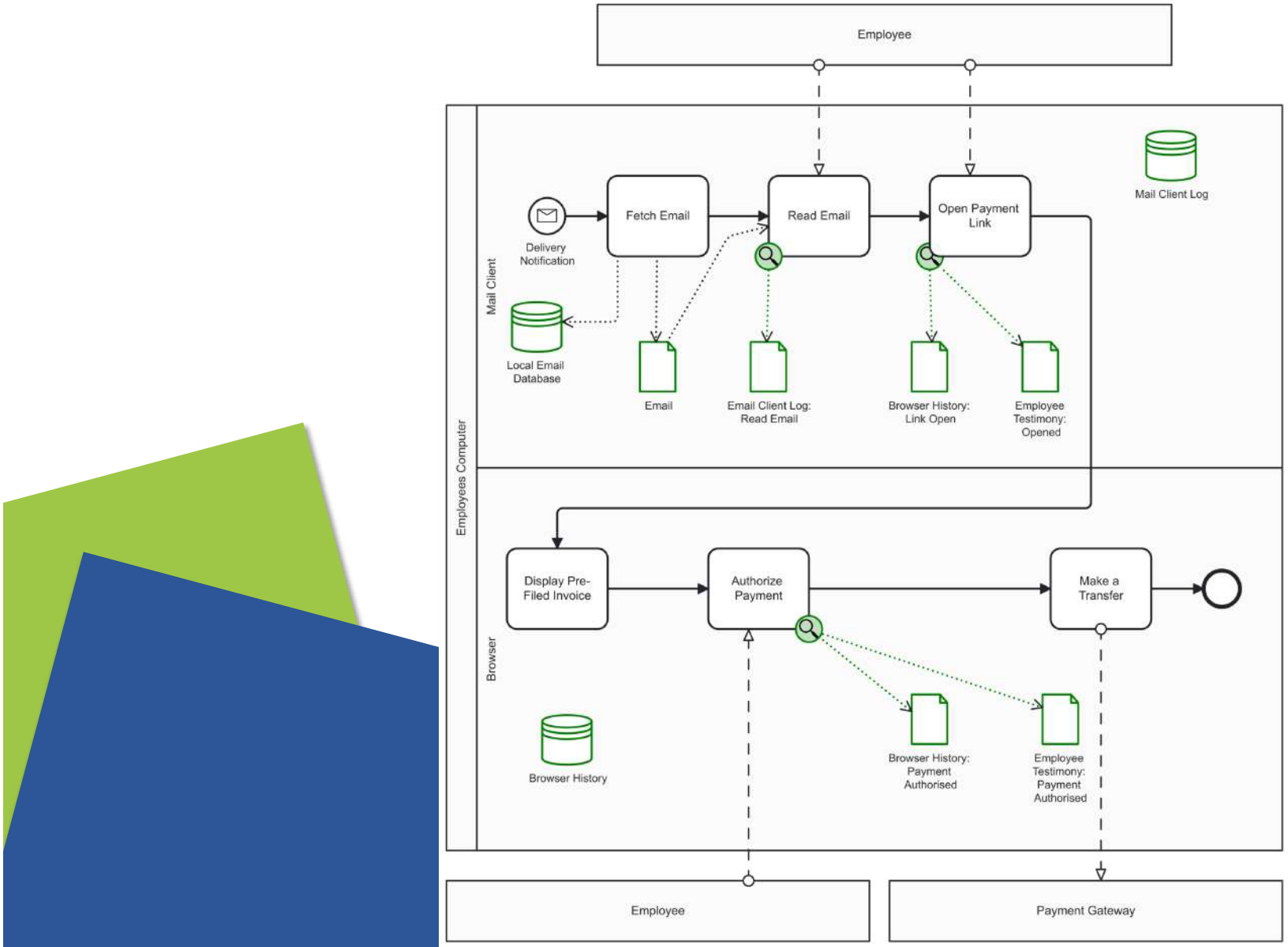
Task: Evidence Store



Task: Scenario Evaluation

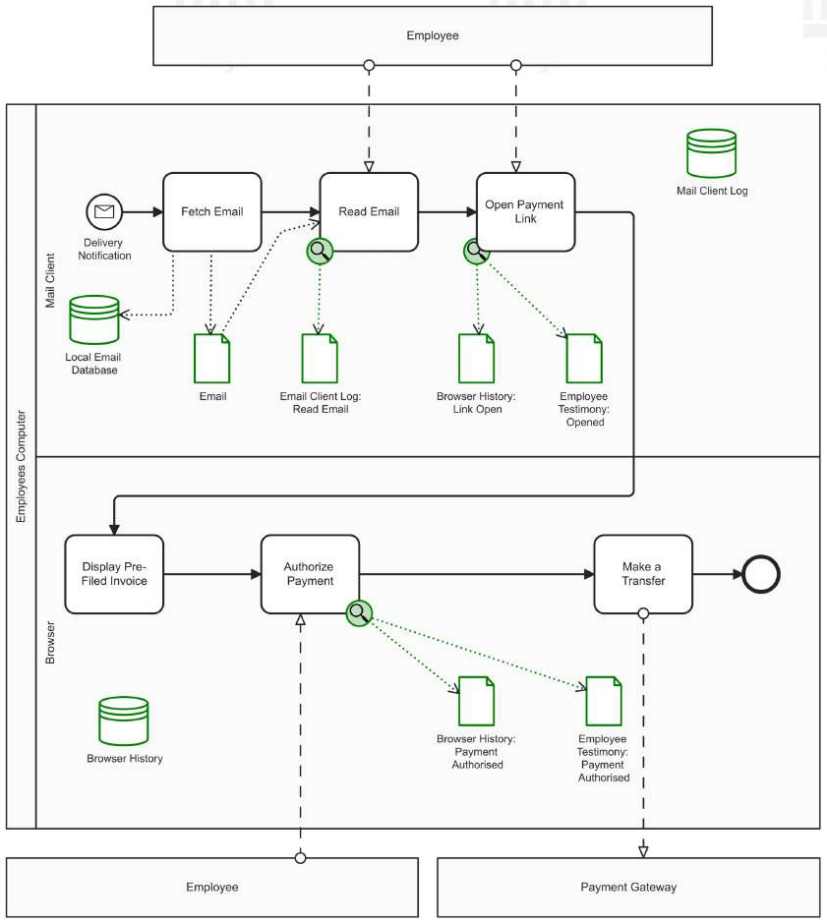


- *Think about the modelled risk*
- *Are there blind spots?*
  - *How could you cover them?*
  - *Is it feasible to cover them?*
- *Are there assumptions?*


Employee
Employees Computer
Mail Client
Delivery Notification
Fetch Email
Read Email
Open Payment Link
Mail Client Log
Local Email Database
Email
Email Client Log: Read Email
Browser History: Link Open
Employee Testimony: Opened
Browser
Display Pre-Filed Invoice
Authorize Payment
Make a Transfer
Browser History
Browser History: Payment Authorised
Employee Testimony: Payment Authorised
Employee
Payment Gateway

