# Macro Iteration 1

## Phase: Initiating

* Artifact: 1.1.0, Phase=Initiating, mini\_iter=1
* gapID=d6e0ba, gapType=MissedRequirement,  
  Desc=1.1.0 Whole artifact cross-artifact missing security/privacy baselines,  
  Status=NewIssue, Impact=Low,  
  Recommendation=Add session/cookie flags, timeouts, MFA, consent, retention, audit
* Artifact: 1.1.1, Phase=Initiating, mini\_iter=1
* gapID=d6e0ba, gapType=MissedRequirement,  
  Desc=1.1.1 Whole artifact cross-artifact security baseline gaps,  
  Status=InProgress, Impact=Low,  
  Recommendation=Add session/cookie flags, timeouts, MFA, consent, retention, audit
* (Teacher doc) End of Mini-Iteration 1 (Phase=Initiating, Macro=1):  
  Root causes identified:  
  - global-1: UUID identifiers chosen because ensure stable keys  
  - global-2: Lack of unified security baseline causes inconsistent module security expectations  
    
  Lessons learned:  
  - global-1: Standardise UUID identifiers across artifacts because ensure stable keys  
  - global-2: Require a minimal security baseline and map it into each module's DevSecOps / Security column (Whole artifact)
* Artifact: 1.1.0, Phase=Initiating, mini\_iter=2
* gapID=d6e0ba, gapType=MissedRequirement,  
  Desc=1.1.0 Whole artifact security/privacy baseline partial,  
  Status=Resolved, Impact=Low,  
  Recommendation=Add session/cookie flags, timeouts, MFA, consent, retention, audit
* Artifact: 1.1.1, Phase=Initiating, mini\_iter=2
* gapID=d6e0ba, gapType=MissedRequirement,  
  Desc=1.1.0 Whole artifact cross-artifact missing security/privacy baselines,  
  Status=Resolved, Impact=Low,  
  Recommendation=Add session/cookie flags, timeouts, MFA, consent, retention, audit
* gapID=0a5003, gapType=SecurityGap,  
  Desc=1.1.1 UUID-0005 No auth lockout/brute-force control,  
  Status=NewIssue, Impact=Medium,  
  Recommendation=Add lockout/backoff policy in Auth-Session
* gapID=9d77eb, gapType=SecurityGap,  
  Desc=1.1.1 UUID-0005 Session rotation not specified,  
  Status=NewIssue, Impact=Medium,  
  Recommendation=Implement session rotation and rotatedAt field
* gapID=2ac8a1, gapType=SecurityGap,  
  Desc=1.1.1 UUID-0004 Server-side deletionNonce missing,  
  Status=NewIssue, Impact=Medium,  
  Recommendation=Add deletionNonce TTL verification in API-Service

### Lessons learned – Initiating / Mini 2

- global-1: Standardise UUID identifiers across artifacts because ensure stable keys  
- global-2: Require a minimal security baseline and map it into each module's DevSecOps / Security column (Whole artifact)

### Lessons learned – Initiating / Mini 2

- global-1: Standardise UUID identifiers across artifacts because ensure stable keys  
- global-2: Require a minimal security baseline and map it into each module's DevSecOps / Security column (Whole artifact)

* (Teacher doc) End of Mini-Iteration 2 (Phase=Initiating, Macro=1):  
  Root causes identified:  
  - global-1: UUIDv7 identifiers chosen because sortable time-based  
  - global-2: Security baseline mandated because crypto/compliance rule  
  - 1.1.0: Security baseline partial because consolidated baseline and traceability missing  
  - 1.1.1: Module security controls unspecified because table lacks DevSecOps/Security column  
    
  Lessons learned:  
  - global-1: Adopt UUIDv7 across services because sortable time-based  
  - global-2: Enforce project security baseline across modules because crypto/compliance rule  
  - 1.1.0: Centralise full security/privacy baseline here and link controls to Related Reqs (Whole artifact)  
  - 1.1.1: Add DevSecOps/Security column and require explicit controls per module e.g. lockout, session-rotation, deletionNonce (DevSecOps / Security)

