DORA. REPORT

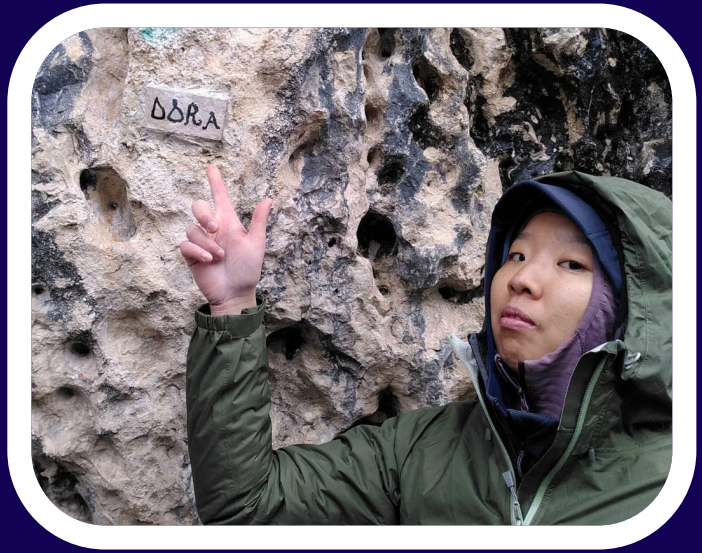
Practical DORA (Digital Operational Resilience Act) for SREs

October 2025

SRE CON_ EUROPE MIDDLE EAST AFRICA

Hello 👋

- Laura Woo
- Co-founder of DORA.report



https://www.ukclimbing.com/logbook/crags/citta_dei_sassi_city_of_rocks-10601/dora-142263

Disclaimer

I am not a lawyer

DORA. REPORT

The relevant bits of DORA for SREs

Incident Management

Digital OpRes

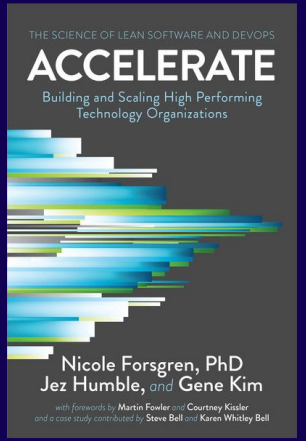
TPP Risk Management

DORA

DORA

DORA. REPORT

DORA



DORA. REPORT

DORA = Digital Operational Resilience Act

DORA. REPORT

➔ Applicable since **Jan 17th 2025**

JAN

DORA Facts ⚡

DORA Facts

- In scope:
  - **20** types of Financial entities
  - Critical 3rd party providers

https://dora.report/blog/who-is-in-scope-for-dora/

DORA Facts ⚡

- Non-compliance
  - “penalties and measures shall be effective, proportionate and dissuasive”
- TPP Non-compliance
  - Up to 1% of of avg. daily global turnover

https://eur-lex.europa.eu/eli/reg/2022/2554/oj (Article 50)
https://eur-lex.europa.eu/eli/reg/2022/2554/oj (Article 35 [8])

DORA. REPORT

1

ICT Risk Management

5 Key Pillars

DORA. REPORT

1

ICT Risk Management

2

Incident Management, Classification, and Reporting

5 Key Pillars

DORA. REPORT

1

ICT Risk Management

2

Incident Management, Classification, and Reporting

3

Digital Operational Resilience Testing

5 Key Pillars

DORA. REPORT

5 Key Pillars

1. ICT Risk Management
2. Incident Management, Classification, and Reporting
3. Digital Operational Resilience Testing
4. Managing ICT Third-Party Risk

DORA. REPORT

5 Key Pillars

1. ICT Risk Management
2. Incident Management, Classification, and Reporting
3. Digital Operational Resilience Testing
4. Managing ICT Third-Party Risk
5. Information Sharing Agreements

DORA. REPORT

5 Key Pillars

DORA. REPORT

Digital OpRes

‘critical or important function’

*means a function, the **disruption** of which would materially impair the financial **performance** of a financial entity, or the **soundness** or **continuity** of its **services** and activities, or the discontinued, defective or failed performance of that function would materially **impair** the continuing **compliance** of a financial entity with the conditions and obligations of its authorisation, or with its other obligations under applicable financial services law;*

- Article 3 (22) , Regulation (EU) 2022/2554

What are the core offerings or processes that if they fail - would severely impact your companies ability to operate or hinder you from meeting your regulatory obligations

Digital OpRes

- Do you know what your Critical or important functions (CIFs) are?
- Which services underpin your CIFs?
- Is the information accessible?

