FIG. 1

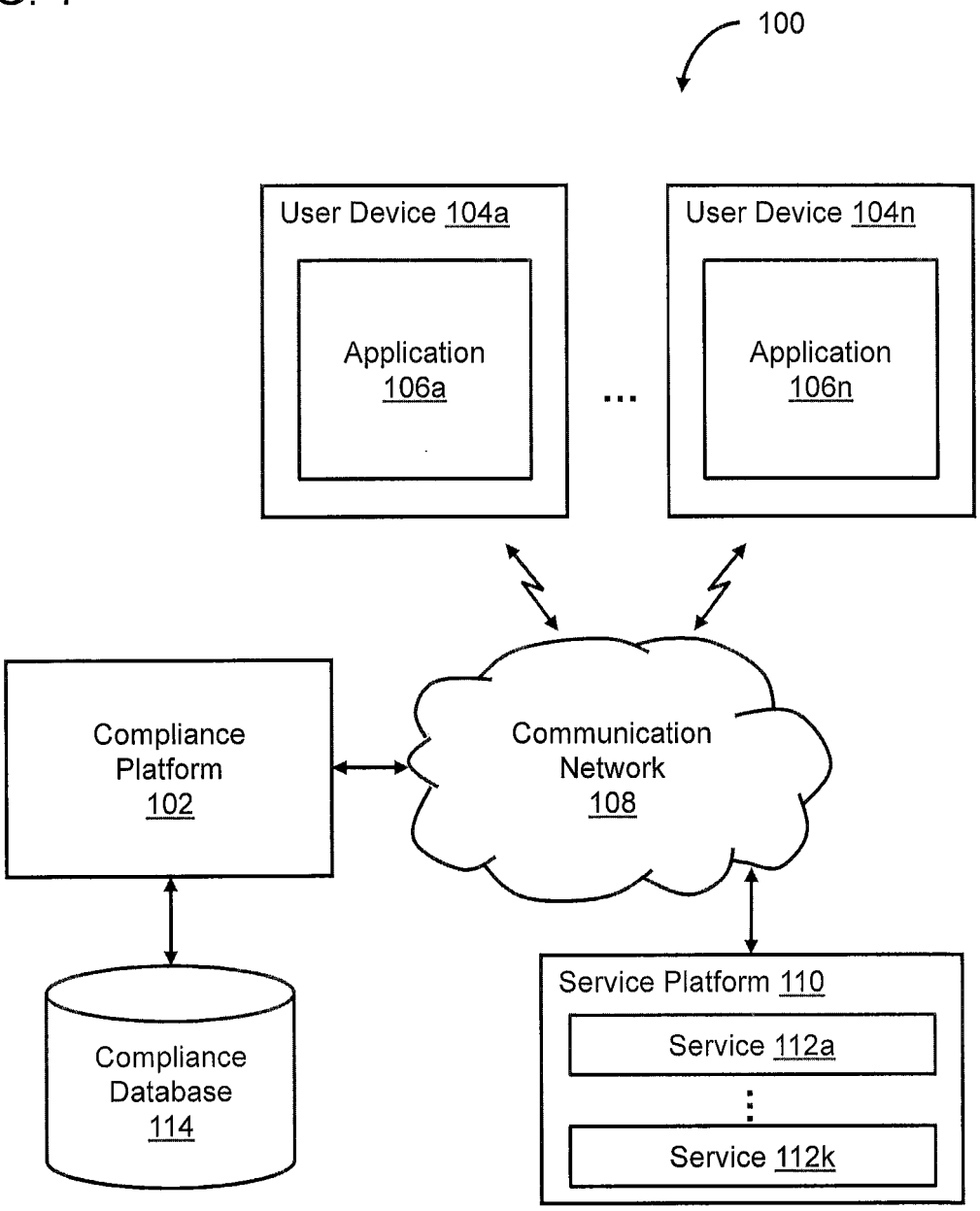

100
User Device 104a
Application 106a
...
User Device 104n
Application 106n
Compliance Platform 102
Communication Network 108
Compliance Database 114
Service Platform 110
Service 112a
Service 112k

