

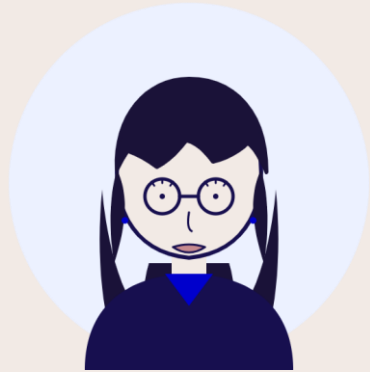
GOVERNANCE, RISK & COMPLIANCE

From *Heat Maps to Decisions*: GRC as a Strategic Management Tool

Peter Trier Jørgensen

Security Architect · VENZO

- 01 Is your security posture aligned with where the organization is going?
- 02 Can your GRC program tell you which risks matter to your business strategy?
- 03 Can it give leadership the data to make informed security decisions?



Maria

GRC analyst

2

weeks of preparation

47

*risks scored on the standard
likelihood × impact matrix*

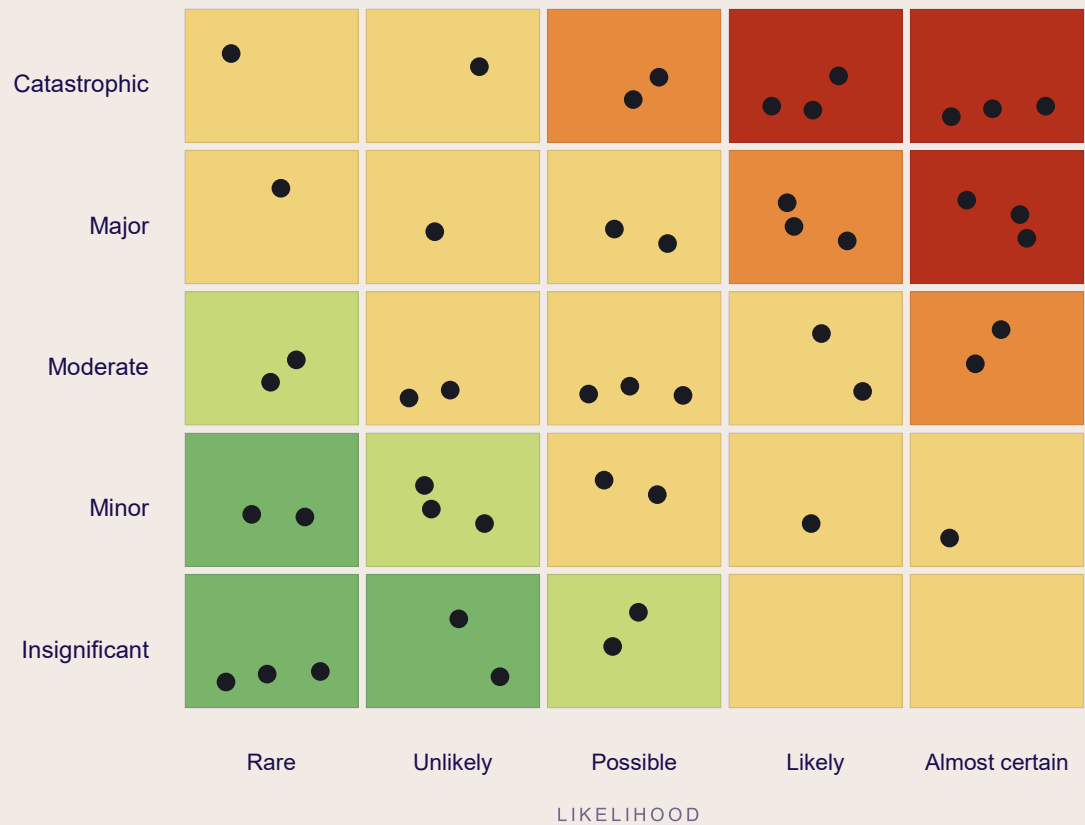
6

*analysts consolidated across
IT security, legal, operations*

1

*heatmap, color-coded, ready
for the executive summary*

IMPACT



47 RISKS · 12 RED · 8 AMBER · 27 GREEN & YELLOW

“We had 11 red risks last quarter. Now 12.
Are we getting worse?”

— CFO

Outcome: continue monitoring × 3 · the loudest voice's pick gets funded × 1

Why did the meeting turn out like this?