DORA. REPORT

Digital OpRes

CIFs
Test yearly

TPP CIFs
Test periodically

TLPT
Every 3 years

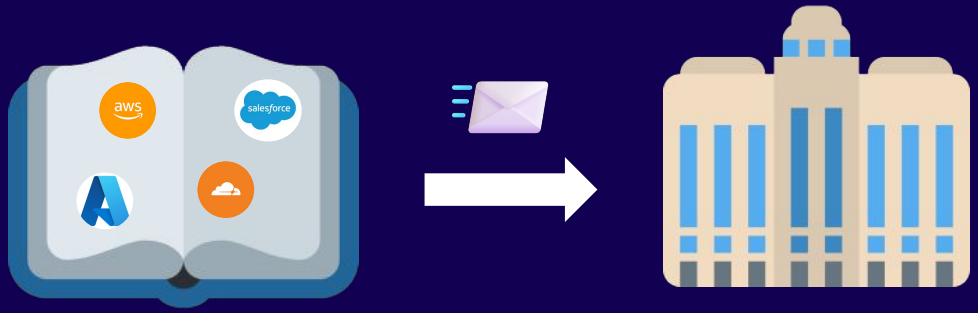
https://eur-lex.europa.eu/eli/reg/2022/2554/oj (Article 24 - 27)

ROI = Register of information

https://eur-lex.europa.eu/eli/reg/2022/2554/oj (Article 28 - 30)

DORA. REPORT

TPP Risk Management



Report yearly to your CA

DORA. REPORT

TPP Risk Management

Onboard a new vendor that underpins critical function

Inform your CA

TPP Risks

Fail or
degrade in quality

Service
disruption

Breach regs / laws =
contract termination

Do you have an exit strategy?

Exit Strategy

Documented

Tested

Reviewed periodically

DORA. REPORT

“Raising incidents became so **complicated** with the addition of DORA requirements that developers are now **scared** to raise incidents.”