Task: Scenario Evaluation

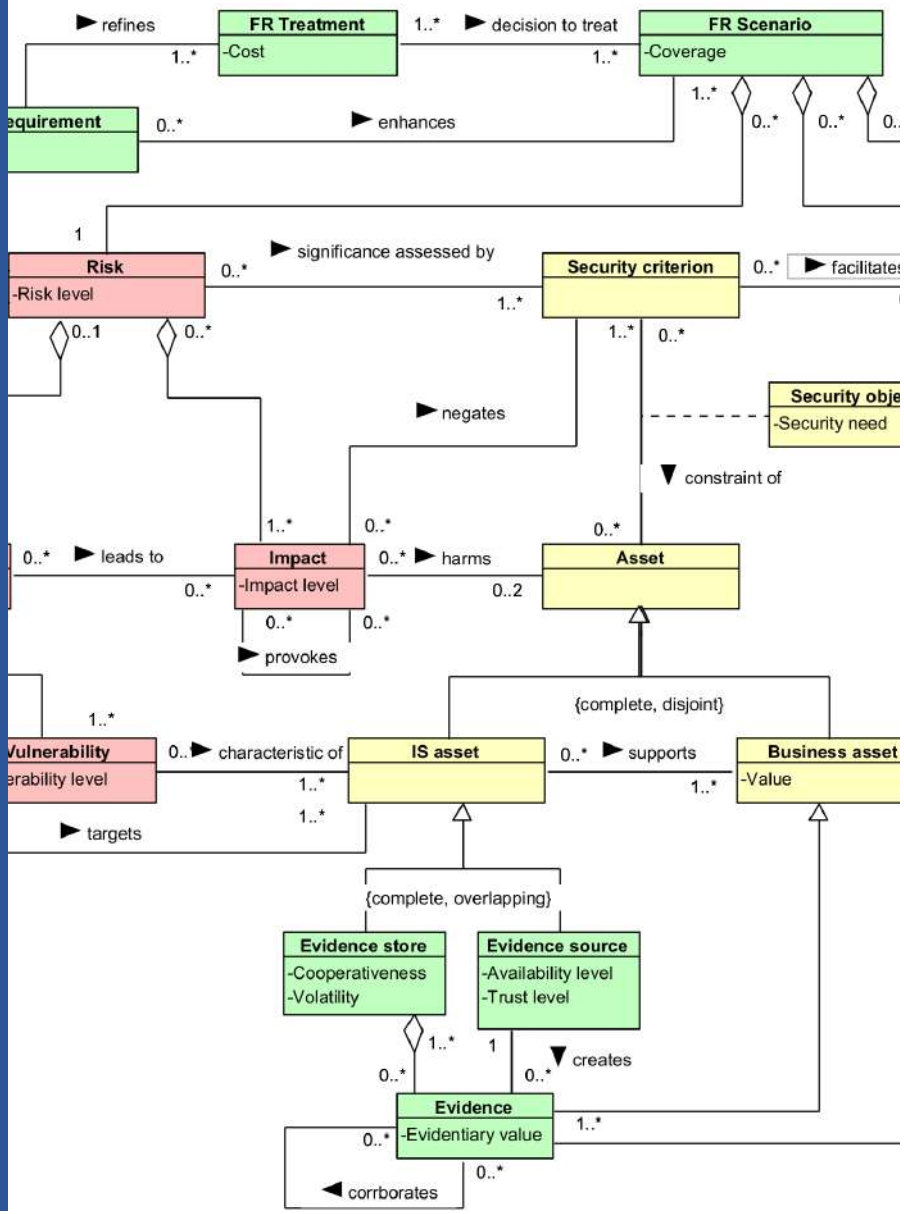
- **Evidence replication**
  - **Remote collection of Mail Client Log**
    - **Mitigates the unwillingness to release**
  - **Collection of network flows/communication**
    - **Partially mitigates the deleted history**



- **Investigation leads**
  - **Is the invoice from that company expected?**
  - **Are there anomalies in the reception?**
    - **(e.g., period does not fit, duplicate invoice)**
  - **Were the sender and the company flagged in the past?**