FIG. 2

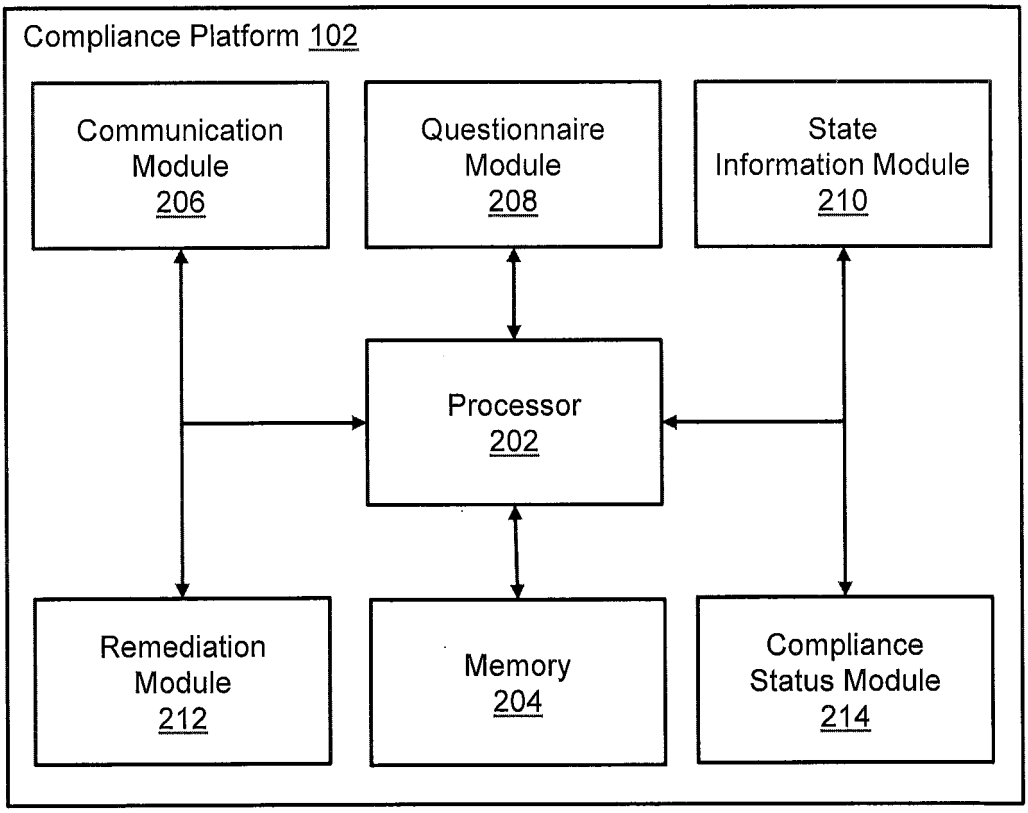

Compliance Platform 102
Communication Module 206
Questionnaire Module 208
State Information Module 210
Processor 202
Remediation Module 212
Memory 204
Compliance Status Module 214