01 **Compliance as the dominant lens**

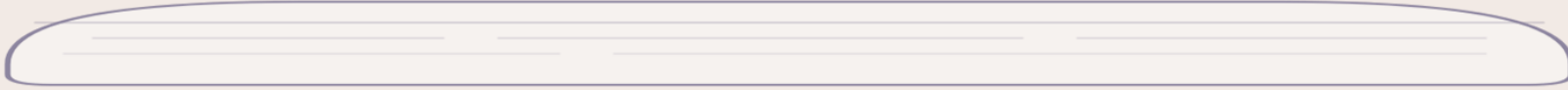
Optimized for evidence, not decisions.

02 **Assessment without data**

The infrastructure measures what the analysts guess.

03 **A tool that compresses, not clarifies**

5×5 grids destroy the distinctions that matter.



Looking backwards. Detached from technology. Disconnected from reality.

What if Maria could walk into that meeting with a *different kind of answer?*

Where the organization is actually exposed. How much it could cost. Which investment moves the needle most.

SECTION 2 OF 4

A different approach to GRC.

Vocabulary, model, and where the rest of this talk lives.

GRC:

the integrated capabilities that enable an organization to *achieve objectives, address uncertainty, and act with integrity.*

A MODEL FOR SECURITY CHOICES - THREE LAYERS · TWO LENSES

Verify

Continuous assurance

Telemetry that tells you, in real time, whether the controls you've built and invested in are still working — and surfaces drift before it becomes an incident.

Live monitoring

Evidence collection

Drift & regression alerts

Invest

Where choices get made

Obligations & Compliance

Meet the controls regulators and frameworks require — proof of conformance, not a measure of safety.

ISO 27001

NIS2

GDPR

Risk

Spend where it actually moves the loss curve — quantified against stated appetite.

Threat-informed

Scenario-based

Quantified exposure

REST OF TALK

Build

Non-negotiable hygiene

The baseline every modern organization must have in place before risk-based investment even becomes a sensible conversation.

MFA everywhere

Patch cadence

Tested backups

***"A decision is only as strong as
its weakest link."***

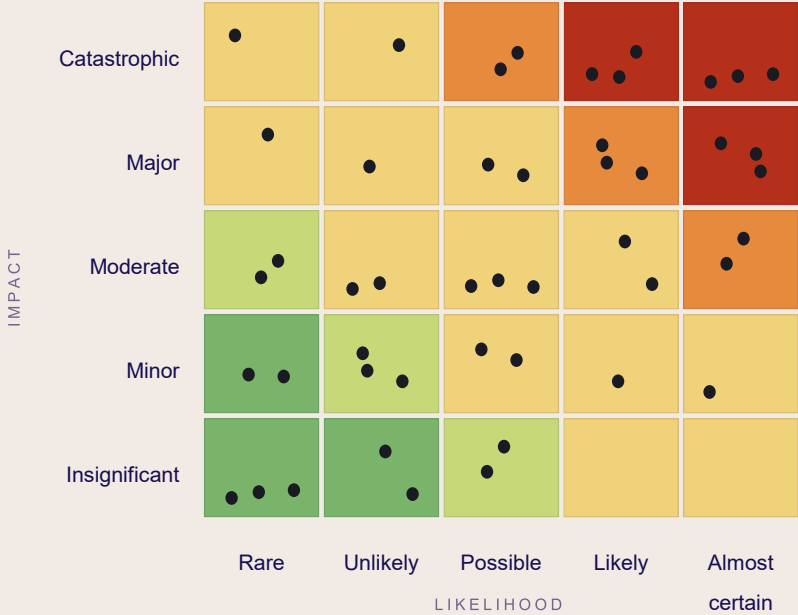
CARL SPETZLER · DECISION QUALITY

A quality decision needs all six — and each one was missed for BEC.