## Phase: FeasibilityStudy

* Artifact: 1.1.1.1, Phase=FeasibilityStudy, mini\_iter=1
* gapID=d6e0ba, gapType=MissedRequirement,  
  Desc=1.1.0 Whole artifact cross-artifact missing security/privacy baselines,  
  Status=Resolved, Impact=Low,  
  Recommendation=Add session/cookie flags, timeouts, MFA, consent, retention, audit
* gapID=0a5003, gapType=SecurityGap,  
  Desc=1.1.1.1 FR-005 I-5 Missing rate-limit,  
  Status=KnownIssue, Impact=High,  
  Recommendation=Add throttling for POST /feedback; define thresholds
* gapID=9d77eb, gapType=SecurityGap,  
  Desc=1.1.1.1 FR-025 I-25 Missing session rotation,  
  Status=KnownIssue, Impact=Medium,  
  Recommendation=Define session rotation policy and rotatedAt field
* gapID=2ac8a1, gapType=SecurityGap,  
  Desc=1.1.1.1 FR-022 I-22 deletionNonce partial,  
  Status=InProgress, Impact=Medium,  
  Recommendation=Add deletionNonce TTL verification in API-Service
* Artifact: 1.1.2, Phase=FeasibilityStudy, mini\_iter=1
* gapID=0a5003, gapType=SecurityGap,  
  Desc=1.1.2 Feedback Submission rate-limit missing,  
  Status=KnownIssue, Impact=High,  
  Recommendation=Define rate-limit policy and thresholds for POST /feedback
* gapID=2ac8a1, gapType=SecurityGap,  
  Desc=1.1.2 Admin UI: Feedback Management deletionNonce missing,  
  Status=KnownIssue, Impact=Medium,  
  Recommendation=Add server-side deletionNonce with TTL and verification
* gapID=9d77eb, gapType=SecurityGap,  
  Desc=1.1.2 Admin Access & Auth session rotation unspecified,  
  Status=KnownIssue, Impact=Medium,  
  Recommendation=Specify session rotation mechanism and rotation TTL

### Lessons learned – FeasibilityStudy / Mini 1

- global-1: Adopt UUIDv7 across services because sortable time-based  
- global-2: Enforce project security baseline across modules because crypto/compliance rule  
- 1.1.0: Centralise full security/privacy baseline here and link controls to Related Reqs (Whole artifact)  
- 1.1.1: Add DevSecOps/Security column and require explicit controls per module e.g. lockout, session-rotation, deletionNonce (DevSecOps / Security)

### Lessons learned – FeasibilityStudy / Mini 1

- global-1: Adopt UUIDv7 across services because sortable time-based  
- global-2: Enforce project security baseline across modules because crypto/compliance rule  
- 1.1.0: Centralise full security/privacy baseline here and link controls to Related Reqs (Whole artifact)  
- 1.1.1: Add DevSecOps/Security column and require explicit controls per module e.g. lockout, session-rotation, deletionNonce (DevSecOps / Security)

* (Teacher doc) End of Mini-Iteration 1 (Phase=FeasibilityStudy, Macro=1):  
  Root causes identified:  
  - global-1: UUIDv7 chosen because sortable, time-based  
  - global-2: Security baseline mandated because cookie flags,MFA enforced  
  - 1.1.0: Security/privacy baseline not consolidated so controls not traceable (Related Reqs)  
  - 1.1.2: Artifact tables allow ad-hoc security entries so feature controls missing (DevSecOps / Security)  
    