- *Fintech Engineering Lead*

DORA. REPORT

Incident Management

Andy

DORA. REPORT

Incident Management

Andy

SRE
Payments Team

DORA. REPORT

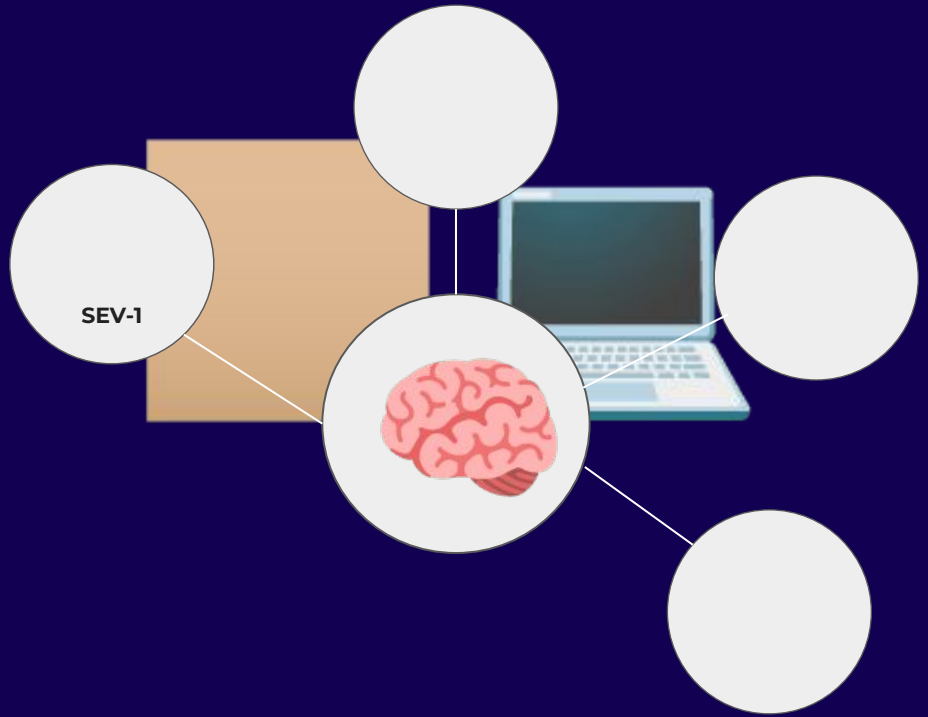
Incident Management

High Priority Alert

Andy is on-call

DORA. REPORT

Incident Management



Andy

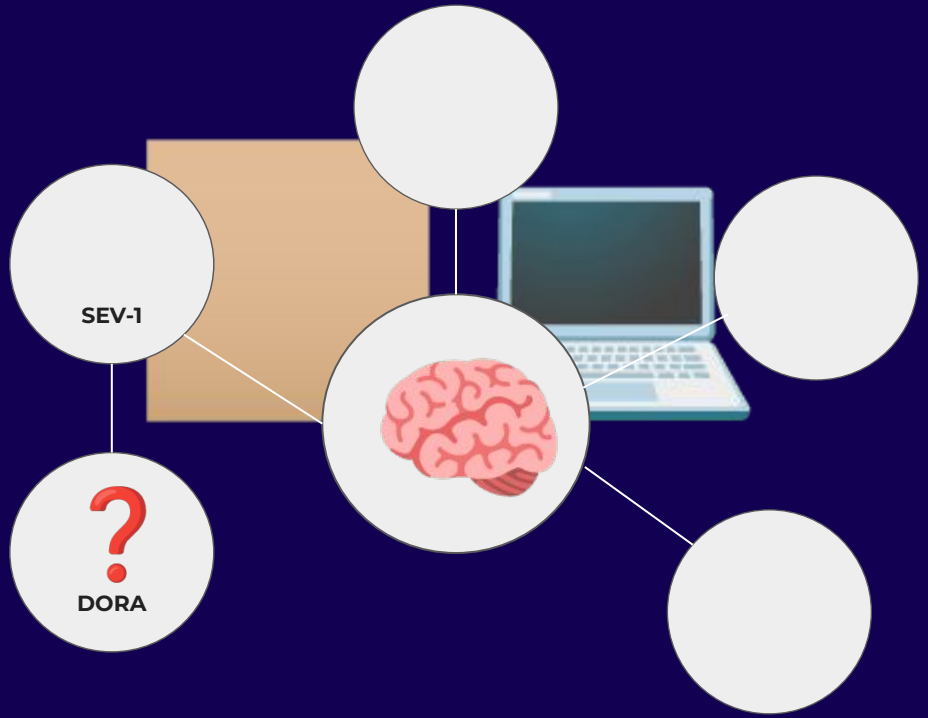
SRE
Payments Team

DORA. REPORT

Incident Management

Andy

SRE
Payments Team

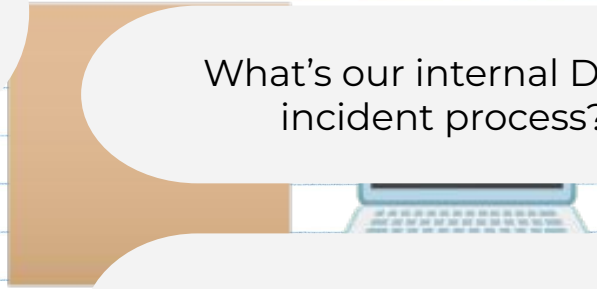


DORA. REPORT

Incident Management

Andy

SRE
Payments Team



What's our internal DORA incident process?

What's the DORA incident classification?

Is this a recurring incident that's considered DORA Major?

DORA. REPORT

Does the incident originate from a TPP? If so, does aggregate reporting apply?

What are the DORA reporting timelines?

Andy

SRE
Payments Team

DORA. REPORT

Incident Management

What's our internal DORA incident process?

DORA. REPORT

Incident Management

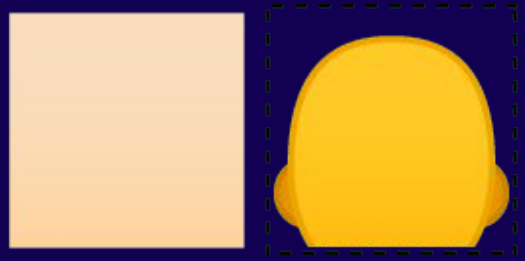
Roles and Responsibilities ?