DQ FACTOR	WHERE IT LIVES IN THE RISK PROCESS	MARIA'S BEC: WHAT WAS MISSED
01 Frame · <i>what & why</i>	Context establishment + scenario analysis	<i>"BEC" framed as generic phishing — not wire fraud against finance.</i>
02 Alternatives · <i>options</i>	Identification + treatment options	<i>Treatment was "continue monitoring." No options explored.</i>
03 Information · <i>evidence</i>	Analysis grounded in data	<i>Mailbox-compromise data existed. Phishing telemetry existed. Never used.</i>
04 Tradeoffs · <i>values</i>	Evaluation against quantified appetite	<i>"Amber" meant nothing in financial terms. No quantified appetite to compare to.</i>
05 Reasoning · <i>logic</i>	Structured analysis with decomposition	<i>Single rating. No decomposition into frequency and impact.</i>
06 Commitment · <i>action</i>	Treatment decision with owner + timeline	<i>"Continue monitoring" — no owner, no date, no budget.</i>
		<i>Six factors. Six gaps. Together they made the decision impossible.</i>

From colored adjectives to *probable ranges of loss*

Not about precision. About clarity. Quantification expresses uncertainty without pretending to eliminate it.



THREE SOURCES · THREE QUESTIONS · STRUCTURED UPDATING

Each source answers a different question.

EXTERNAL

What happens to organizations like ours?

Industry base rates · peer experience · sector-wide incident records.

Anchor in empirical reality.

INTERNAL

What actually happens here?

Your environment · control posture · incident history · exposure surface.

Narrows external estimates toward your reality.

SME

What's likely to happen next?

Forward-looking change · planned migrations · zero-trust rollout · emerging actors.

Calibrated, structured elicitation — not "pick a number."

VERIFY LAYER · WHAT YOUR STACK ALREADY PRODUCES

The data is *already* in your environment.

Most of the internal data is being generated continuously. You don't need new data — you need to use what's there.

Likelihood

Threat intelligence · attack-surface exposure · identity posture · attack-path analysis

Impact

Data classification · asset criticality · business-process mapping — what would actually break

Control effectiveness

Posture scores · drift detection · control coverage · continuous monitoring — not just "in place," but working

Technology

Microsoft Defender · Entra · Purview · Sentinel — and equivalents in any modern stack.

From *technical signal* to *risk insight*.

ENTRA ID — PHISHING-RESISTANT MFA

28	challenges issued	23	succeeded
5	fell back to legacy auth	82%	coverage

DEFENDER — PHISHING TELEMETRY

8	phishing emails reached inbox	2	led to credential entry
0	completed compromise	25%	click-through

↓ *translates to* ↓

Frequency of attempt

Measurable, not estimated.

Control effectiveness

Partial — legacy auth fallback is the gap.

Likelihood of materialization

Anchored in real numbers, not a 1–5 rating.

SHOWCASE · 6 SCREENSHOTS · NOT A LIVE DEMO

When the technology carries the *weight*.

A walkthrough of how the tools support each DQ factor — and what Maria's second meeting looks like.

Maria's second meeting.

Same organization. Same meeting in two weeks. A walk-through, not a demo.

srp.nordvind.dk/posture/strategy

OBJECTIVES LINKED RISKS ABOVE APPETITE

4 **47** **3**

S SECURITY RISK PLATFORM

POSTURE

- Objectives
- Controls
- Evidence

RISK

- Risk register
- Scenarios
- Analysis

TREAT

- Compare
- Decisions

Lars Henriksen
Admin · NordVind

Posture / Strategy

NordVind · Strategic Objectives FY 2026

Source: Board strategy 2025–27 · Owner: Executive team · Last reviewed 04 Feb 2026

MISSION

Decarbonize 2.4M Danish homes by 2030

Reliable, expanding renewable supply across the Nordic grid.

LINKED RISKS	EAL	VS. APPETITE
9	4.1M	within

Top contributor · OT intrusion at North Sea wind farm

OPERATIONS

Maintain >98% turbine availability across the fleet

Uninterrupted power generation · SCADA, OT, remote ops continuity.

LINKED RISKS	EAL	VS. APPETITE
14	11.8M	+18%

Top contributor · Ransomware on SCADA controller

TRUST & LICENSE TO OPERATE

Operate securely & compliantly — customer, employee, financial data

Maintain regulatory standing (NIS2, GDPR) · protect financial integrity · zero material breach.

LINKED RISKS	EAL	VS. APPETITE
17	8.2M	+9%

→ **STRONG-AUTH · R07 (BEC) · R03 · R12**

CLICK · DRILL IN

CAPITAL & GROWTH

Deliver Baltic II expansion on time and on budget by Q4 2027

Capex execution, supply-chain integrity, contractor due diligence.