FIG. 3

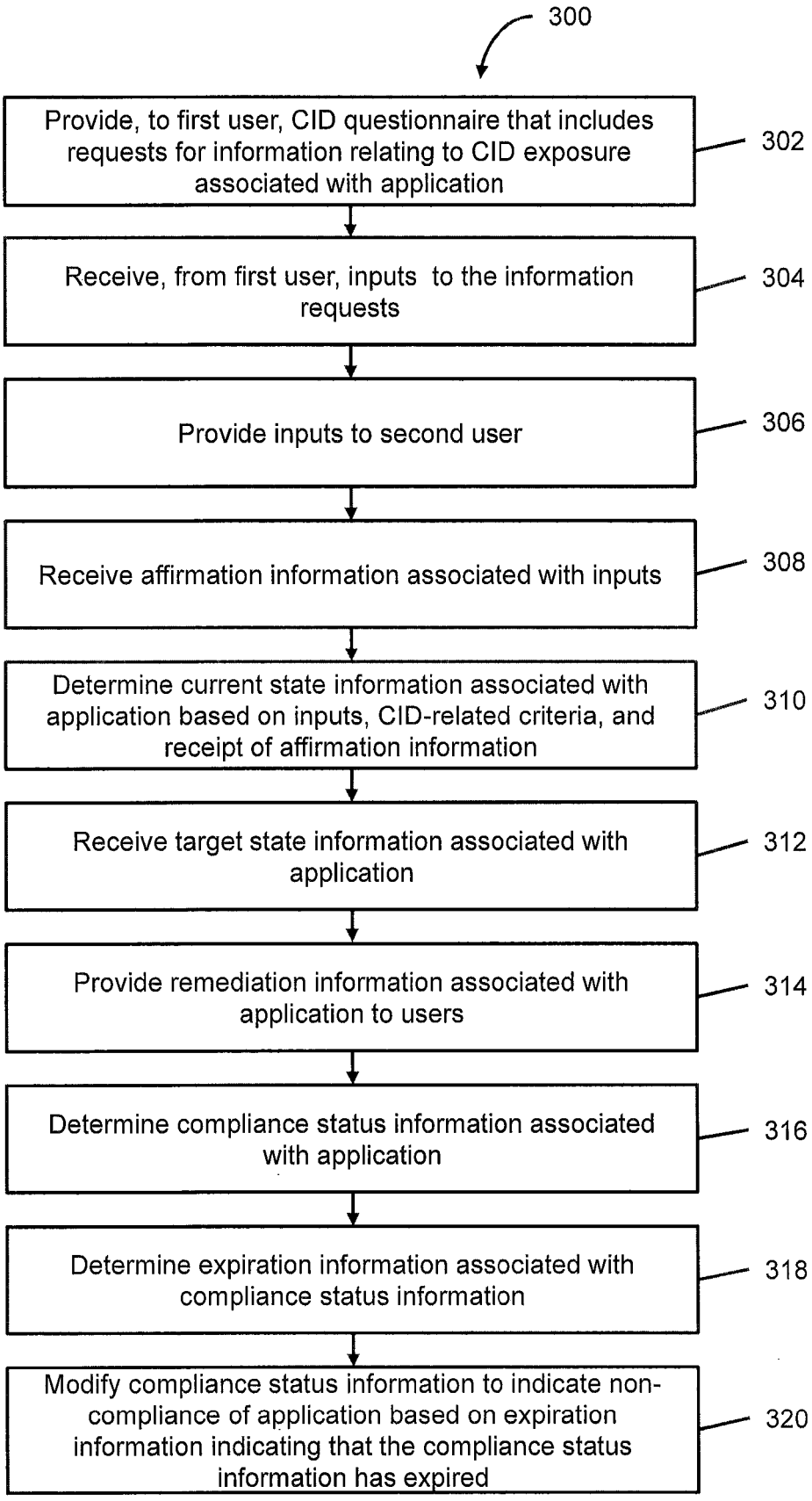

300
Provide, to first user, CID questionnaire that includes requests for information relating to CID exposure associated with application
302
Receive, from first user, inputs to the information requests
304
Provide inputs to second user
306
Receive affirmation information associated with inputs
308
Determine current state information associated with application based on inputs, CID-related criteria, and receipt of affirmation information
310
Receive target state information associated with application
312
Provide remediation information associated with application to users
314
Determine compliance status information associated with application
316
Determine expiration information associated with compliance status information
318
Modify compliance status information to indicate non-compliance of application based on expiration information indicating that the compliance status information has expired
320

FIG. 4

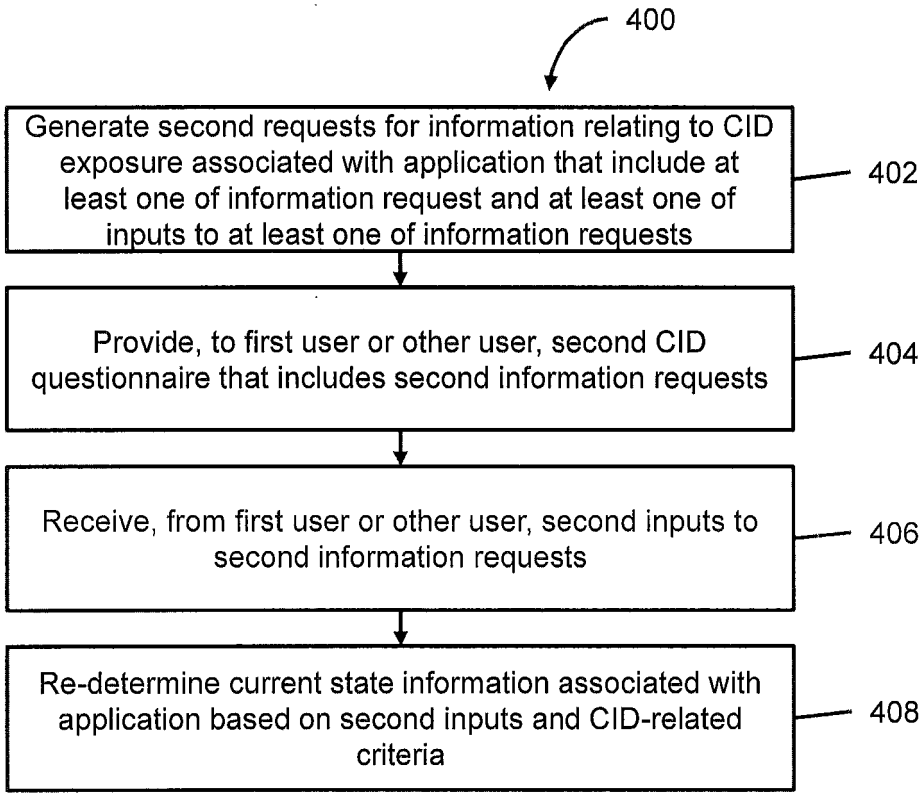

400
Generate second requests for information relating to CID exposure associated with application that include at least one of information request and at least one of inputs to at least one of information requests
402
Provide, to first user or other user, second CID questionnaire that includes second information requests
404
Receive, from first user or other user, second inputs to second information requests
406
Re-determine current state information associated with application based on second inputs and CID-related criteria
408

