UNIVERSAL FRAMEWORK Domain 6. Learning & Improvement - evidence notes

Metric: Repeat incidents or repeat failures

Evidence

E1 – Exists (Gateway Evidence)
Does a defined organisational process exist for learning from incidents, failures, and reviews?

E2 – Enabled
Are root cause analysis and improvement mechanisms consistently applied?

E3 – Executed
Is there evidence that lessons learned have reduced repeat incidents or failures?

You can support each level (E1–E3) with a mix of documented processes, consistent practice, and trend data that shows fewer repeats over time.[1][2]

E1 – Exists (Gateway Evidence)

Show that there is a defined, organisation-wide process for learning from incidents, failures and reviews.[2][3]

Useful evidence:

- Policy or standard that describes your “learning from incidents” process, scope, and responsibilities (e.g. based on steps like collect, evaluate, decide, act, review).[4][2]
- Documented procedure or workflow for incident handling, including investigation, root cause analysis, corrective/preventive actions, and effectiveness review.[3][5]
- Defined triggers for formal reviews (e.g. incident severity thresholds, repeat failures, significant near misses).[2]
- Templates and tools: investigation/RCA templates, lessons learned forms, action-tracking registers, after-action review checklists.[5][6]
- Governance: reference in management system, risk framework, or ISO 27001/9001/Safety management documentation showing how learning from events is embedded.[1][2]

- Clear roles: named owners for incident management, investigation leads, learning coordinators or “local safety leaders.”[7][2]

Notes an assessor might write:

- “Documented ‘Learning from Incidents’ procedure v3.2 covers reporting, investigation, RCA, action management, effectiveness review.”
- “Standard templates used for investigations and lessons learned workshops are available in QMS.”
- “Policy A.5.27 references requirements to capture and act on lessons from information security incidents.”[1]

E2 – Enabled (RCA and improvement consistently applied)

Show that the process is not only written down but actively and consistently used for applicable incidents.[5][7]

Useful evidence:

- Incident records that consistently include: description, classification, root cause analysis, contributing factors, and recommended actions.[8][5]
- Use of a recognised RCA or analysis method (e.g. 5 Whys, fishbone, fault tree, discussion groups) applied to all significant incidents, not just a few.[9][7][5]
- Documented criteria for when RCA is required and evidence those criteria are followed (e.g. “all high/critical incidents have an RCA within 10 working days”).[5][1]
- Action logs showing improvement actions are:
  - SMART (specific, measurable, achievable, realistic, timely).[2][5]
  - Assigned to owners with due dates.
  - Tracked through to completion in a unified system.
- Evidence of quality checks on RCAs (e.g. peer review, standard evaluation criteria, checks that causes are evidence-based and logically linked).[6][10]
- Training material and attendance records for staff who conduct investigations and facilitate lessons learned.[7][2]

Notes an assessor might write:

- “Sample of 10 high-severity incidents: all have documented RCA using standard template; actions assigned and tracked in central register.”
- “RCA quality checklist used; investigations reviewed by safety manager before closure.”[6]
- “>80% of significant incidents have a documented post-incident review within 30 days (per KPI dashboard).”[1]

E3 – Executed (Lessons reduce repeat incidents/failures)

Show that learning and improvements are actually changing outcomes, particularly reducing repeat incidents and failures.[7][1]

Evidence types:

1. Outcome metrics and trends
    - Rate of repeat incidents with the same root cause over time (e.g. per quarter), by system/asset/service.[1]
    - Trends in number or rate of high-impact incidents, normalised (per site, per user, per system).[7][1]
    - Percentage of improvement actions that are verified as effective (not just “closed”).[1]
    - Studies or internal analyses showing reductions in near misses/adverse events after implementation of specific actions.[7]

2. Effectiveness reviews
    - Post-implementation reviews that explicitly ask “Did this action prevent recurrence?” and document evidence (e.g. no similar incidents for X months, control performance data).[9][2]
    - Cases where ineffective actions were revised or strengthened following an effectiveness check.[7][1]