Jane

Compliance

Fred

Security Operations



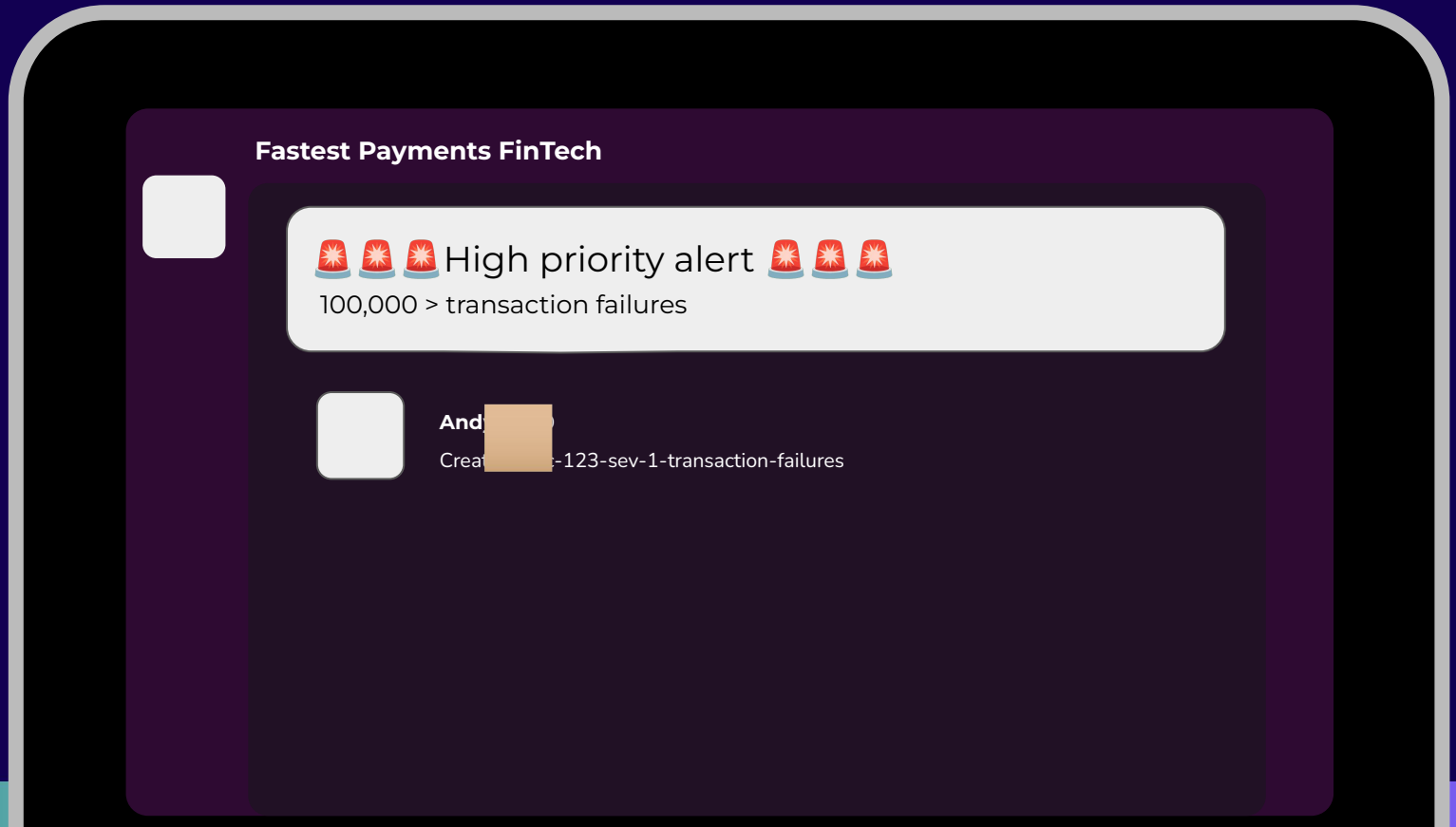
Amy

Senior Management Stakeholder

✉️

DORA. REPORT

Incident Management



DORA. REPORT

Incident Management

What's the DORA incident classification?

🔥 Major

🕯️ Minor

Re-classified

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1772 (Chapter 2)

DORA. REPORT

Incident Management

🔥 Major

Does the incident impact CIFs?

DORA. REPORT

Incident Management

🔥 Major

Does the incident impact CIFs?

Criteria A

Incident affects ICT services or network and information systems that support critical or important functions

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1772

DORA. REPORT

Incident Management

🔥 Major

Does the incident impact CIFs?

Criteria A

Incident affects ICT services or network and information systems that support critical or important functions

||

Criteria B

Incident affects financial services that require authorisation, registration or are otherwise supervised by CA’s

DORA. REPORT

Incident Management

🔥 Major

Does the incident impact CIFs?

Criteria A

Incident affects ICT services or network and information systems that support critical or important functions

Criteria B

Incident affects financial services that require authorisation, registration or are otherwise supervised by CA's

Criteria C

Incident represents a successful, malicious and unauthorised access to the network and information systems

DORA. REPORT

Incident Management

🔥 Major

Does the incident impact CIFs?

Criteria A

Incident affects ICT services or network and information systems that support critical or important functions

=

Criteria B

Incident affects financial services that require authorisation, registration or are otherwise supervised by CA's

=

Criteria C

Incident represents a successful malicious and unauthorised access to the network and information systems

DORA. REPORT

Incident Management

🔥 Major ✔

Does the incident impact CIFs?

Criteria A

Incident affects ICT services or network and information systems that support critical or important functions

X

=

Criteria B

Incident affects financial services that require authorisation, registration or are otherwise supervised by CA's

X

=

Criteria C

Incident represents a successful, malicious and unauthorised access to the network and information systems

✔

DORA. REPORT

Incident Management

🔥 Major

Does the incident impact CIFs?

Criteria A

Incident affects ICT services or network and information systems that support critical or important functions

=

Criteria B

Incident affects financial services that require authorisation, registration or are otherwise supervised by CA's

Other classification criteria...

DORA. REPORT

Incident Management

🔥 Major

Other classification criteria...

Criteria 1

Reputational Impact

Criteria 3

Geographical Spread

Criteria 5

Economic Impact

Criteria 2

Duration and service downtime

Criteria 4

Data losses

Criteria 6

Clients, financial counterparts and transactions

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1772

DORA. REPORT

Incident Management

🔥 Major

Criteria 1

Reputational Impact

***At least 1**

Reflected in the media

Repetitive complaints

Won't meet Reg requirements

Lose clients

DORA. REPORT

Incident Management

🔥 Major

Criteria 2

Duration and service downtime

Duration
when the incident occurs -> resolved

Service downtime
service is fully or partially unavailable -> regular activities/operations restored to levels prior to incident

DORA. REPORT

Incident Management

🔥 Major

Criteria 2

Duration and service downtime

Duration > 24 hours

Service downtime > 2 hours
(services that underpin CIFs)

DORA. REPORT

Incident Management

🔥 Major

Criteria 3

Geographical Spread

≥ 2 member states impacted

DORA. REPORT

Incident Management

🔥 Major

Criteria 4

Data losses

***Any are fulfilled**

- ➔ Incident has rendered the data unavailable - temporarily or permanently
- ➔ Incident has compromised the trustworthiness of the data
- ➔ Incident has resulted in inaccurate or incomplete data - unauthorised modification
- ➔ Incident has resulted in data being accessed by or disclosed to unauthorised party or system

DORA. REPORT

Incident Management

🔥 Major

Criteria 5

Economic Impact

Costs and losses due to incident > 100,000 euros

DORA. REPORT

Incident Management

🔥 Major

Criteria 6

Clients, financial counterparts and transactions

***Any are fulfilled**

- Affected **clients > 10%** of all clients using impacted service
- Affected **clients** using impacted service **> 100,000**
- Affected financial counterparts **> 30%** of **financial counterparts** that use the affected service
- Affected **transactions > 10%** of avg. daily **number** of transactions
- Affected **transactions > 10%** of avg. daily **value** of transactions
- Affected ‘relevant’ clients / financial counterparts

DORA. REPORT

Incident Management

🔥 Major

Criteria 6

Clients, financial counterparts and transactions

Transactions

You need to account for all affected transactions that involve a monetary amount where **at least 1 part** of the transaction is carried out in the **EU**

DORA. REPORT

Incident Management

🔥 Major ✅

Other classification criteria...