  Lessons learned:  
  - global-1: Adopt UUIDv7 across artifacts because sortable, time-based  
  - global-2: Require and enforce project security baseline because cookie flags,MFA enforced  
  - 1.1.0: Populate security/privacy baseline rows and link each control to Related Reqs (Related Reqs)  
  - 1.1.2: Require explicit per-feature control checklist entries in DevSecOps / Security (DevSecOps / Security)
* Artifact: 1.1.1.1, Phase=FeasibilityStudy, mini\_iter=2
* gapID=0a5003, gapType=SecurityGap,  
  Desc=1.1.2 Feedback Submission rate-limit missing,  
  Status=Resolved, Impact=High,  
  Recommendation=Define rate-limit policy and thresholds for POST /feedback
* gapID=9d77eb, gapType=SecurityGap,  
  Desc=1.1.2 Admin Access & Auth session rotation unspecified,  
  Status=InProgress, Impact=Medium,  
  Recommendation=Specify session rotation mechanism and rotation TTL
* gapID=2ac8a1, gapType=SecurityGap,  
  Desc=1.1.2 Admin UI: Feedback Management deletionNonce missing,  
  Status=Resolved, Impact=Medium,  
  Recommendation=Add server-side deletionNonce with TTL and verification
* gapID=7f6e8d, gapType=SecurityGap,  
  Desc=1.1.1.1 Whole artifact CSRF token not specified cross-artifact,  
  Status=NewIssue, Impact=Medium,  
  Recommendation=Add CSRF tokens or same-site anti-CSRF for admin flows
* gapID=2f71be, gapType=MissedRequirement,  
  Desc=1.1.1.1 FR-005 Decision metric lacks instrumentation owner,  
  Status=NewIssue, Impact=Medium,  
  Recommendation=Assign instrumentation owner and source for rate-limit metric
* Artifact: 1.1.2, Phase=FeasibilityStudy, mini\_iter=2
* gapID=0a5003, gapType=SecurityGap,  
  Desc=1.1.1 UUID-0002 Missing rate-limit for submissions,  
  Status=Resolved, Impact=High,  
  Recommendation=Add rate-limit/backoff at API-Service
* gapID=2ac8a1, gapType=SecurityGap,  
  Desc=1.1.1 UUID-0004 Server-side deletionNonce missing,  
  Status=Resolved, Impact=Medium,  
  Recommendation=Add deletionNonce TTL verification in API-Service
* gapID=9d77eb, gapType=SecurityGap,  
  Desc=1.1.1 UUID-0005 Session rotation not specified,  
  Status=Resolved, Impact=Medium,  
  Recommendation=Implement session rotation and rotatedAt field
* gapID=7f6e8d, gapType=SecurityGap,  
  Desc=1.1.2 Whole artifact cross-artifact CSRF missing,  
  Status=KnownIssue, Impact=Medium,  
  Recommendation=Add CSRF tokens or same-site anti-CSRF for admin flows
* gapID=2f71be, gapType=MissedRequirement,  
  Desc=1.1.2 Feedback Submission metric instrumentation owner missing,  
  Status=KnownIssue, Impact=Medium,  
  Recommendation=Assign instrumentation owner and source for rate-limit metric

### Lessons learned – FeasibilityStudy / Mini 2

- global-1: Adopt UUIDv7 across artifacts because sortable, time-based  
- global-2: Require and enforce project security baseline because cookie flags,MFA enforced  
- 1.1.0: Populate security/privacy baseline rows and link each control to Related Reqs (Related Reqs)  
- 1.1.2: Require explicit per-feature control checklist entries in DevSecOps / Security (DevSecOps / Security)

### Lessons learned – FeasibilityStudy / Mini 2

- global-1: Adopt UUIDv7 across artifacts because sortable, time-based  
- global-2: Require and enforce project security baseline because cookie flags,MFA enforced  
- 1.1.0: Populate security/privacy baseline rows and link each control to Related Reqs (Related Reqs)  
- 1.1.2: Require explicit per-feature control checklist entries in DevSecOps / Security (DevSecOps / Security)

* (Teacher doc) End of Mini-Iteration 2 (Phase=FeasibilityStudy, Macro=1):  
  Root causes identified:  
  - global-1: POST /feedback rate-limit chosen because protect from abuse  
  - global-2: Session rotation policy chosen because enforce token renewal  
  - global-3: Security controls fragmented across artifacts causing missing protections  
  - 1.1.1.1: Components lack mapped security controls and owners (Whole artifact)  
  - 1.1.2: Domain context omits concrete controls and owners in DevSecOps / Security (DevSecOps / Security)  
    
  Lessons learned:  
  - global-1: Apply and document rate-limit for POST /feedback across artifacts because protect from abuse  
  - global-2: Implement session-rotation with rotatedAt and TTL and document token renewal because enforce token renewal  
  - global-3: Standardise a minimal security checklist and require DevSecOps entries across artifacts to ensure consistent controls  
  - 1.1.1.1: Map every component to a security control and owner and reference Related Reqs (Whole artifact)  
  - 1.1.2: Record rate-limit,deletionNonce,session-rotation,CSRF,and metrics owner in DevSecOps / Security (DevSecOps / Security)
* Feedback Implementation Rate: 0.0%
* Mean Closure Time: 3.0 iteration(s)
* Macro Iteration 1 Summary:
* Total new issues: 6
* Total known (carried in) issues: 0
* Total in-progress: 1
* Total resolved: 3