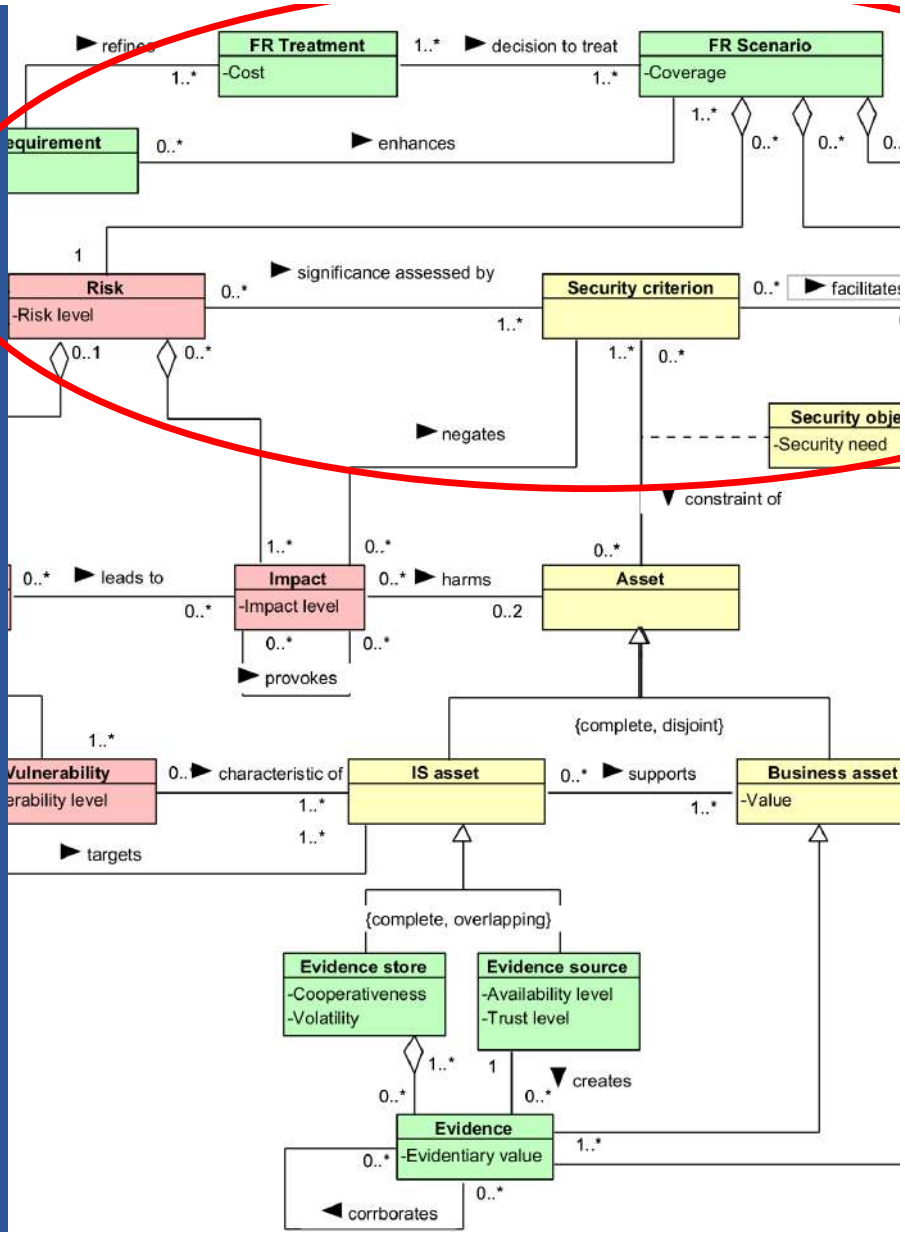
Formalised Scenario

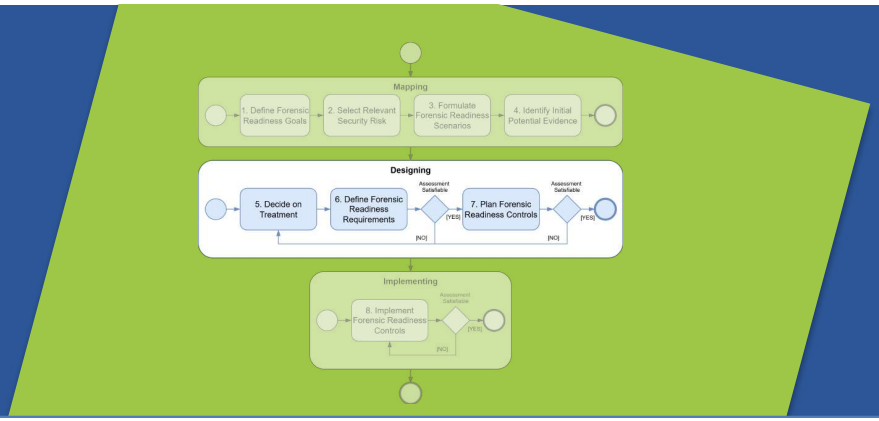
- *Concern – Risk*
  - *Why it is important to care*
- *Aim – Goal*
  - *Why do you care from forensic perspective*
- *Data – Evidence*
  - *What supporting data is available*