Criteria 1

Reputational Impact

Criteria 3

Criteria 5

Economic Impact

≥ 2 Additional criteria are met == DORA 🔥 **Major**

Criteria 2

Duration and service downtime

Criteria 4

Data losses

Criteria 6

Clients, financial counterparts and transactions

DORA. REPORT

Incident Management

🔥 Major

Is this a recurring incident that's considered DORA Major?

1 DORA 🔥 Major Incident

Incidents have occured at least **2x** within **6 months** ✔

Incidents have **same** apparent **root cause** ✔

Incidents collectively meet **Major incident criteria** ✔

DORA. REPORT

Incident Management

🔥 Major

Is this a recurring incident that's considered DORA Major?

*expect FE's to review recurring incidents on monthly basis

1 DORA 🔥 Major Incident

Incidents have occured at least **2x** within **6 months** ✔

Incidents have **same** apparent **root cause** ✔

Incidents collectively meet **Major incident criteria** ✔

DORA. REPORT

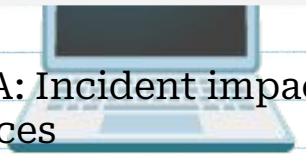
Incident Management

Andy

SRE
Payments Team

DORA

What's the DORA incident classification?



- Meets Criteria A: Incident impacts a number of critical services

DORA. REPORT

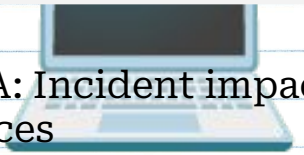
Incident Management

Andy

SRE
Payments Team

❓
DORA

What's the DORA incident classification?



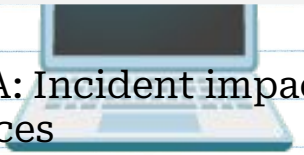
- Meets Criteria A: Incident impacts a number of critical services
- Meets additional criteria:
  - Criteria 3: Geographical spread
    - 🇩🇪🇫🇷

Andy

SRE
Payments Team

❓
DORA

What's the DORA incident classification?



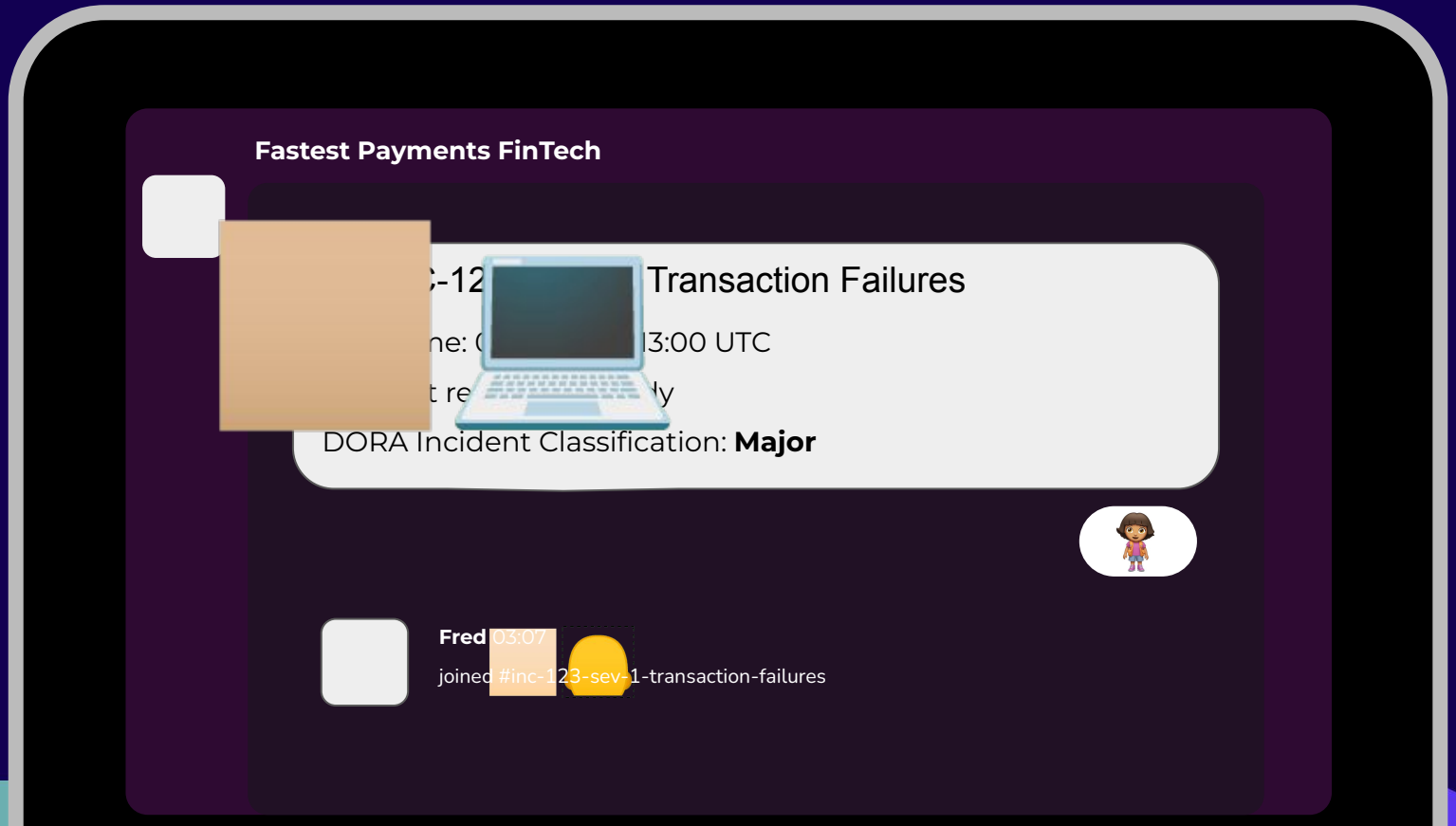
- Meets Criteria A: Incident impacts a number of critical services
- Meets additional criteria:
  - Criteria 3: Geographical spread
    - 🇩🇪🇫🇷
  - Criteria 6: Clients, financial counterparts and transactions
    - > 10% of clients impacted
    - > 10% of daily average number of transactions impacted