## Lessons Learned (Macro Iteration 1)

Phase=Initiating, mini=1:  
Root causes identified:  
- global-1: UUID identifiers chosen because ensure stable keys  
- global-2: Lack of unified security baseline causes inconsistent module security expectations  
  
Lessons learned:  
- global-1: Standardise UUID identifiers across artifacts because ensure stable keys  
- global-2: Require a minimal security baseline and map it into each module's DevSecOps / Security column (Whole artifact)  
--  
Phase=Initiating, mini=2:  
Root causes identified:  
- global-1: UUIDv7 identifiers chosen because sortable time-based  
- global-2: Security baseline mandated because crypto/compliance rule  
- 1.1.0: Security baseline partial because consolidated baseline and traceability missing  
- 1.1.1: Module security controls unspecified because table lacks DevSecOps/Security column  
  
Lessons learned:  
- global-1: Adopt UUIDv7 across services because sortable time-based  
- global-2: Enforce project security baseline across modules because crypto/compliance rule  
- 1.1.0: Centralise full security/privacy baseline here and link controls to Related Reqs (Whole artifact)  
- 1.1.1: Add DevSecOps/Security column and require explicit controls per module e.g. lockout, session-rotation, deletionNonce (DevSecOps / Security)  
--  
Phase=FeasibilityStudy, mini=1:  
Root causes identified:  
- global-1: UUIDv7 chosen because sortable, time-based  
- global-2: Security baseline mandated because cookie flags,MFA enforced  
- 1.1.0: Security/privacy baseline not consolidated so controls not traceable (Related Reqs)  
- 1.1.2: Artifact tables allow ad-hoc security entries so feature controls missing (DevSecOps / Security)  
  
Lessons learned:  
- global-1: Adopt UUIDv7 across artifacts because sortable, time-based  
- global-2: Require and enforce project security baseline because cookie flags,MFA enforced  
- 1.1.0: Populate security/privacy baseline rows and link each control to Related Reqs (Related Reqs)  
- 1.1.2: Require explicit per-feature control checklist entries in DevSecOps / Security (DevSecOps / Security)  
--  
Phase=FeasibilityStudy, mini=2:  
Root causes identified:  
- global-1: POST /feedback rate-limit chosen because protect from abuse  
- global-2: Session rotation policy chosen because enforce token renewal  
- global-3: Security controls fragmented across artifacts causing missing protections  
- 1.1.1.1: Components lack mapped security controls and owners (Whole artifact)  
- 1.1.2: Domain context omits concrete controls and owners in DevSecOps / Security (DevSecOps / Security)  
  
Lessons learned:  
- global-1: Apply and document rate-limit for POST /feedback across artifacts because protect from abuse  
- global-2: Implement session-rotation with rotatedAt and TTL and document token renewal because enforce token renewal  
- global-3: Standardise a minimal security checklist and require DevSecOps entries across artifacts to ensure consistent controls  
- 1.1.1.1: Map every component to a security control and owner and reference Related Reqs (Whole artifact)  
- 1.1.2: Record rate-limit,deletionNonce,session-rotation,CSRF,and metrics owner in DevSecOps / Security (DevSecOps / Security)

# Macro Iteration 2

## Phase: Initiating

* Artifact: 1.1.0, Phase=Initiating, mini\_iter=1
* gapID=0a5003, gapType=SecurityGap,  
  Desc=1.1.1 UUID-0002 Missing rate-limit for submissions,  
  Status=Resolved, Impact=High,  
  Recommendation=Add rate-limit/backoff at API-Service
* gapID=9d77eb, gapType=SecurityGap,  
  Desc=1.1.0 Session rotation policy I-? InProgress,  
  Status=Resolved, Impact=Medium,  
  Recommendation=Specify session rotation mechanism and rotation TTL
* gapID=2ac8a1, gapType=SecurityGap,  
  Desc=1.1.1 UUID-0004 Server-side deletionNonce missing,  
  Status=KnownIssue, Impact=Medium,  
  Recommendation=Add deletionNonce TTL verification in API-Service
* gapID=7f6e8d, gapType=SecurityGap,  
  Desc=1.1.0 Whole artifact cross-artifact CSRF missing,  
  Status=Resolved, Impact=Medium,  
  Recommendation=Add CSRF tokens or same-site anti-CSRF for admin flows
* gapID=2f71be, gapType=MissedRequirement,  
  Desc=1.1.0 Submission reliability instrumentation owner missing,  
  Status=KnownIssue, Impact=Medium,  
  Recommendation=Assign instrumentation owner and source for rate-limit metric
* Artifact: 1.1.1, Phase=Initiating, mini\_iter=1
* gapID=7f6e8d, gapType=SecurityGap,  
  Desc=1.1.1.1 Whole artifact CSRF token not specified cross-artifact,  
  Status=Resolved, Impact=Medium,  
  Recommendation=Add CSRF tokens or same-site anti-CSRF for admin flows
* gapID=2f71be, gapType=MissedRequirement,  
  Desc=1.1.1 M-1 Decision metric missing owner,  
  Status=KnownIssue, Impact=Medium,  
  Recommendation=Assign instrumentation owner and source for rate-limit metric
* gapID=9d77eb, gapType=SecurityGap,  
  Desc=1.1.1 UUID-0005 Session rotation not specified,  
  Status=Resolved, Impact=Medium,  
  Recommendation=Implement session rotation and rotatedAt field
* gapID=2ac8a1, gapType=SecurityGap,  
  Desc=1.1.1 M-2 deletionNonce partial fix,  
  Status=Resolved, Impact=Medium,  
  Recommendation=Add deletionNonce TTL verification in API-Service