3. Specific case studies (“stories”)
    - Before/after examples: a recurring failure mode, the investigation and system changes, followed by a documented drop in that failure type.[1][7]
    - Behaviour change evidence (e.g. fewer “repeat clickers” in phishing tests, improved reporting and safer practices following targeted coaching).[11][12]

4. Organisational learning and spread
    - Evidence that lessons from one area are communicated and applied more widely (alerts,

safety bulletins, toolbox talks, learning sessions).[4][2]
    - Records showing controls or standards were updated and adopted across sites as a result of specific incidents.[3][2]

Notes an assessor might write:

- "Dashboard shows 60% reduction in incidents with root cause 'incorrect configuration' over 12 months after implementing new change control and training."[7][1]
- "Effectiveness reviews carried out for 90% of high-risk incident actions; two ineffective measures were redesigned after follow-up incidents."[7]
- "Lessons learned bulletins issued quarterly; evidence of procedure updates and toolbox talks referencing those bulletins."[4][2]

Example evidence table you could use

Level	What to look for	Typical documents/artefacts
E1 – Exists	Defined process for learning from incidents	Policies, procedures, LFI standard, investigation and lessons learned templates, role descriptions, QMS references.[2][3]
E2 – Enabled	Consistent application of RCA and improvement mechanisms	Sample incident files with RCA and actions, RCA criteria, action logs, training records, RCA quality checks.[5][6][7]
E3 – Executed	Demonstrable reduction in repeats due to learning	Trend metrics on repeat incidents, effectiveness reviews, case studies, evidence of wider rollout of improvements.[1][7][4]

Sources

[1] A.5.27 Learning From Information Security Incidents – MSP Lessons ... https://www.isms.online/managed-service-providers/a-5-27-learning-from-information-security-incidents-msp-lessons-learned-loops/

[2] [PDF] Components of Organisational Learning From Events https://www.veiligheidvoorop.nu/wp-content/uploads/2024/02/Oct23-LVI-021-IOGP-552-Components-of-Organisational-Learning-from-Events.pdf
[3] [PDF] Guidance on Learning From Incidents, Accidents and Events - IChemE https://www.icheme.org/media/8444/xxv-paper-02.pdf
[4] Enhancing Learning from Incidents – Five Tried and Tested ... https://www.icheme.org/media/16945/hazards-28-paper-39.pdf
[5] [PDF] Root cause analysis toolkit - Clinical Excellence Commission https://www.cec.health.nsw.gov.au/__data/assets/pdf_file/0009/606735/Root-cause-analysis-toolkit.pdf
[6] Evaluating the quality of a root cause analysis investigation https://www.bakerhughes.com/cordant/blog/evaluating-quality-root-cause-analysis-investigation
[7] Effectiveness and limitations of an incident-reporting system ... - PMC https://pmc.ncbi.nlm.nih.gov/articles/PMC6160204/
[8] using learning potential in the process from reporting an ... https://pubmed.ncbi.nlm.nih.gov/23498711/
[9] What Is Root Cause Analysis? The Complete RCA Guide - Splunk https://www.splunk.com/en_us/blog/learn/root-cause-analysis.html
[10] The Effectiveness of Root Cause Analysis: What Does the Literature Tell Us? https://www.sciencedirect.com/science/article/abs/pii/S1553725008340495
[11] Learning From Incidents: Key Indicators of Real Organizational Growth https://www.safetywise.com/post/how-to-know-when-you-ve-truly-learned-from-an-incident
[12] Security Awareness Metrics That Matter: Predicting Breach Reduction https://hoxhunt.com/blog/security-awareness-metrics
[13] [PDF] Learning from incidents November 2019 https://www.coalminesinquiry.qld.gov.au/__data/assets/pdf_file/0005/1621076/Anglo-American-SandSD-Group-Standard-Learning-from-Incidents-November-2019.pdf
[14] Using a survey of incident reporting and learning practices to ... - PMC https://pmc.ncbi.nlm.nih.gov/articles/PMC2464979/
[15] Why Aren't Organisations Learning from What Goes Wrong in Their ... https://www.incidentanalytics.com.au/blog/how-can-we-learn-more-from-unwanted-events