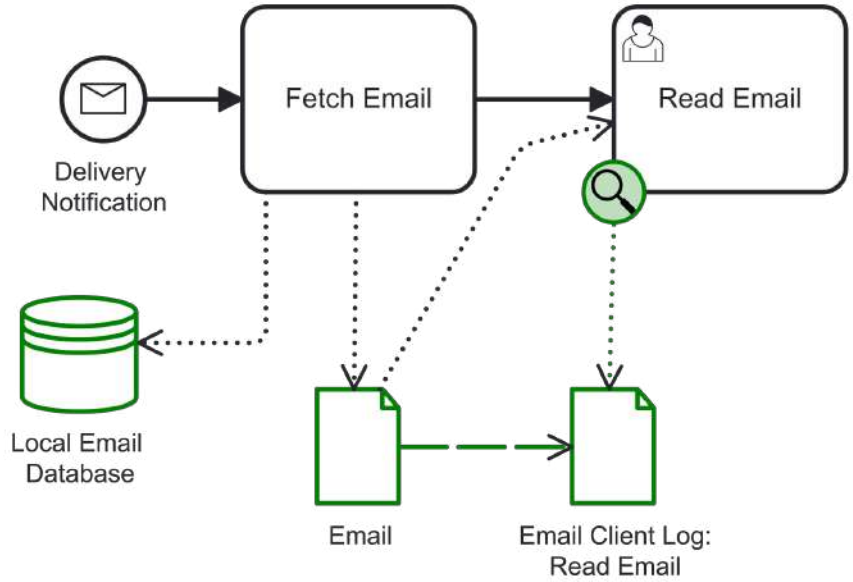


Formalised Scenario

- *Concern – Risk*
  - *Why it is important to care*
- *Aim – Goal*
  - *Why do you care from forensic perspective*
- *Data – Evidence*
  - *What supporting data is available*