### Lessons learned – Initiating / Mini 1

- global-1: Apply and document rate-limit for POST /feedback across artifacts because protect from abuse  
- global-2: Implement session-rotation with rotatedAt and TTL and document token renewal because enforce token renewal  
- global-3: Standardise a minimal security checklist and require DevSecOps entries across artifacts to ensure consistent controls  
- 1.1.1.1: Map every component to a security control and owner and reference Related Reqs (Whole artifact)  
- 1.1.2: Record rate-limit,deletionNonce,session-rotation,CSRF,and metrics owner in DevSecOps / Security (DevSecOps / Security)

### Lessons learned – Initiating / Mini 1

- global-1: Apply and document rate-limit for POST /feedback across artifacts because protect from abuse  
- global-2: Implement session-rotation with rotatedAt and TTL and document token renewal because enforce token renewal  
- global-3: Standardise a minimal security checklist and require DevSecOps entries across artifacts to ensure consistent controls  
- 1.1.1.1: Map every component to a security control and owner and reference Related Reqs (Whole artifact)  
- 1.1.2: Record rate-limit,deletionNonce,session-rotation,CSRF,and metrics owner in DevSecOps / Security (DevSecOps / Security)

* (Teacher doc) End of Mini-Iteration 1 (Phase=Initiating, Macro=2):  
  Root causes identified:  
  - global-1: rate-limit POST because prevent abuse  
  - global-2: session-rotation tokens because enforce TTL  
  - global-3: security controls fragmented because missing baselines and cross-artifact tokens  
  - 1.1.1: module security entries inconsistent because DevSecOps / Security column not enforced per module  
  - 1.1.1.1: metrics lack owner because Potential Metrics entries omit owner field  
    
