

Measurement Paradox Checklist

When measuring performance changes the performance being measured.



avsec-resilience.com



Why measurement can mislead

Measurement supports decisions, but poorly chosen measures can distort priorities and create false confidence.



For professional discussion and reflection • Illustrative, not prescriptive • Measures should be interpreted in context and considered alongside evidence, risk, unintended consequences and professional judgement.

When a measure becomes a target

Once people are judged against a measure, behaviours may change to improve the number rather than the underlying security outcome.



For professional discussion and reflection • Illustrative, not prescriptive • Measures should be interpreted in context and considered alongside evidence, risk, unintended consequences and professional judgement.

Measure activity or effectiveness?

Completing activities does not automatically mean security outcomes have improved.



For professional discussion and reflection • Illustrative, not prescriptive • Measures should be interpreted in context and considered alongside evidence, risk, unintended consequences and professional judgement.

Watch for target fixation

People may concentrate on achieving the metric while losing sight of the wider security objective.



For professional discussion and reflection • Illustrative, not prescriptive • Measures should be interpreted in context and considered alongside evidence, risk, unintended consequences and professional judgement.



Look for gaming behaviour

Measures can be manipulated, intentionally or unintentionally, to make the metric look better without improving security.

How measures can be gamed

- Change definitions**
e.g. reclassify incidents
- Change timing**
e.g. delay reporting
- Alter processes**
e.g. change thresholds
- Select what to report**
e.g. focus on positive data
- Influence the numerator**
e.g. exclude certain events
- Influence the denominator**
e.g. limit exposure or activity

Common examples

- Reclassifying incidents**
e.g. record as non-security
- Delaying or batching reports**
e.g. report after the period
- Changing thresholds**
e.g. raise the reporting level
- Reporting only positive activity**
e.g. completed rather than effective
- Excluding certain events**
e.g. specific locations or shifts
- Reducing the denominator**
e.g. fewer passengers or flights
- Changing processes**
e.g. reduce inspections to lower reported issues

For professional discussion and reflection • Illustrative, not prescriptive • Measures should be interpreted in context and considered alongside evidence, risk, unintended consequences and professional judgement.

Check for under-reporting

A reduction in reports may indicate improvement, or a reduced willingness or ability to report.

✓ May be a real improvement

- Fewer security incidents are occurring
- Controls are working effectively
- Greater awareness and prevention
- Risk has genuinely been reduced

SECURITY INCIDENT REPORTS

Year	Reports
2022	200
2023	150
2024	100
2025	50

POTENTIAL ALTERNATIVE EXPLANATIONS

- Reduced willingness to report
- Changes to reporting process or definitions
- Under-reporting of minor incidents
- Lack of confidence in the system
- Reclassification or removal of events

! May indicate under-reporting

- Staff do not report minor incidents
- Reporting process has become more complex
- Incidents are reclassified as non-security issues
- Lack of confidence in the reporting system
- Management pressure to reduce reported numbers

WHY THE DROP?

INCIDENT REPORTS

UNDER-REPORTING RISK FACTORS

- CULTURE
- PROCESS
- DEFINITIONS
- CLASSIFICATION
- FEEDBACK
- CONFIDENCE

Question improving metrics

A better KPI does not necessarily mean security performance has improved.
Always consider what else could explain the change.



For professional discussion and reflection • Illustrative, not prescriptive • Measures should be interpreted in context and considered alongside evidence, risk, unintended consequences and professional judgement.

Look for displaced risk

Improving one measured area may move risk, workload or undesirable behaviour to another area that is not being measured.



For professional discussion and reflection • Illustrative, not prescriptive • Measures should be interpreted in context and considered alongside evidence, risk, unintended consequences and professional judgement.

Check for unintended consequences

Actions to improve one metric can sometimes create new risks or problems elsewhere. Look for trade-offs and side effects.

✓ Good practice

- Consider the wider security picture
- Look for potential trade-offs
- Involve different stakeholders
- Monitor for unintended effects

IMPROVE METRIC A

! Check for side effects

- LONGER SCREENING TIMES
Increased delays and congestion
- STAFF PRESSURE
Negative impact on customer experience
- PASSENGER DISSATISFACTION
Higher costs or resource demands
- NEW VULNERABILITIES
Creates workarounds or non-compliance
- Moves risk to another area
- A new vulnerability is introduced

THINK BEYOND THE METRIC

- ✓ What else could change?
- ✓ Who might be affected?
- ✓ What new risks could emerge?
- ✓ Are there acceptable trade-offs?
- ✓ How will we monitor the impact?