FIG. 5

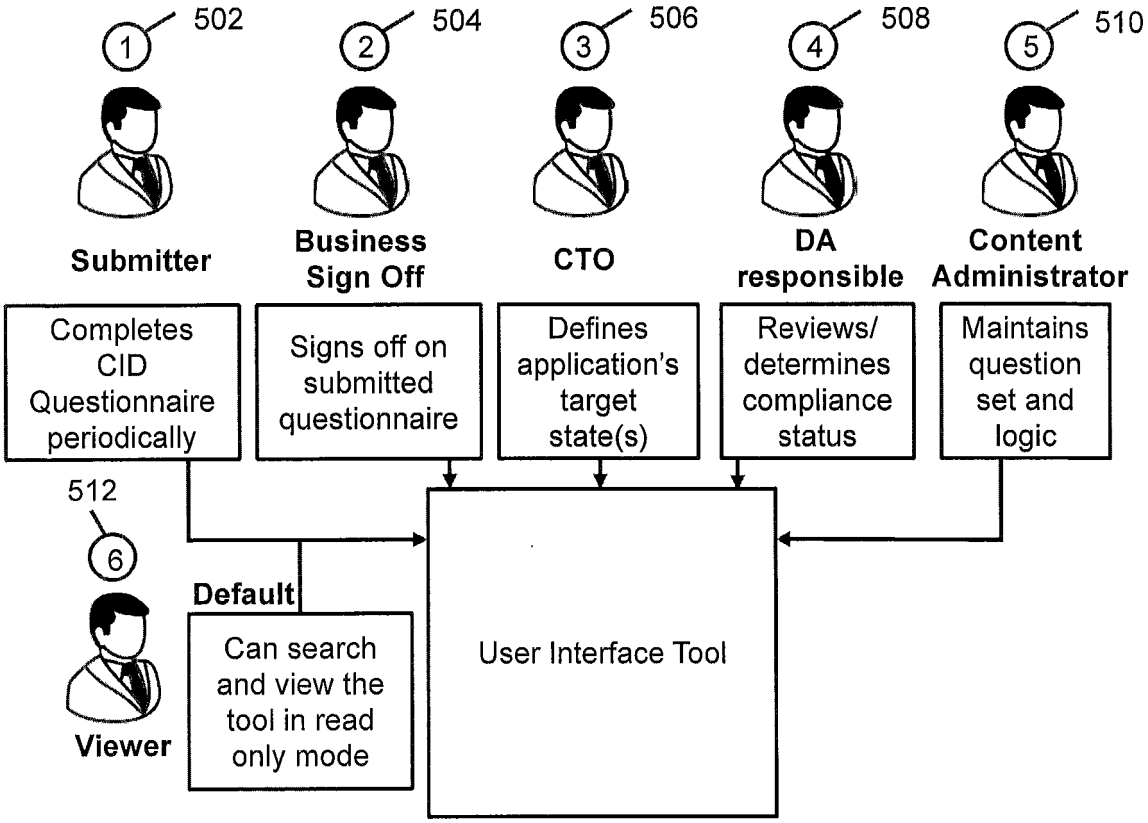

1
502
2
504
3
506
4
508
5
510
Submitter
Business Sign Off
CTO
DA responsible
Content Administrator
Completes CID Questionnaire periodically
Signs off on submitted questionnaire
Defines application's target state(s)
Reviews/ determines compliance status
Maintains question set and logic
512
6
Default
Viewer
Can search and view the tool in read only mode
User Interface Tool