LINKED RISKS	EAL	VS. APPETITE
7	2.9M	+4%

Top contributor · Vendor compromise — supply-chain

Risk doesn't start in a register. *It starts from what the organization is trying to achieve — and what threatens that.*

STEP 01 · FRAME THE SECURITY OBJECTIVE - DQ · FRAME

srp.nordvind.dk/posture/objectives/STRONG-AUTH

SECURITY RISK PLATFORM

POSTURE

- Objectives
- Controls
- Evidence

RISK

- Risk register
- Scenarios
- Analysis

TREAT

- Compare
- Decisions

Lars Henriksen
Admin · NordVind

Posture / Objectives / STRONG-AUTH

Enforce Strong Authentication STRONG-AUTH

IDENTITY & ACCESS MANAGEMENT · OWNER: ANNA SØRENSEN, IAM LEAD

58%

AVG. POSTURE · CURRENT MONTH
▼ -7 pts vs. target (65%)

Ensure all authentication into NordVind systems is verifiably strong — phishing-resistant where credentials carry financial or privileged authority.

PHISHING BRUTE_FORCE MFA_BYPASS CREDENTIAL_THEFT BEC

● 2 PASSING

● 3 FAILING

● 1 NOT ASSESSED

CONTROL	NAME	SEVERITY	POSTURE	PASS
IAM-MFA-001	Conditional Access for admin MFA	HIGH	82%	✓
IAM-MFA-002	User MFA enforcement	HIGH	71%	✓
IAM-MFA-003	Phishing-resistant methods · finance team	HIGH	43%	✗
IAM-MFA-004	Legacy authentication blocking	HIGH	28%	✗
IAM-MFA-005	Risk-based MFA	MEDIUM	54%	✗

LINKED RISKS · 3

- R07 · Wire fraud due to BEC targeted finance **High**
- R12 · Broad phishing & credential theft **Med**
- R03 · Privileged credential compromise **High**

Maria isn't browsing 47 risks. **Risk starts from objectives** — and the controls that measure them.

srp.nordvind.dk/risks/R07

S SECURITY RISK PLATFORM

Risk / Risk register / R07

Wire fraud due to BEC targeted finance R07

RISK SCENARIO · NARRATIVE FLOW
5-element structure

CATEGORY · FINANCIAL · ESTIMATED BY MARIA KJELDEN · LAST REVIEWED 12 APR 2026

THREAT	ASSET	VULNERABILITY	EVENT	CONSEQUENCE
BEC operator / wire-fraud group	Finance team mailboxes (28 accounts)	Absence of dual-authorisation controls on high-value payment workflows	Fraudulent wire transfer or payroll redirection to attacker account	Direct financial loss, forensic costs, regulatory reporting

IMPACTS → THROUGH → RESULTING IN → CAUSING →

ANNUAL FREQUENCY 0.5 / yr	IMPACT RANGE 1.5M – 30M DKK	EAL 3.3M DKK	VAR · 95% ~28M DKK
-------------------------------------	---------------------------------------	------------------------	------------------------------

↳ KPIs covered on next slide

Lars Henriksen
Admin · NordVind

Scenario, not a line in a register. Five elements you can actually reason about.

srp.nordvind.dk/analysis/risks?risk=R07

S SECURITY RISK PLATFORM

POSTURE

- Objectives
- Controls
- Evidence

RISK

- Risk register
- Scenarios
- Analysis

TREAT

- Compare
- Decisions

Lars Henriksen
Admin · NordVind

Analysis / Risks / R07 · Wire fraud due to BEC targeted finance

ANNUAL FREQUENCY
0.5 / yr

IMPACT RANGE
1.5M – 30M DKK

EAL
3.3M DKK

VAR · 95%
~28M DKK

EXTERNAL BASE RATE

Industry benchmark

FBI IC3 2024 · energy mid-market

Annual BEC frequency, sector	0.3 – 1.0
Anchor used	0.5
Median loss, comparable orgs	4M DKK

CONFIDENCE · MEDIUM

INTERNAL POSTURE TELEMETRY

LIVE TENANT

Microsoft Graph · last 90 days

Entra ID · Microsoft Defender · finance OU

Phishing-resistant MFA · finance	43%
Legacy-auth fallback events	5 of 28
Defender phishing reaching inbox	8
Credential entry attempts	2
Completed compromise	0

CONFIDENCE · HIGH · AUDITABLE

SME FORWARD-LOOKING

Estimated by Maria Kjeldsen

CISO · NordVind · 12 Apr 2026

Impact range (P10 – P90)	1.5M – 30M DKK
Basis	IC3 median × revenue
Adjustments	+ insurance recall

CONFIDENCE · HIGH

↓ External widens · Internal narrows · SME calibrates the future. Same data already in your Azure tenant — no extra integration.