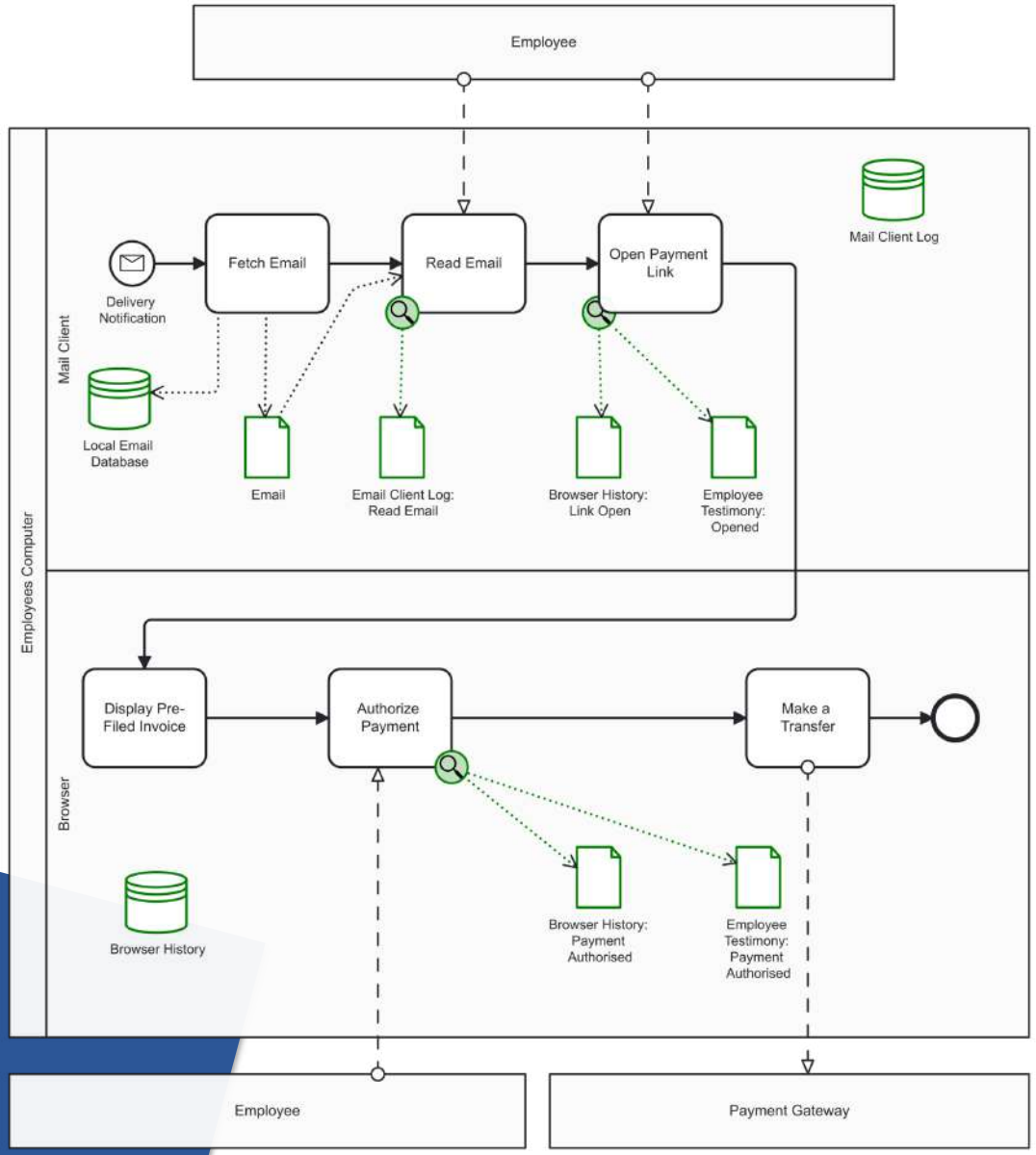




Task: Evidence Relations

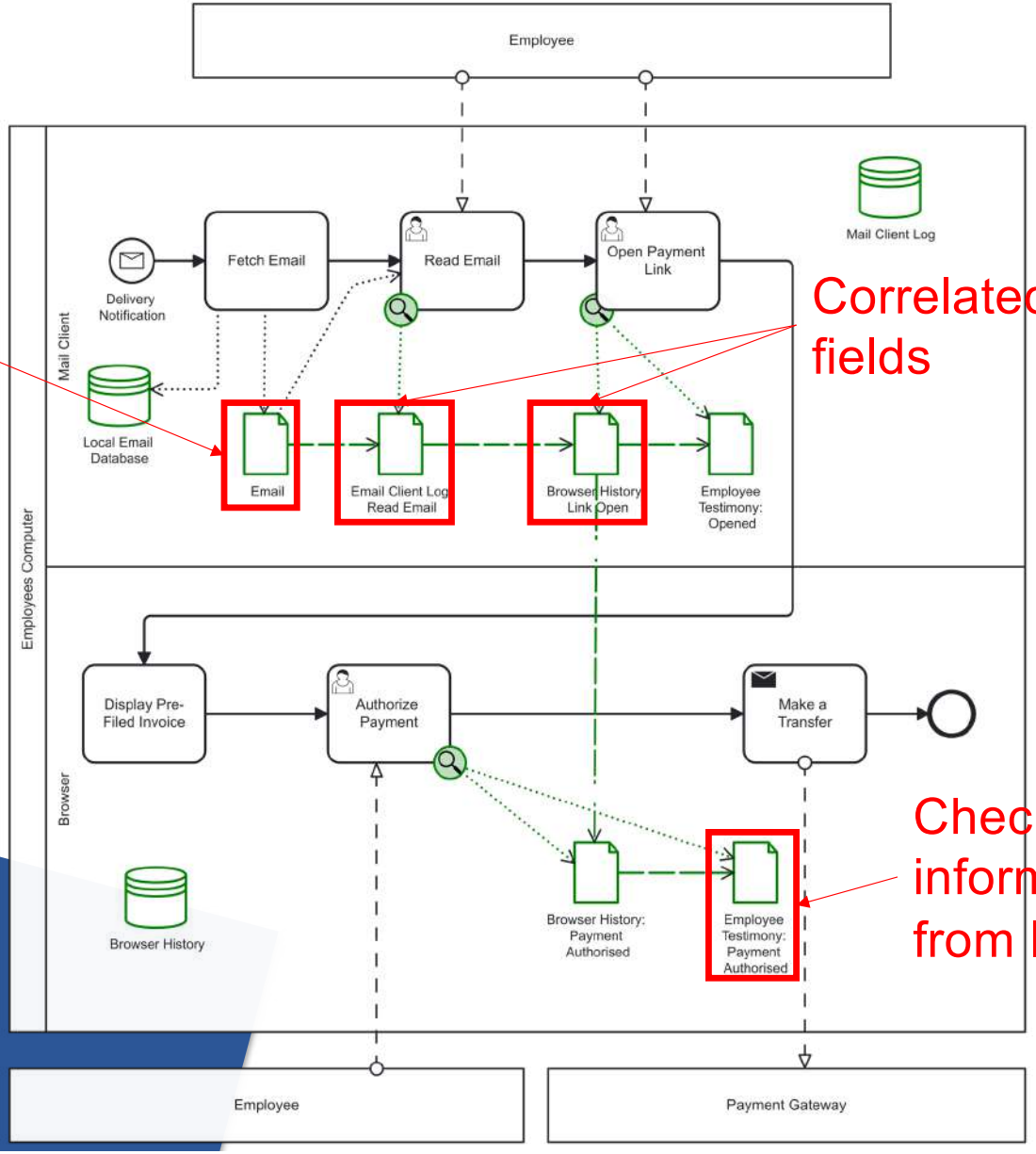
- *Think about related evidence*
  - *Are there some connections?*
  - *Are there reliable dependencies?*
- *Timing*
  - *What comes first?*
- *Model the relations*