FIG. 6

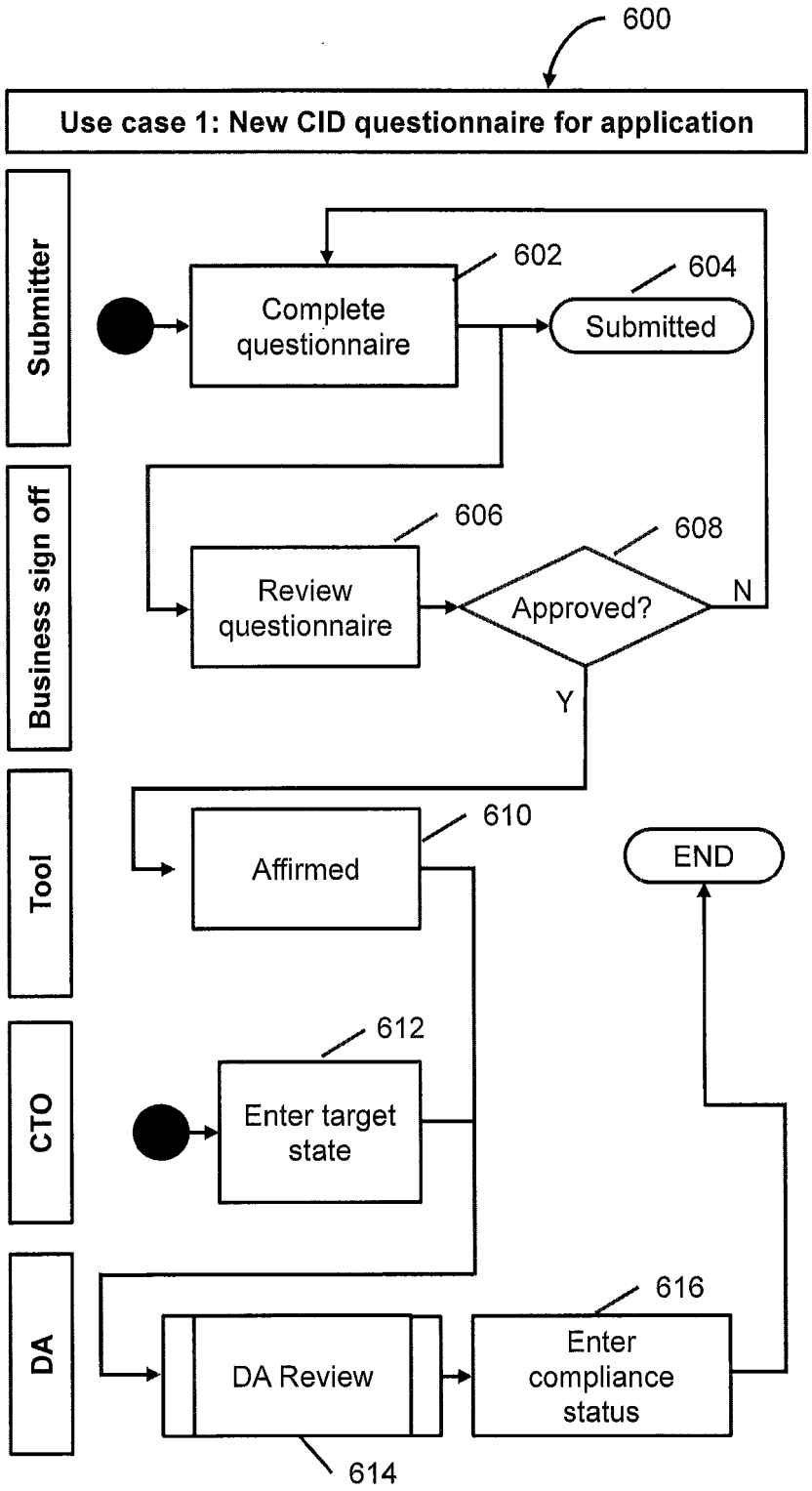

600
Use case 1: New CID questionnaire for application
Submitter
Business sign off
Tool
CTO
DA
Complete questionnaire
602
Submitted
604
Review questionnaire
606
Approved?
608
N
Y
Affirmed
610
END
Enter target state
612
DA Review
614
Enter compliance status
616

FIG. 7

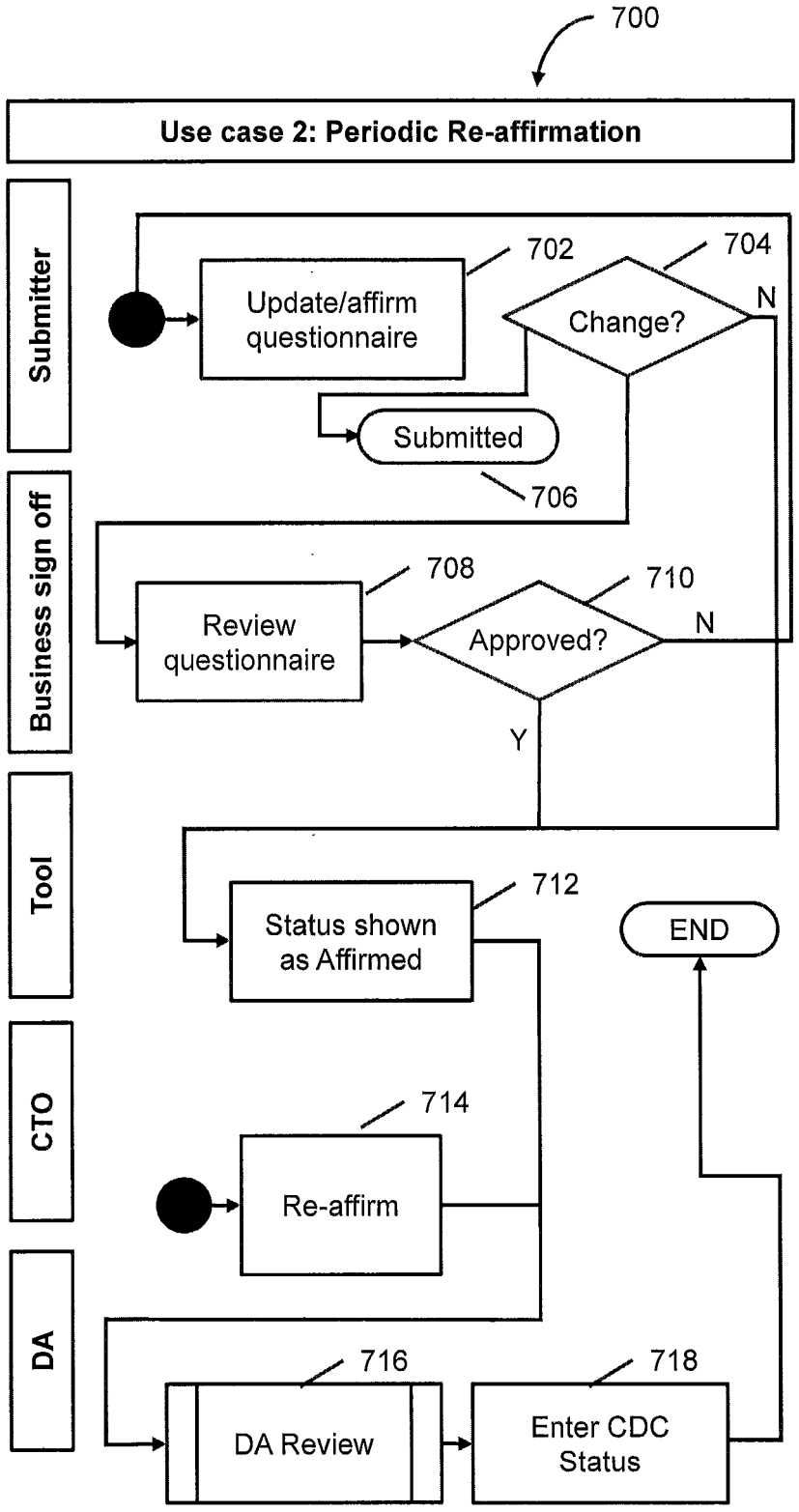

700
Use case 2: Periodic Re-affirmation
Submitter
Business sign off
Tool
CTO
DA
Update/affirm questionnaire
702
Change?
704
N
Submitted
706
Review questionnaire
708
Approved?
710
N
Y
Status shown as Affirmed
712
END
Re-affirm
714
DA Review
716
Enter CDC Status
718