  Lessons learned:  
  - global-1: enforce rate-limit for POST/feedback across artifacts because prevent abuse  
  - global-2: require session-rotation token TTL across artifacts because enforce TTL  
  - global-3: harmonise security baseline and specify CSRF/session controls across artifacts (Whole artifact)  
  - 1.1.1: require a populated DevSecOps / Security cell for every module before acceptance (DevSecOps / Security)  
  - 1.1.1.1: assign owner and acceptance criteria for each Potential Metrics entry (Potential Metrics)
* Artifact: 1.1.0, Phase=Initiating, mini\_iter=2
* gapID=9d77eb, gapType=SecurityGap,  
  Desc=1.1.1 UUID-0005 Session rotation not specified,  
  Status=Resolved, Impact=Medium,  
  Recommendation=Implement session rotation and rotatedAt field
* gapID=2ac8a1, gapType=SecurityGap,  
  Desc=1.1.1 M-2 deletionNonce partial fix,  
  Status=InProgress, Impact=Medium,  
  Recommendation=Add deletionNonce TTL verification in API-Service
* gapID=7f6e8d, gapType=SecurityGap,  
  Desc=1.1.1.1 Whole artifact CSRF token not specified cross-artifact,  
  Status=Resolved, Impact=Medium,  
  Recommendation=Add CSRF tokens or same-site anti-CSRF for admin flows
* gapID=2f71be, gapType=MissedRequirement,  
  Desc=1.1.1 M-1 Decision metric missing owner,  
  Status=Resolved, Impact=Medium,  
  Recommendation=Assign instrumentation owner and source for rate-limit metric
* gapID=5fe616, gapType=MissedRequirement,  
  Desc=1.1.0 Related Reqs placeholders,  
  Status=NewIssue, Impact=Medium,  
  Recommendation=Populate Related Reqs with requirement IDs per row
* Artifact: 1.1.1, Phase=Initiating, mini\_iter=2
* gapID=2f71be, gapType=MissedRequirement,  
  Desc=1.1.1.1 FR-005 Decision metric lacks instrumentation owner,  
  Status=Resolved, Impact=Medium,  
  Recommendation=Assign instrumentation owner and source for rate-limit metric
* gapID=2ac8a1, gapType=SecurityGap,  
  Desc=1.1.1 M-4 Server-side deletionNonce missing,  
  Status=InProgress, Impact=Medium,  
  Recommendation=Add deletionNonce TTL verification in API-Service
* gapID=5fe616, gapType=MissedRequirement,  
  Desc=1.1.1 M-3 Related Reqs placeholders present,  
  Status=KnownIssue, Impact=Medium,  
  Recommendation=Populate Related Reqs with requirement IDs per row
* gapID=d0923d, gapType=MissedRequirement,  
  Desc=1.1.1 M-2 Email storage method conflict,  
  Status=NewIssue, Impact=Medium,  
  Recommendation=Use deterministic encryption for emails

### Lessons learned – Initiating / Mini 2

- global-1: enforce rate-limit for POST/feedback across artifacts because prevent abuse  
- global-2: require session-rotation token TTL across artifacts because enforce TTL  
- global-3: harmonise security baseline and specify CSRF/session controls across artifacts (Whole artifact)  
- 1.1.1: require a populated DevSecOps / Security cell for every module before acceptance (DevSecOps / Security)  
- 1.1.1.1: assign owner and acceptance criteria for each Potential Metrics entry (Potential Metrics)

### Lessons learned – Initiating / Mini 2

- global-1: enforce rate-limit for POST/feedback across artifacts because prevent abuse  
- global-2: require session-rotation token TTL across artifacts because enforce TTL  
- global-3: harmonise security baseline and specify CSRF/session controls across artifacts (Whole artifact)  
- 1.1.1: require a populated DevSecOps / Security cell for every module before acceptance (DevSecOps / Security)  
- 1.1.1.1: assign owner and acceptance criteria for each Potential Metrics entry (Potential Metrics)

* (Teacher doc) End of Mini-Iteration 2 (Phase=Initiating, Macro=2):  
  Root causes identified:  
  - global-1: inconsistent security-control specification across artifacts causing cross-artifact security gaps  
  - global-2: metrics and ownership not assigned across modules and components causing unowned metrics and unclear SRE responsibilities  
  - 1.1.1.1: component-level requirements lack required security attributes and protections (nonce, rate-limit, session-rotation)  
    
  Lessons learned:  
  - global-1: adopt a project-wide security-control checklist and enforce entries in DevSecOps / Security and Related Reqs because enforceable baseline  
  - global-2: mandate metric owner and map Potential Metrics to an owner on each module/component (Potential Metrics)  
  - 1.1.1.1: require every Requirement ID row to declare DevSecOps / Security, Related Reqs, and Potential Metrics before acceptance (DevSecOps / Security, Related Reqs, Potential Metrics)