LOSS EXCEEDANCE · WIRE FRAUD DUE TO BEC TARGETED FINANCE

Three sources, **one refined range**. The numbers underneath the risk are auditable, back to a Graph endpoint.

srp.nordvind.dk/posture/controls/IAM-MFA-003

SECURITY RISK PLATFORM

POSTURE

- Objectives
- Controls**
- Evidence

RISK

- Risk register
- Scenarios
- Analysis

TREAT

- Compare
- Decisions

Lars Henriksen
Admin · NordVind

Posture / Controls / IAM-MFA-003

Phishing-resistant MFA — finance team IAM-MFA-003

IDENTITY & ACCESS · LINKED OBJECTIVE: STRONG-AUTH · LINKED RISK: R07

43%
POSTURE - CURRENT
▲ +23 over 4 months (20→30→45→43)2

Auth method registration · finance OU · 28 users
collector: graph.microsoft.com · pulled 09:14 today · cached 4h

12 / 28 ✓ live
phishing-resistant

RAW EVIDENCE · GRAPH RESPONSE

GET /REPORTS/AUTHENTICATIONMETHODS/USERREGISTRATIONDETAILS?\$FILTER=DEPARTMENT EQ 'FINANCE'

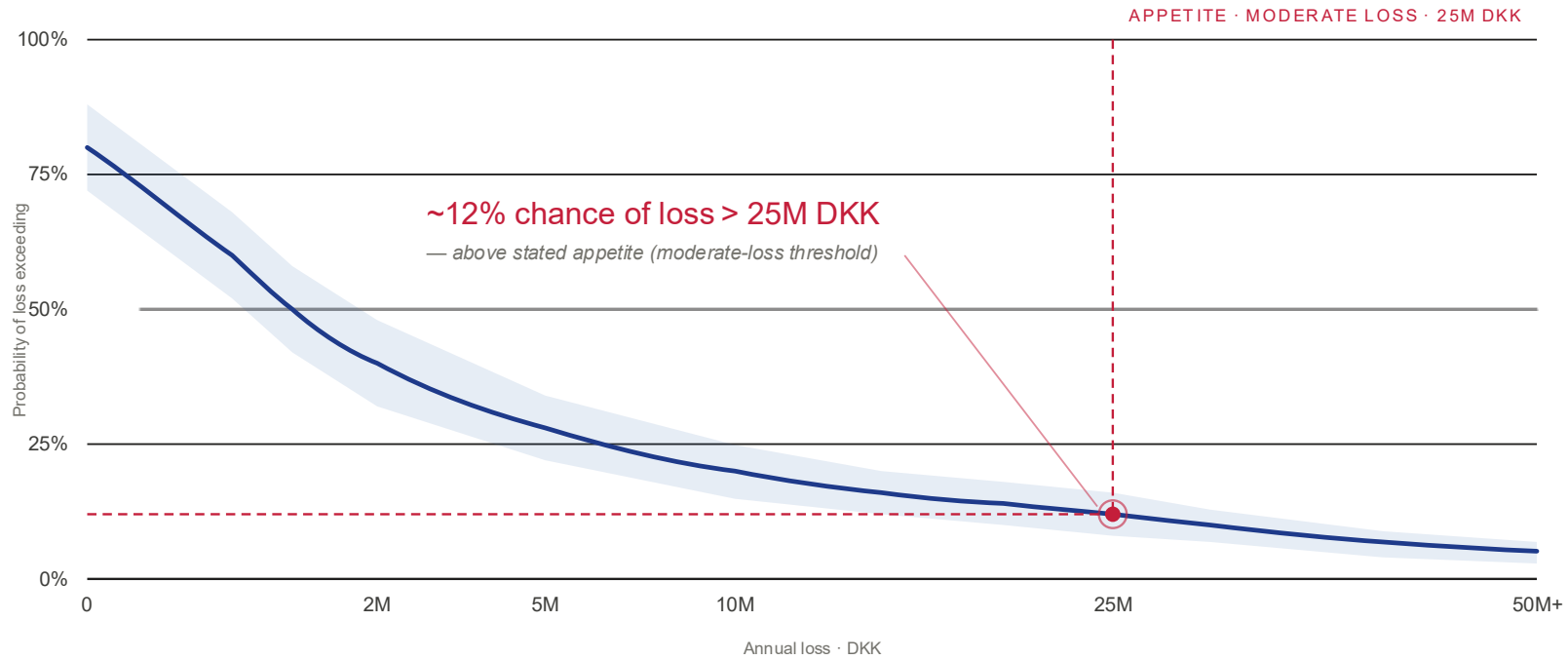
```
// 28 users - finance OU - NordVind tenant
{
  "@odata.context" : "https://graph.microsoft.com/v1.0/$metadata#..."
  "@odata.count" : 28
  :{"summary"
  , "phishingResistantMethodRegistered" : 12
  , "softwareOathRegistered" : 11
  , "smsOnlyRegistered" : 5
  , "noMfaRegistered" : 0
  },
  : [ "value"
  , { "userPrincipalName" : "anna.sorensen@nordvind.dk"
    , "methodsRegistered" : [ "fido2" , "windowsHelloForBusiness"
    , "isPhishingResistant" : true
    , "userPrincipalName" : "Maria.kjeldsen@nordvind.dk"
    , "methodsRegistered" : [ "microsoftAuthenticator" , "sms"
    , "isPhishingResistant" : false
    , "userPrincipalName" : "jens.olsen@nordvind.dk"
    , "methodsRegistered" : [ "sms"
    , "isPhishingResistant" : false
  },
  // ... 25 more rows
  ]
}
```