DORA. REPORT

Incident Management

Andy

SRE
Payments Team



DORA. REPORT

Incident Management

Recover services

Page Customer Support

Andy

SRE
Payments Team

Fred

Security Operations

DORA. REPORT

Incident Management

Priority

Recover services

Page Customer Support ?

Andy

SRE
Payments Team

Fred

Security Operations

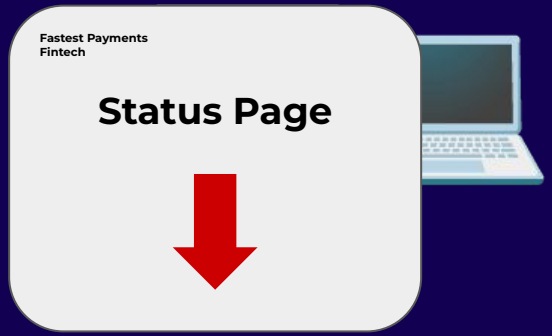
DORA. REPORT

Incident Management

Who is responsible for crisis communication?

Andy

SRE
Payments Team



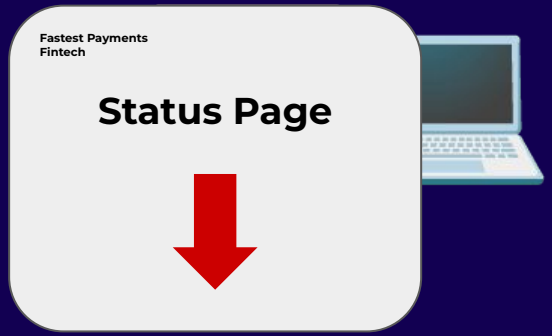
https://eur-lex.europa.eu/eli/reg/2022/2554/oj (Article 14)

Incident Management

Who is responsible for crisis communication?