Task: Evidence Relations



Task: Evidence Relations

Email comes first



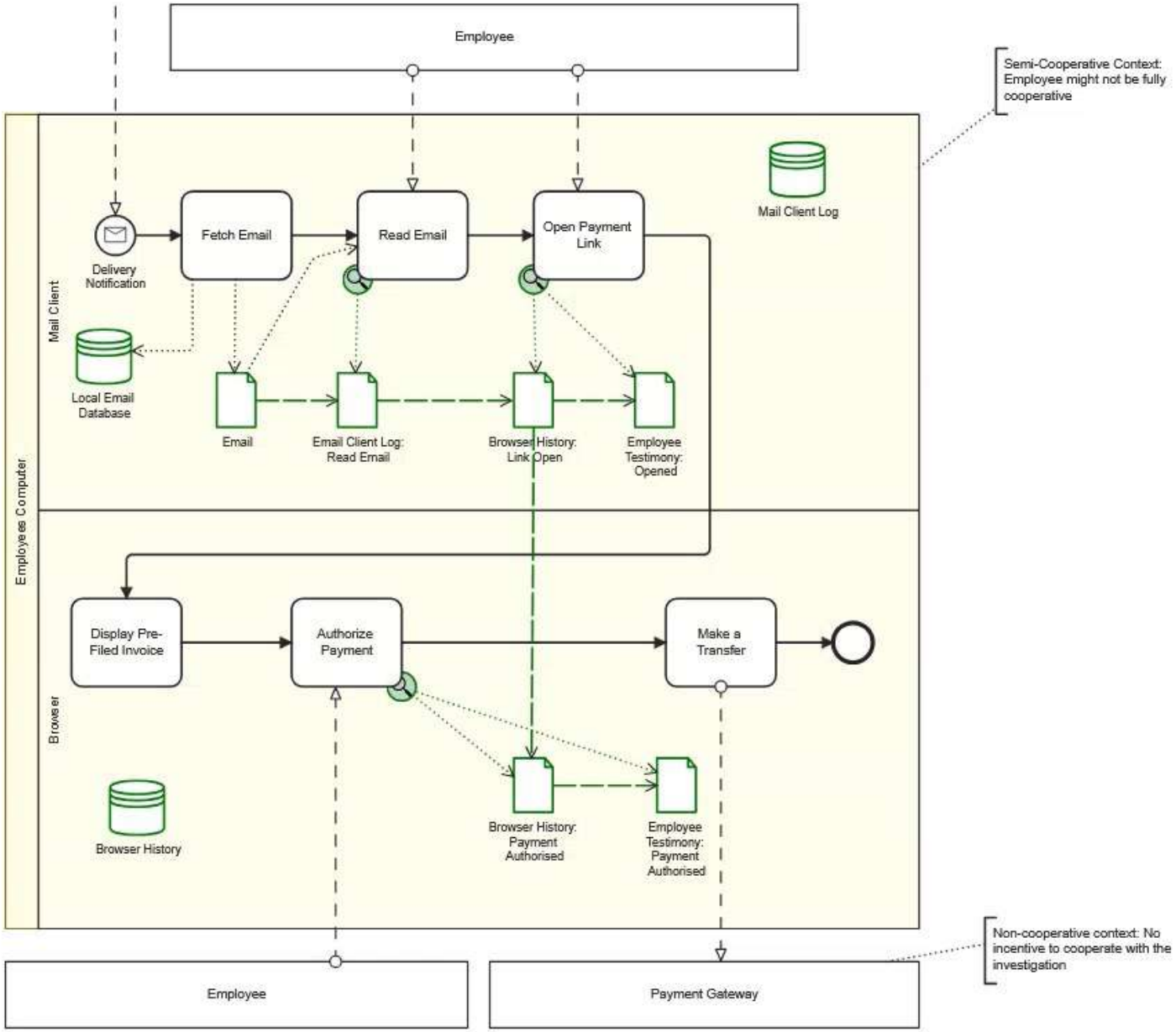
Correlated fields

Checking the information from logs

Model Analysis

FREAS Tool

https://freas.cs.ut.ee/



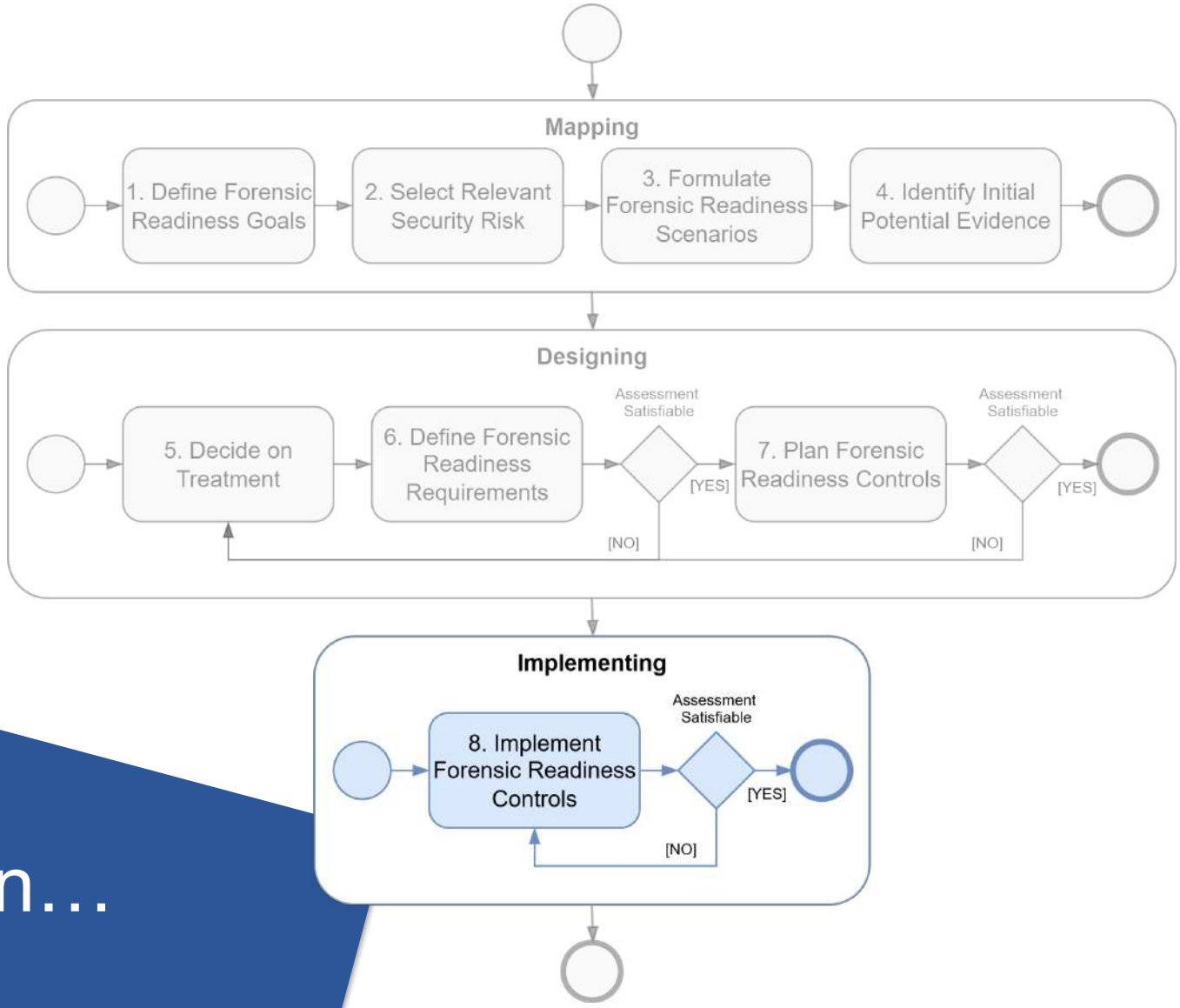
RUN BPMN4FRSS DIAGRAM VALIDATION

Select the analysis type

Validity + Hint

Run validation | Hide overlays

Implementation…



Do you want to know more about

FR-ISSRM Method?

https://frssdesign.github.io/

CHESS

Cyber-security Excellence Hub in Estonia and South Moravia

Funded by the European Union under Grant Agreement No. 101087529. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.