## Phase: FeasibilityStudy

* Artifact: 1.1.1.1, Phase=FeasibilityStudy, mini\_iter=1
* gapID=2ac8a1, gapType=SecurityGap,  
  Desc=1.1.1.1 FR-022 I-22 deletionNonce partial,  
  Status=Resolved, Impact=Medium,  
  Recommendation=Add deletionNonce TTL verification in API-Service
* gapID=2f71be, gapType=MissedRequirement,  
  Desc=1.1.1.1 FR-005 Decision metric lacks instrumentation owner,  
  Status=Resolved, Impact=Medium,  
  Recommendation=Assign instrumentation owner and source for rate-limit metric
* gapID=5fe616, gapType=MissedRequirement,  
  Desc=1.1.1 M-3 Related Reqs placeholders present,  
  Status=Resolved, Impact=Medium,  
  Recommendation=Populate Related Reqs with requirement IDs per row
* gapID=d0923d, gapType=MissedRequirement,  
  Desc=1.1.1.1 FR-003 Encryption vs hashing inconsistency,  
  Status=KnownIssue, Impact=Medium,  
  Recommendation=Decide and document email storage method
* Artifact: 1.1.2, Phase=FeasibilityStudy, mini\_iter=1
* gapID=5fe616, gapType=MissedRequirement,  
  Desc=1.1.0 Related Reqs placeholders,  
  Status=Resolved, Impact=Medium,  
  Recommendation=Populate Related Reqs with requirement IDs per row
* gapID=2ac8a1, gapType=SecurityGap,  
  Desc=1.1.1 UUID-0004 Server-side deletionNonce missing,  
  Status=Resolved, Impact=Medium,  
  Recommendation=Add deletionNonce TTL verification in API-Service
* gapID=d0923d, gapType=MissedRequirement,  
  Desc=1.1.2 Optional Email Email storage conflict,  
  Status=KnownIssue, Impact=Medium,  
  Recommendation=Resolve encryption vs hashing; choose one method

### Lessons learned – FeasibilityStudy / Mini 1

- global-1: adopt a project-wide security-control checklist and enforce entries in DevSecOps / Security and Related Reqs because enforceable baseline  
- global-2: mandate metric owner and map Potential Metrics to an owner on each module/component (Potential Metrics)  
- 1.1.1.1: require every Requirement ID row to declare DevSecOps / Security, Related Reqs, and Potential Metrics before acceptance (DevSecOps / Security, Related Reqs, Potential Metrics)

### Lessons learned – FeasibilityStudy / Mini 1

- global-1: adopt a project-wide security-control checklist and enforce entries in DevSecOps / Security and Related Reqs because enforceable baseline  
- global-2: mandate metric owner and map Potential Metrics to an owner on each module/component (Potential Metrics)  
- 1.1.1.1: require every Requirement ID row to declare DevSecOps / Security, Related Reqs, and Potential Metrics before acceptance (DevSecOps / Security, Related Reqs, Potential Metrics)

* (Teacher doc) End of Mini-Iteration 1 (Phase=FeasibilityStudy, Macro=2):  
  Root causes identified:  
  - global-1: CSRF tokens for admin chosen because protect admin flows  
  - global-2: Security controls fragmented across modules causing missing rate-limit session-rotation CSRF deletionNonce  
  - global-3: Decision and telemetry metrics lack explicit owners causing unassigned instrumentation and poor traceability  
    
  Lessons learned:  
  - global-1: Enforce CSRF tokens for all admin interfaces across artifacts because protect admin flows  
  - global-2: Consolidate a project security baseline and require explicit DevSecOps / Security entries per component (DevSecOps / Security)  
  - global-3: Require a Metric Owner field and mandate owner assignment for each potential metric to ensure instrumentation (Potential Metrics)
* Artifact: 1.1.1.1, Phase=FeasibilityStudy, mini\_iter=2
* gapID=2ac8a1, gapType=SecurityGap,  
  Desc=1.1.1 UUID-0004 Server-side deletionNonce missing,  
  Status=InProgress, Impact=Medium,  
  Recommendation=Add deletionNonce TTL verification in API-Service
* gapID=5fe616, gapType=MissedRequirement,  
  Desc=1.1.0 Related Reqs placeholders,  
  Status=Resolved, Impact=Medium,  
  Recommendation=Populate Related Reqs with requirement IDs per row
* gapID=d0923d, gapType=MissedRequirement,  
  Desc=1.1.1.1 FR-003 Email storage method conflict,  
  Status=Resolved, Impact=Medium,  
  Recommendation=Align hashing vs encryption method; pick one and document
* Artifact: 1.1.2, Phase=FeasibilityStudy, mini\_iter=2
* gapID=d0923d, gapType=MissedRequirement,  
  Desc=1.1.1 M-2 Email storage method conflict,  
  Status=Resolved, Impact=Medium,  
  Recommendation=Use deterministic encryption for emails
* gapID=2ac8a1, gapType=SecurityGap,  
  Desc=1.1.1 UUID-0004 Server-side deletionNonce missing,  
  Status=Resolved, Impact=Medium,  
  Recommendation=Add deletionNonce TTL verification in API-Service

