WHITE PAPER 03 / RISK AND GAP ANALYSIS

Understanding Identity Risks and Gaps

A practical guide to findings, severity, heatmaps, maturity comparisons and the decisions behind the dashboard.

AIdentX Editorial | September 2026

Executive summary

A risk dashboard becomes useful when a reader can move from a chart to an understandable finding and then to a decision. A gap describes what is missing or insufficient compared with an expected state. A risk describes what could happen and why it matters. This paper shows how to keep those concepts connected without confusing counts, scores or attractive charts with evidence of improvement.

What you will take away

- Write findings that explain both the condition and its consequence.
- Read every chart with its scope, time period and scoring method.
- Verify improvement with evidence rather than a falling issue count.

Written for risk owners, security reviewers and business leaders.

The worked scenarios are fictional. The checklists and examples are practical editorial guidance, not customer results or a certification method.

1. Explain the finding before assigning a colour

In a fictional supplier-access assessment at Cedar Vale Services, reviewers find that three selected access requests do not record an end date. The gap is the missing expiry information in those records. The risk is that access may continue beyond the period of legitimate business need. The assessment has not established that someone misused access. That distinction matters when management decides how urgently to act.

A useful finding names the condition, the affected system or process, the evidence and the potential consequence. Avoid labels such as “poor IAM” or “critical governance failure” without explanation. The person receiving the finding should understand what needs attention even if they have never used the assessment platform.

NIST SP 800-30 treats risk assessment as input to decisions about responses to risk. It considers likelihood and impact in the context of threats, vulnerabilities and existing conditions. NIST SP 800-30 Rev. 1: Guide for Conducting Risk Assessments.

Concept	Plain-language question
Observation	What did the reviewer actually see?
Gap	What expected practice is missing or insufficient?
Risk	What could go wrong because of that condition?
Action	What will change, and who will check the result?

2. Make severity understandable

Before comparing findings, define the rating method. A score is useful only when the people assigning and reading it share an understanding of the scale. Record why the consequence matters and what supports the likelihood judgement. Include existing controls that reduce exposure, while distinguishing those controls from improvements that are only planned.

The same missing end date can have different implications in two environments. An account with access to production finance data presents a different concern from an account limited to a disposable training environment. A separate control that reliably blocks expired supplier engagements may reduce exposure, but the reviewer needs evidence that it operates for the accounts in question.

Keep rating changes traceable. A lower rating after an owner explains a control may be justified if the control is verified. A lower rating merely because a remediation task was created is premature. If the evidence is incomplete, record that uncertainty instead of using a precise-looking number to hide it.

> **Avoid false precision**
>
> An ordinal rating such as low, medium or high expresses an ordered judgement. A score of four is not automatically twice as risky as a score of two. Use the configured method consistently and retain the reasoning behind the rating.

3. Read charts as routes into the evidence

AssessX risk and gap pages provide KPIs, distribution views, heatmaps and detail views. Start by checking the filters. A chart for one campaign is not the same as a view across all campaigns. An open-findings count is not a count of all findings ever identified. Explain the population before presenting a result to a wider audience.

View	Useful question	Common mistake
KPI cards	How many in-scope findings need attention?	Treating a smaller count as proof of lower exposure.
Severity heatmap	Where are the most serious rated findings concentrated?	Ignoring the scoring definitions and filtered population.
Domain or category view	Which areas need a closer review?	Assuming more findings always means poorer controls.
Trend view	What changed between comparable periods?	Comparing periods with different assessment coverage.
Detail view	What evidence and rationale support this finding?	Acting only on a chart label.

A domain with many findings may have received more detailed assessment than another domain. Show assessment coverage beside the interpretation, even if it requires a note outside the chart. The right next action may be additional assessment of the quiet area, rather than a conclusion that it is performing well.

4. Interpret maturity without hiding weak points

A maturity comparison describes how established a capability is relative to a defined scale or target. It does not directly measure the probability of an incident. A process can be well documented and still fail in operation; a small team can carry out a reliable control without sophisticated automation.

Agree what each level means for the capability being assessed. For temporary access, the distinction might be between an informal practice, a documented process and an evidenced process with exception review. These are illustrative anchors for a local rubric, not a claim about a universal maturity scale or the platform's configured labels.

Use radar charts to locate differences that deserve explanation, then open the underlying detail. An average can hide a weak critical capability. If supplier removal is poorly controlled, a strong score in an unrelated domain does not cancel that exposure. Set targets according to the business need and the consequences of failure.

When sharing a current-to-target comparison, identify who approved the target and when. A changing target can make progress appear worse or better without any operational change. Keep the earlier target in the review history so readers can understand why the plan changed.

5. Use pattern analysis to ask better questions

AI pattern analysis can help reviewers examine relationships among risks or gaps in AssessX. A suggested cluster around supplier ownership may point to a shared cause. It is a lead to investigate. Similar wording across findings does not establish that they have the same cause or that one action will resolve them all.

In the fictional example, missing sponsors, absent end dates and unverified removals might all involve supplier onboarding. Review the linked records before grouping the work. One application may have an integration problem, while another has a responsibility gap. A single generic initiative could leave one of those causes untouched.

Check duplicate findings before reporting totals. Repeated assessments may describe the same unresolved weakness. Preserve the links to each assessment, but distinguish recurrence from a genuinely new issue. Where findings are grouped, retain the original records and explain which evidence supports the shared interpretation.

- Do the linked findings involve the same process or merely similar language?
- Is the proposed cause supported by operational evidence?
- Would the proposed action address every linked finding?
- Which findings still need separate ownership or verification?

6. Close the loop with a clear decision

For each material finding, record the response, owner, next review date and required evidence. Some issues need immediate containment and longer-term process repair. Some need more investigation before a rating can be defended. If management accepts an exposure, document the rationale and review conditions so acceptance does not become indefinite neglect.

Present three things together in a management review: the concern, the evidence and the decision requested. For Cedar Vale, that could be a proposal to complete the supplier-account inventory, correct missing ownership and expiry information, and test removal for completed engagements. Report progress against those outcomes rather than counting meetings or completed tickets.

Management review prompt

“These findings concern temporary finance access. Here is the evidence and what remains uncertain. We recommend this owner and action. We will consider the improvement effective when a new sample demonstrates the intended removal process.”

After implementation, revisit the original finding. Check that the change operated in the affected scope and that exceptions are managed. A chart becomes persuasive when the reader can trace an apparent improvement to that verification. Keep that evidence available for the next review.

References and further reading

Primary guidance used for the points cited in this paper. Examples, templates and recommended working practices are AIdentX editorial guidance. Sources reviewed September 2026.

NIST SP 800-30 Rev. 1: Guide for Conducting Risk Assessments

https://csrc.nist.gov/pubs/sp/800/30/r1/final

Put the guidance into practice

Read related articles and watch AssessX product demonstrations at www.aidentx.com/assessx/resources.