Andy

SRE
Payments Team



Customer Support

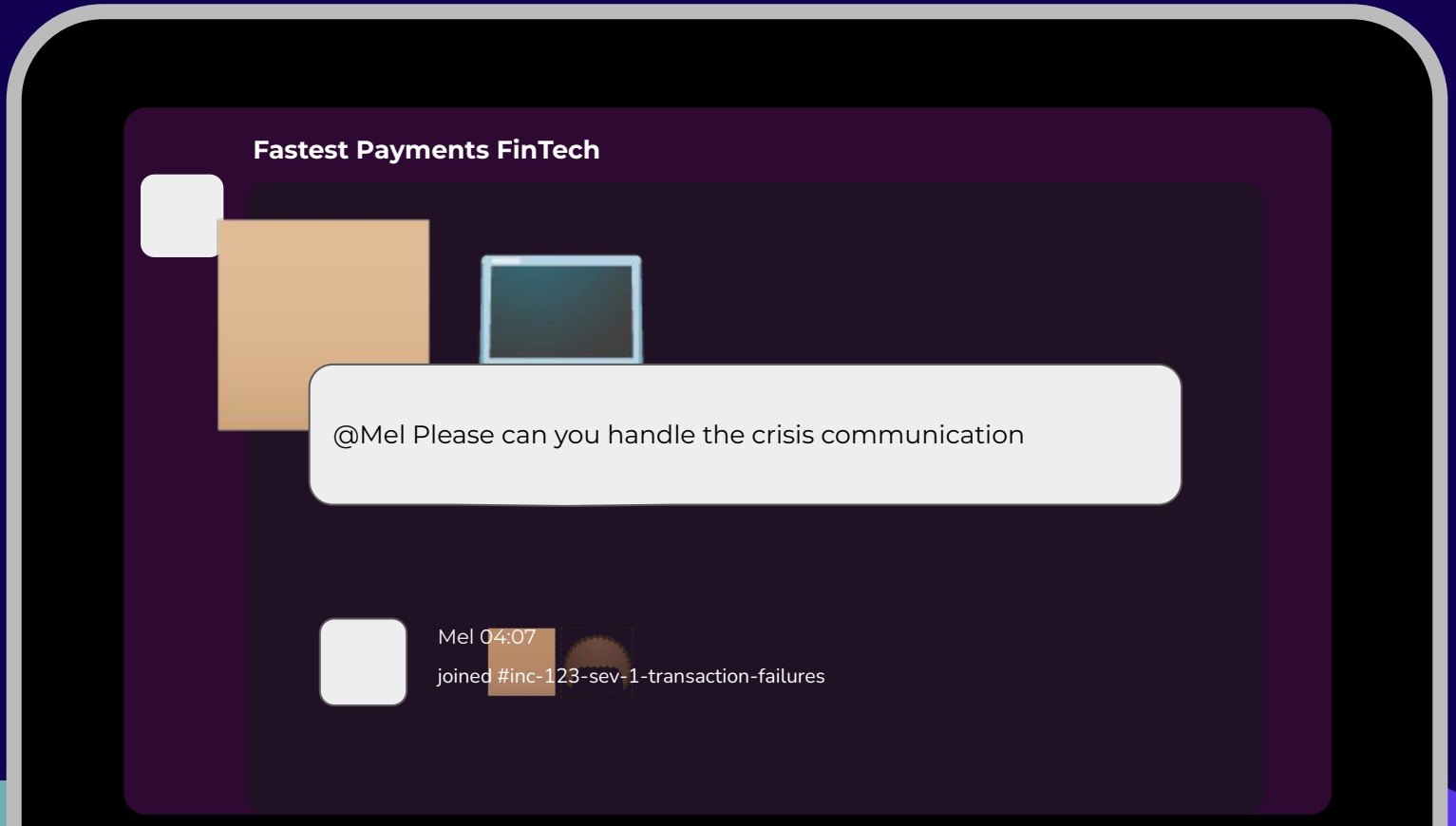
Inform end customers

Inform Financial Counterparts

Media

DORA. REPORT

Incident Management



Andy

SRE
Payments Team

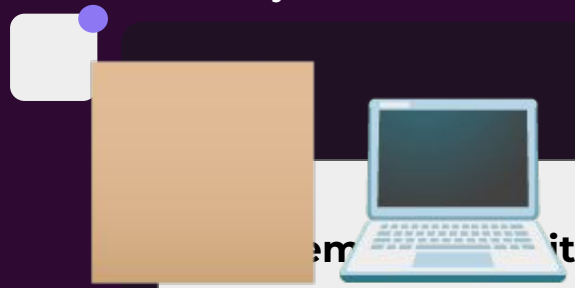
DORA. REPORT

Incident Management

Andy

SRE
Payments Team

Fastest Payments FinTech



em itial Notification due

Incident responder: **@Andy**

DORA Incident Classification: **Major**

Incident: **INC-123 SEV-1 Transaction Failures**

DORA. REPORT

Incident Management

Who is responsible DORA reporting?

Andy

SRE

Jane

Compliance

Competent Authority

DORA. REPORT

Incident Management

You need to submit **3 reports** for DORA Major incidents

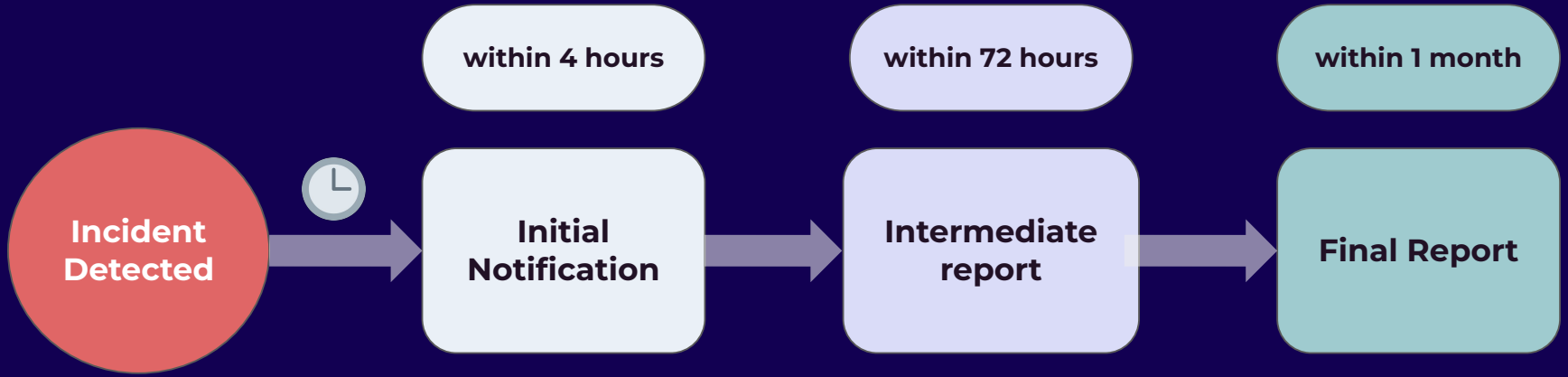
Initial Notification

Intermediate Report

Final Report

DORA. REPORT

Incident Management



https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32025R0301

DORA. REPORT

Incident Management

Weekends and bank holidays

Time limits fall on weekends / bank hols

Submit at Noon the next working day

Except ...