FIG. 8

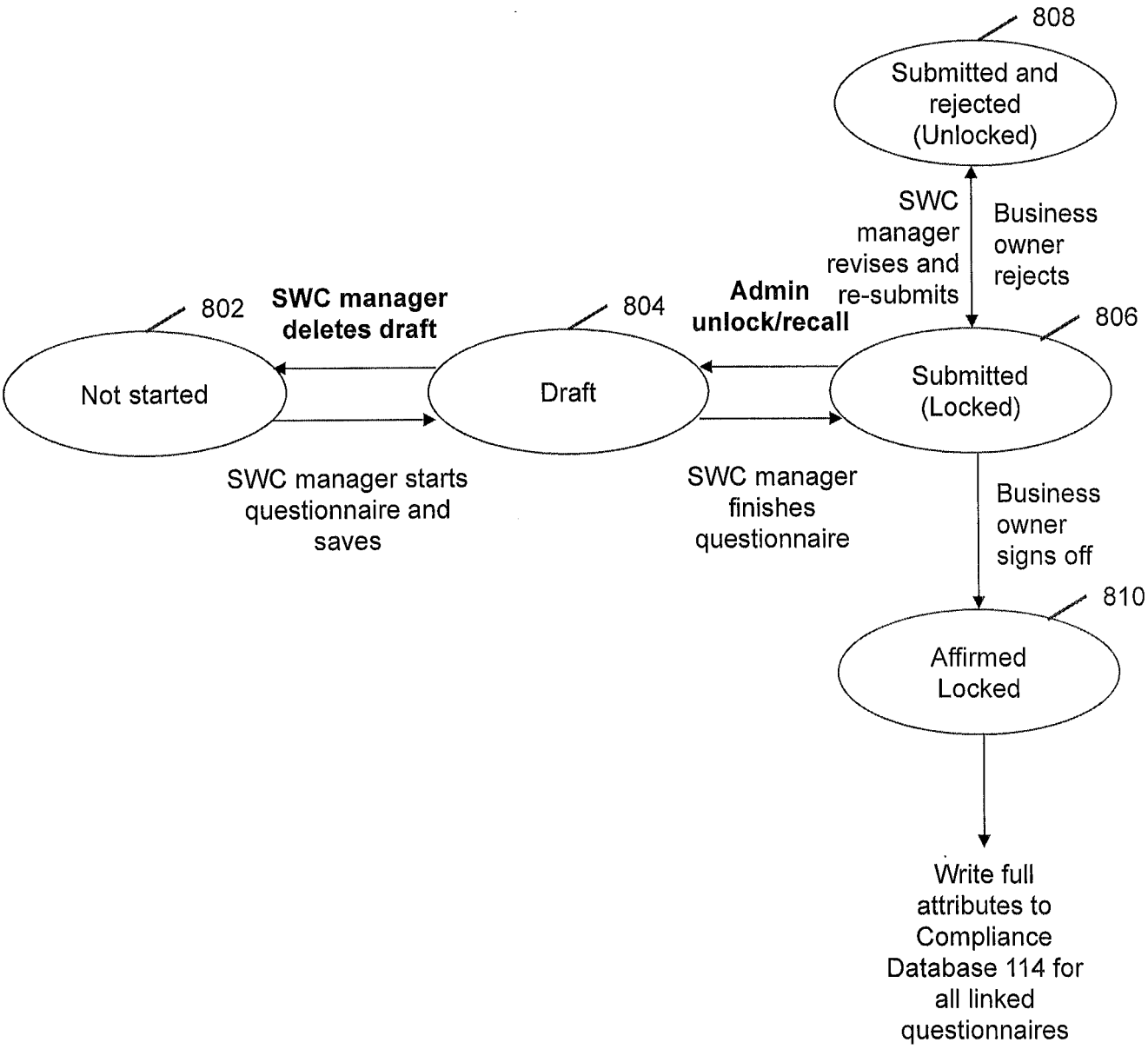

808
Submitted and rejected (Unlocked)
SWC manager revises and re-submits
Business owner rejects
802
SWC manager deletes draft
804
Admin unlock/recall
806
Not started
Draft
Submitted (Locked)
SWC manager starts questionnaire and saves
SWC manager finishes questionnaire
Business owner signs off
810
Affirmed Locked
Write full attributes to Compliance Database 114 for all linked questionnaires