### Lessons learned – FeasibilityStudy / Mini 2

- global-1: Enforce CSRF tokens for all admin interfaces across artifacts because protect admin flows  
- global-2: Consolidate a project security baseline and require explicit DevSecOps / Security entries per component (DevSecOps / Security)  
- global-3: Require a Metric Owner field and mandate owner assignment for each potential metric to ensure instrumentation (Potential Metrics)

### Lessons learned – FeasibilityStudy / Mini 2

- global-1: Enforce CSRF tokens for all admin interfaces across artifacts because protect admin flows  
- global-2: Consolidate a project security baseline and require explicit DevSecOps / Security entries per component (DevSecOps / Security)  
- global-3: Require a Metric Owner field and mandate owner assignment for each potential metric to ensure instrumentation (Potential Metrics)

* (Teacher doc) End of Mini-Iteration 2 (Phase=FeasibilityStudy, Macro=2):  
  Root causes identified:  
  - global-1: Deterministic email encryption chosen because preserve contact capability  
  - global-2: UUIDv7 identifiers adopted because time-sortable IDs  
    
  Lessons learned:  
  - global-1: Standardise deterministic email encryption project-wide to preserve contact capability  
  - global-2: Adopt UUIDv7 for all identifiers to enable time-ordering and analytics
* Feedback Implementation Rate: 200.0%
* Mean Closure Time: 5.38 iteration(s)
* Macro Iteration 2 Summary:
* Total new issues: 2
* Total known (carried in) issues: 6
* Total in-progress: 0
* Total resolved: 8

## Lessons Learned (Macro Iteration 2)

Phase=Initiating, mini=1:  
Root causes identified:  
- global-1: rate-limit POST because prevent abuse  
- global-2: session-rotation tokens because enforce TTL  
- global-3: security controls fragmented because missing baselines and cross-artifact tokens  
- 1.1.1: module security entries inconsistent because DevSecOps / Security column not enforced per module  
- 1.1.1.1: metrics lack owner because Potential Metrics entries omit owner field  
  
Lessons learned:  
- global-1: enforce rate-limit for POST/feedback across artifacts because prevent abuse  
- global-2: require session-rotation token TTL across artifacts because enforce TTL  
- global-3: harmonise security baseline and specify CSRF/session controls across artifacts (Whole artifact)  
- 1.1.1: require a populated DevSecOps / Security cell for every module before acceptance (DevSecOps / Security)  
- 1.1.1.1: assign owner and acceptance criteria for each Potential Metrics entry (Potential Metrics)  
--  
Phase=Initiating, mini=2:  
Root causes identified:  
- global-1: inconsistent security-control specification across artifacts causing cross-artifact security gaps  
- global-2: metrics and ownership not assigned across modules and components causing unowned metrics and unclear SRE responsibilities  
- 1.1.1.1: component-level requirements lack required security attributes and protections (nonce, rate-limit, session-rotation)  
  
Lessons learned:  
- global-1: adopt a project-wide security-control checklist and enforce entries in DevSecOps / Security and Related Reqs because enforceable baseline  
- global-2: mandate metric owner and map Potential Metrics to an owner on each module/component (Potential Metrics)  
- 1.1.1.1: require every Requirement ID row to declare DevSecOps / Security, Related Reqs, and Potential Metrics before acceptance (DevSecOps / Security, Related Reqs, Potential Metrics)  
--  
Phase=FeasibilityStudy, mini=1:  
Root causes identified:  
- global-1: CSRF tokens for admin chosen because protect admin flows  
- global-2: Security controls fragmented across modules causing missing rate-limit session-rotation CSRF deletionNonce  
- global-3: Decision and telemetry metrics lack explicit owners causing unassigned instrumentation and poor traceability  
  
Lessons learned:  
- global-1: Enforce CSRF tokens for all admin interfaces across artifacts because protect admin flows  
- global-2: Consolidate a project security baseline and require explicit DevSecOps / Security entries per component (DevSecOps / Security)  
- global-3: Require a Metric Owner field and mandate owner assignment for each potential metric to ensure instrumentation (Potential Metrics)  
--  
Phase=FeasibilityStudy, mini=2:  
Root causes identified:  
- global-1: Deterministic email encryption chosen because preserve contact capability  
- global-2: UUIDv7 identifiers adopted because time-sortable IDs  
  
Lessons learned:  
- global-1: Standardise deterministic email encryption project-wide to preserve contact capability  
- global-2: Adopt UUIDv7 for all identifiers to enable time-ordering and analytics