- Credit Institution
- Trading venue operator
- Central Counterparties
- ‘Essential’ or ‘Important’ FE

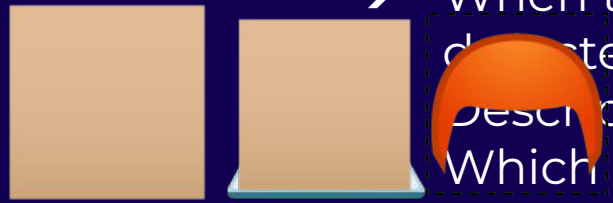
Except ...

- Credit Institution
- Trading venue operator
- Central Counterparties
- ‘Essential’ or ‘Important’ FE

Do you have coverage over the weekend and bank hols?

Initial Notification

- CAs want to receive info about Major Incidents asap
- Contents
  - Significant info
    - ➔ When the incident was d[illegible]ted
    - ➔ Description of the incident
    - ➔ Which member states are impacted
  - etc.



Andy
SRE

Jane
Compliance

DORA. REPORT

Incident Management

Intermediate Report

Jane

Compliance

- Contents
  - More detailed info
    - ➔ When services are recovered
    - ➔ Affected infra supporting business processes
    - ➔ Measures taken to recover from the incident
- Submit updated intermediate report when activities have been recovered
- Collaborative effort

DORA. REPORT

Incident Management

Final Report

Jane
Compliance

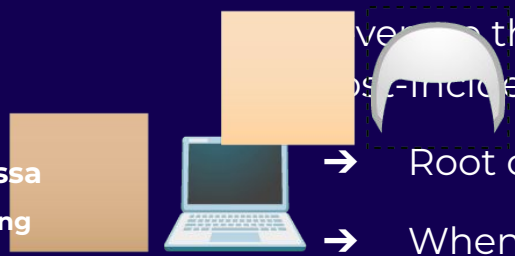
Anna
Product Eng

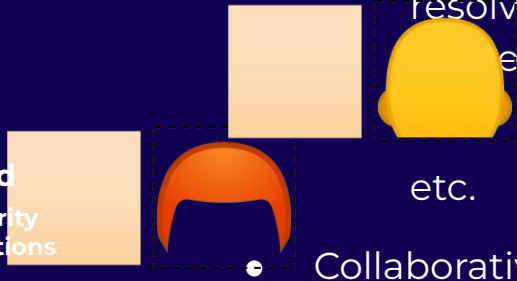
Vanessa
Data Eng

Andy
SRE

Fred
Security Operations

George
Finance





ve the content from your
st-incident report

➔ Root cause analysis

➔ When the incident was resolved and root causes
essed
about the resolution

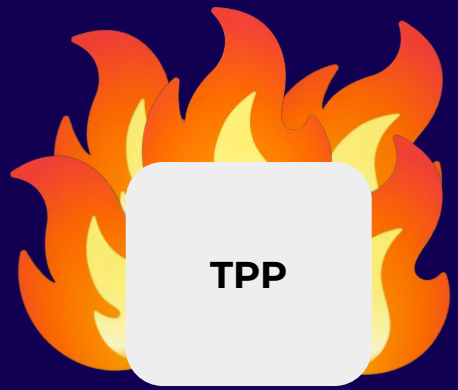
etc.

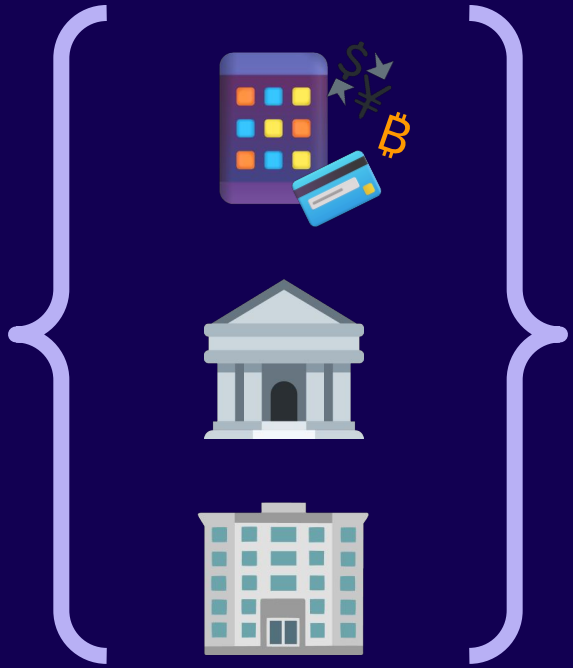
Collaborative effort

DORA. REPORT

Incident Management

Aggregated reporting





https://eur-lex.europa.eu/eli/reg_impl/2025/302/oj/eng (Article 7)

DORA. REPORT

“DORA incident management is easy to follow and I’m comfortable raising incidents”

Thank you