The number is **auditable** — back to its source. Same Graph endpoint your Azure admin uses. Same response.

Loss exceedance — R07 · Wire fraud due to BEC targeted finance

10,000 SIMULATIONS · REFINED INPUTS · 90% CONFIDENCE BAND

• ABOVE TOLERANCE



EAL · BEC
3.3M DKK

VAR · 95%
28M DKK

P(LOSS > 25M)
~12%

ABOVE APPETITE
+2pts

NORDVIND TOLERANCE LADDER

Frequent loss

10M · 25%

Moderate loss

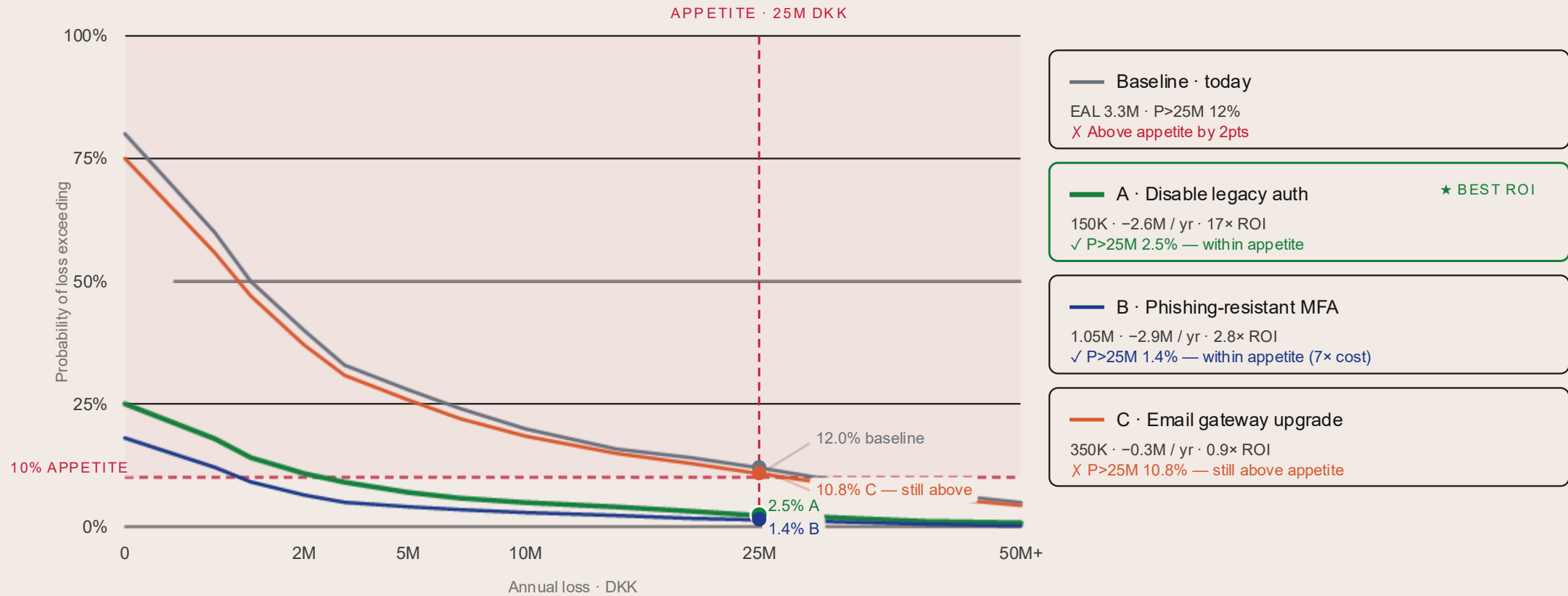
25M · 10%

Occasional loss

50M · 5%

Exposure vs. appetite, explicit. Twelve percent chance of losing more than 25M DKK — above stated appetite.

STEP 05 · COMPARING TREATMENT OPTIONS - DQ · ALTERNATIVES



Which investment moves the needle? The trade-off is visible, not intuited.

ROLLS UP TO STRATEGIC OBJECTIVE

↗ Operate securely & compliantly · Trust & license to operate

DEC-07-A · linked to R07 · Wire fraud due to BEC targeted finance

EAL 8.2M → 5.6M

APPROVED · 15 MAY 2026

Disable legacy authentication across finance by end of Q3.

OWNER: Anna Sørensen, IAM Lead

START · TARGET: 15 May — 30 Sep 2026

BUDGET: 150,000 DKK

RISK OWNER: CISO · Lars Henriksen

ACCEPTANCE CRITERIA: Zero successful legacy auth from finance accounts MFA coverage 100% across finance OU Phishing-resistant enrollment ≥ 95%