INTENDED BENEFITS

UNINTENDED CONSEQUENCES

For professional discussion and reflection • Illustrative, not prescriptive • Measures should be interpreted in context and considered alongside evidence, risk, unintended consequences and professional judgement.



Look for a balanced view

Use a mix of leading and lagging measures to get a clearer and more reliable picture of security performance.

Why a balanced view helps

- Shows early warning signs and final outcomes
- Reduces the risk of wrong conclusions
- Supports better decision-making
- Highlights opportunities and challenges
- Provides a more complete picture

SECURITY PERFORMANCE

LEADING MEASURES	LAGGING MEASURES
☒ Training completed	☒ Security incidents
☒ Inspections carried out	☒ Regulatory findings
☒ Issues identified	☒ Access violations
☒ Feedback received	☒ Disciplinary actions
☒ Vulnerabilities resolved	☒ Financial losses

Risks of an unbalanced view

- Early warning signs may be missed
- Too much focus on incidents after the fact
- Activity may increase without real improvement
- Effort may be placed in the wrong areas
- Leads to incomplete or misleading conclusions

COMBINING THE PICTURE

PEOPLE
PROCESSES
TECHNOLOGY
DATA
STAKEHOLDERS

For professional discussion and reflection • Illustrative, not prescriptive • Measures should be interpreted in context and considered alongside evidence, risk, unintended consequences and professional judgement.



Review and adjust regularly

Measures should evolve as risks, operations, priorities and organisational circumstances change.

Good practice

- Set a regular review cycle
- Check the data quality
- Consider changes in risk and threat
- Involve key stakeholders
- Adjust or replace where needed

Common issues

- Measures become out of date
- Focus on the wrong priorities
- Poor or inconsistent data quality
- Lack of stakeholder engagement
- Changes in the operating environment are not reflected

REVIEW ADJUST IMPROVE

REVIEW
Are the measures still relevant?

ANALYSE
What does the data show?

ADJUST
Refine or replace measures

IMPROVE
Strengthen security outcomes

REVIEW CYCLE

JAN	FEB	MAR	APR	MAY	JUN
✓	✓	✓	✓	✓	✓
JUL	AUG	SEP	OCT	NOV	DEC
✓	✓	✓	✓	✓	✓

SECURITY PERFORMANCE REVIEW

RISK AND THREAT CHANGES
STAKEHOLDER FEEDBACK
DATA QUALITY
MEASURE UPDATES

REVIEW
RELEVANCE
ADJUST
IMPROVE

Communicate the story, not just the numbers

Context, explanation and clear visuals help others understand what the data means and why it matters.

Good practice

- Explain what the data shows and why it matters
- Use clear and simple visuals
- Link to real examples and context
- Tailor the message to your audience
- Be transparent about limitations

SECURITY PERFORMANCE
From data to decisions

Quarter	Incidents (lagging)	Inspections (leading)
Q1 2024	25	20
Q2 2024	24	22
Q3 2024	23	24
Q4 2024	22	26
Q1 2025	21	28
Q2 2025	20	30

WHAT HAPPENED?
Fewer incidents reported.

WHY?
Increased inspections and improved compliance.

SO WHAT?
Lower risk and a stronger security posture.

Common pitfalls

- Presenting numbers without context
- Using technical language that is hard to understand
- Not addressing key questions from stakeholders
- Overstating success or hiding challenges
- Failing to show what actions follow

TURN DATA INTO DECISIONS

DATA

CONTEXT

STORY

ACTION

KEY POINTS

TRENDS

INSIGHTS

ACTIONS

Turn insight into action

Use leading and lagging measures to identify issues early, focus effort and drive continuous improvement.

Key takeaways

- Understand the difference
- Use both leading and lagging measures
- Look for unintended consequences
- Review and adjust regularly
- Communicate the story and take action

What next?

- Review your current measures
- Identify gaps and opportunities
- Agree actions and responsibilities
- Set a review date
- Measure progress and celebrate success

UNDERSTAND
Identify the right measures

MONITOR
Track and analyse

RESPOND
Take action early

ENGAGE
Share and communicate

IMPROVE
Build a stronger security outcome

NEXT STEPS

- Review current leading and lagging measures
- Identify gaps and new opportunities
- Agree actions and responsibilities
- Set a timeline for review
- Monitor progress and adjust as needed