FIG. 9

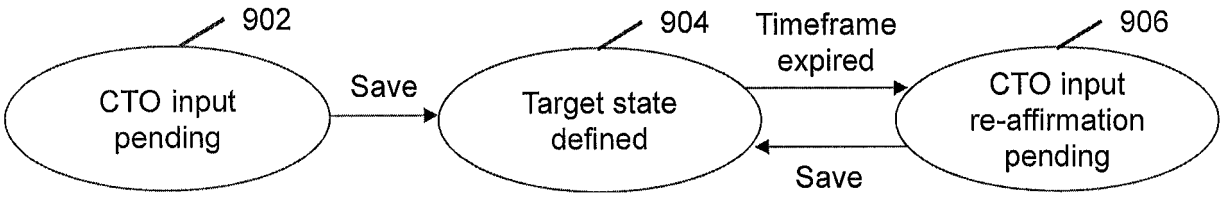

902
CTO input pending
Save
904
Target state defined
Timeframe expired
Save
906
CTO input re-affirmation pending

FIG. 10

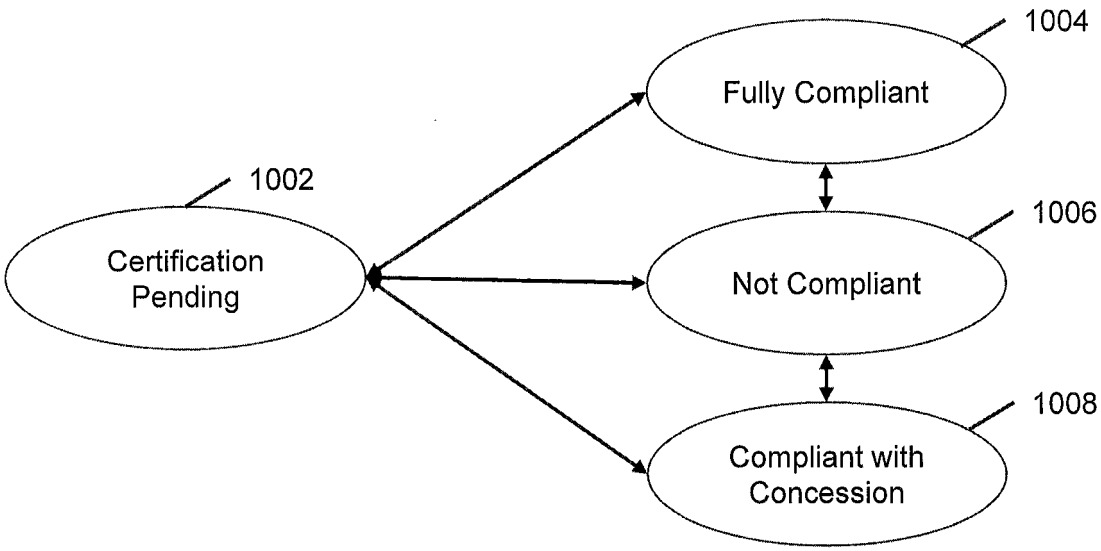

1004
Fully Compliant
1002
Certification Pending
1006
Not Compliant
1008
Compliant with Concession

FIG. 11

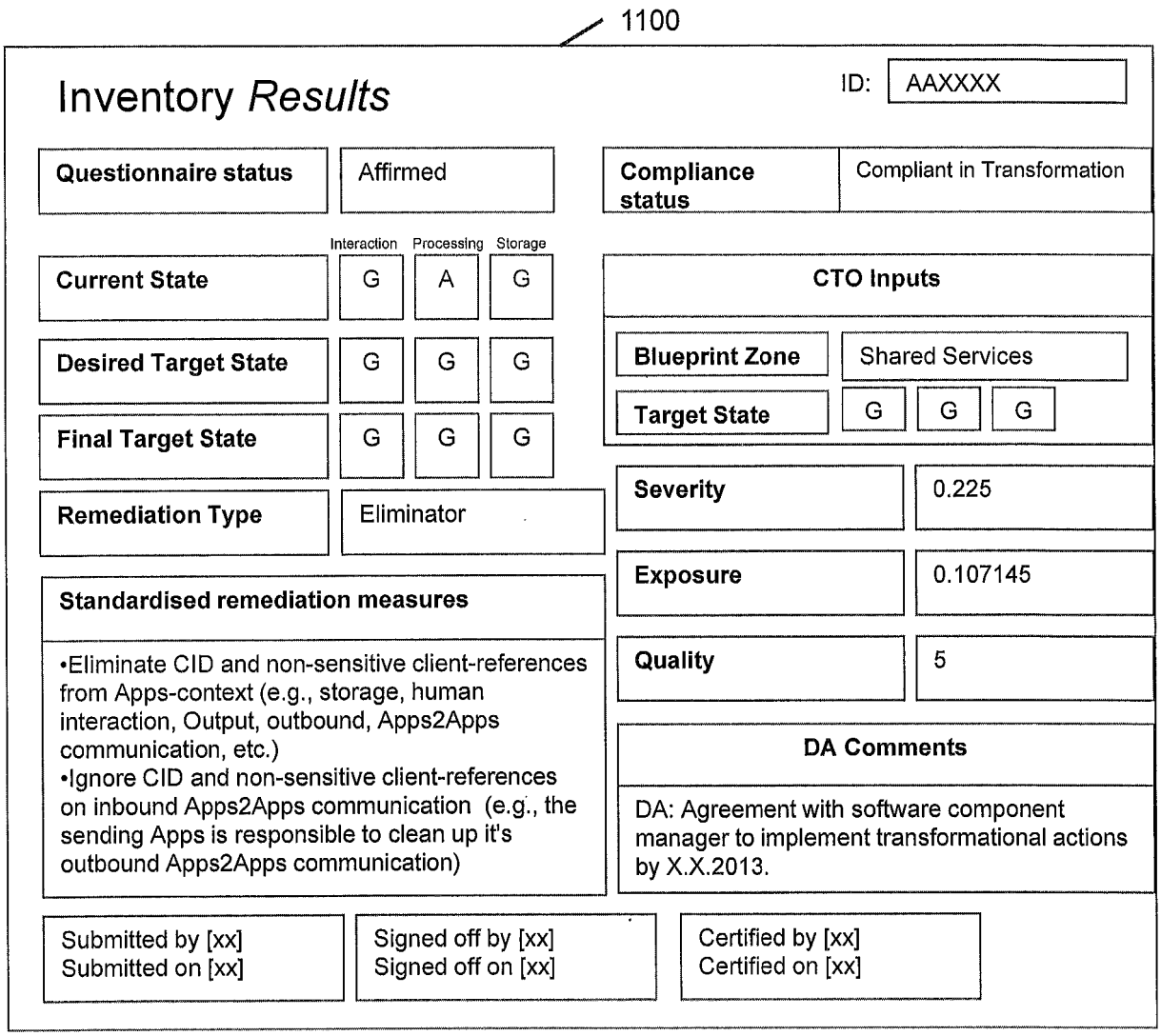
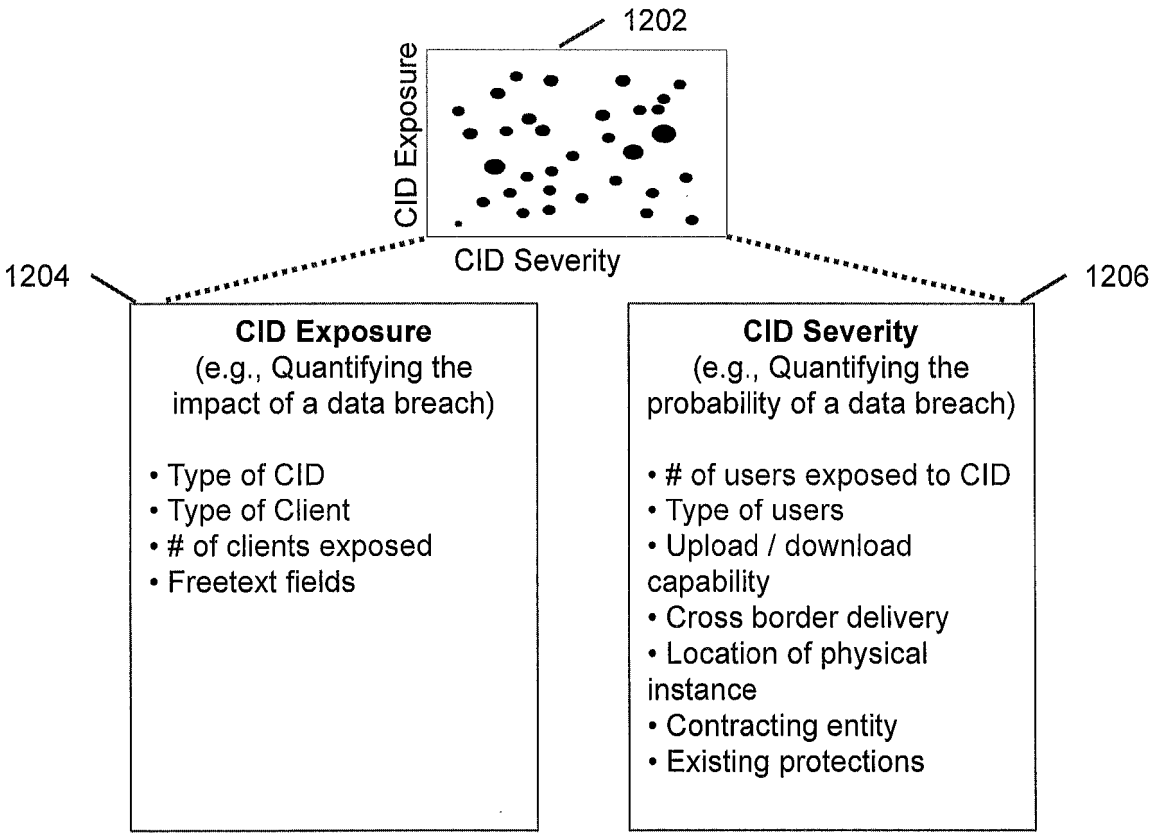

1100
Inventory Results
ID: AAXXXX
Questionnaire status
Affirmed
Compliance status
Compliant in Transformation
Interaction Processing Storage
Current State
G A G
Desired Target State
G G G
Final Target State
G G G
CTO Inputs
Blueprint Zone
Shared Services
Target State
G G G
Remediation Type
Eliminator
Severity
0.225
Exposure
0.107145
Quality
5
Standardised remediation measures
•Eliminate CID and non-sensitive client-references from Apps-context (e.g., storage, human interaction, Output, outbound, Apps2Apps communication, etc.)
•Ignore CID and non-sensitive client-references on inbound Apps2Apps communication (e.g., the sending Apps is responsible to clean up it's outbound Apps2Apps communication)
DA Comments
DA: Agreement with software component manager to implement transformational actions by X.X.2013.
Submitted by [xx]
Submitted on [xx]
Signed off by [xx]
Signed off on [xx]
Certified by [xx]
Certified on [xx]

FIG. 12


1202
CID Exposure
CID Severity
1204
1206
CID Exposure
(e.g., Quantifying the impact of a data breach)
• Type of CID
• Type of Client
• # of clients exposed
• Freetext fields
CID Severity
(e.g., Quantifying the probability of a data breach)
• # of users exposed to CID
• Type of users
• Upload / download capability
• Cross border delivery
• Location of physical instance
• Contracting entity
• Existing protections