LINKED TREATMENT · REVIEWERS: Option A · from /scenarios/compare Reviewers · CFO · CISO · DPO Cycle · Q3 2026 governance review

MONITORING METRIC · VERIFY LAYER

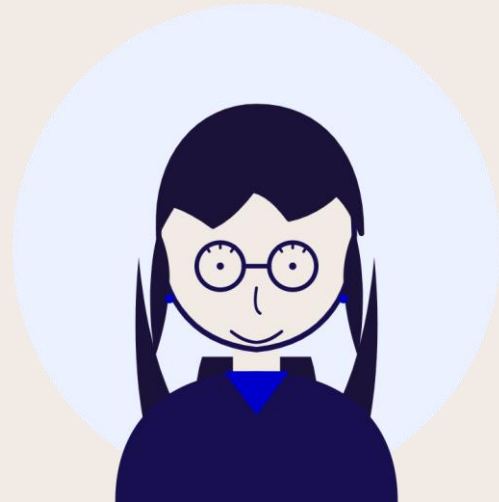
Weekly Entra coverage report · finance OU

current: 43% → target: 100% · drift alerts on regression

SOURCE · SAME GRAPH ENDPOINT AS STEP 03

graph.microsoft.com/v1.0/reports/authenticationMethods/userRegistrationDetails

A decision has an owner, a date, a budget — and a way to know if it worked. The Verify layer closes the loop.



SAME ROOM. SAME QUESTIONS.

Different *process*.

"Are we getting worse?"

A curve. With an appetite line.

"Which initiative gets the budget?"

A ranked recommendation. With reasoning.

"What did we decide?"

A record. With an owner. With a date.

Same Maria. *Different process.*

WHAT YOU CAN DO MONDAY

Three shifts.

01

Start from *objectives* , not the register.

What is the organization trying to achieve, and what threatens that?

02

Make your *weakest DQ link* your roadmap.

Where is your process weakest? That's where you fix first.

03

Let the *data you already have* count the risk.

The Verify layer is already producing it. Use it.

Thank you.

PETER TRIER JØRGENSEN
SECURITY ARCHITECT · VENZO
PETER.TRIER@OUTLOOK.COM