SAFECOM
Alert SA Independent Review

1 December 2017

Commercial in confidence

Building a better working world

Introduction

This report has been prepared following significant issues experienced that impacted the Alert SA application (app). Following the Alert SA app issues, the Minister made a commitment to the public that an independent audit of the identified remediation activities would be undertaken. As a result, SAFECOM's CEO engaged EY to conduct the independent review.

This report evaluates the appropriateness and sufficiency of actions taken by SAFECOM and RIPE Intelligence, based on supplied documentation and interviews conducted, to logically mitigate against the causes reported. The purpose of this review is to independently determine whether the remediation works implemented by all relevant parties will logically mitigate against a reoccurrence of the causes reported and that SAFECOM's user acceptance testing (UAT) plan sufficiently tests the successful implementation of the remediation works.

Background

The Alert SA solution was developed from an existing solution by RIPE Intelligence for SAFECOM and can be accessed at no cost to users via mobile application or website. The purpose of the solution is to provide SA residents with up to date public information and warnings for all hazards. Users can opt in to receive notifications for areas of interest to them by creating 'watch zones'.

Executive summary

Incident
On Friday 27th October and Sunday 29th October, the Alert SA solution suffered a P1 incident due to unexpected increased server load caused by high frequency data received which also contained anomalies. The effects experienced by app users from this incident included delay and non-delivery of notifications and short periods of downtime.

Root Cause
Immediately following the incident, the root cause was identified as unexpected data from a BoM data feed. Through further investigation by RIPE Intelligence, the root cause was then identified as CFS Total Fire Ban/Fire Danger Rating (TFB/FDR) data feed content frequently and unexpectedly changing (every 60 seconds) and those changes being processed. The solution was programmed to check for a change in data from this particular feed every 60 seconds therefore it was expected that such a scenario was manageable regardless of whether it was uncharacteristic of this data feed. Therefore the root cause of this incident has been deemed to be a combination of the problematic data feed and shortcomings of the solution in its ability to sufficiently handle this frequency of data processing.

Remediation
A remediation plan focusing on prevention has been developed by SAFECOM and RIPE Intelligence and is currently being implemented. Remediation activities relating directly to mitigating re-occurrence of the root cause include:

- Increased data handling and management rules including processing frequency
- Develop a new custom CFS TFB/FDR data feed for Alert SA consumption
- Data custodians reminded of their obligation to their existing agreement not to modify data structures or variables without consultation
- Extensive user acceptance testing (UAT) of the remediated application
- Data feed monitoring of data consistency, reliability and adherence with the provided data dictionary (where available)

Conclusion
Based on the information provided when undertaking this review, the remediation works and subsequent testing conducted by SAFECOM and RIPE Intelligence appear to address the key issues identified through the root cause analysis.

A number of risks have been identified in relation to the remediation, testing and deployment of the updated Alert SA app that mean SAFECOM cannot with 100% certainty guarantee that issues similar to those previously experienced will not be reoccur, however these risks are no greater than a typical software upgrade of this nature and should not prohibit deployment provided the controls defined in this report are effectively implemented.

Risks

Multiple risks were identified in the process of composing this report which have the potential to impact performance of the Alert SA application post release of the new version of both the application itself and the data processing service. The key risks are outlined below and should be considered in reviewing this report and determining whether to deploy the new version of Alert SA.

Risk description	Consequence	Control	Responsible	Likelihood	Impact	Rating*
Unexpected issues arise in production where corresponding functionality/ performance was successfully tested in UAT. It is noted that despite significant testing coverage, unforeseen issues with deployment of new software versions can occur	Functionality and/or performance issues with Alert SA	• 100% of functionality is being tested in UAT. SAFECOM have engaged additional test resources to test Alert SA thoroughly • Roll back or fix issues in production based on severity • Extensively monitor in production post release	SAFECOM / RIPE	Rare	Major	
The UAT environment is indicative and comparable to production but not identical due to time and resource constraints	Test results will be indicative rather than 100% conclusive as to whether the remediation performed resolves the identified issues with Alert SA, therefore performance issues may still arise once deployed to production	• Restrict release of other upgrades to UAT during testing • UAT has been replicated as close to the production environment as possible • Load that will be applied to UAT is comparably higher than that which will be experienced in production based on the technical specifications of both environments	SAFECOM / RIPE	Unlikely	Major	
The remediation plan includes measures to limit the impact of erroneous external data feeds but does not include validation of all data feeds prior to consumption	Erroneous data feeds may still be processed that impact the functionality and/or performance of Alert SA	• Closely monitor data feeds and respond quickly where issues are noted (e.g. disabling notifications where required)	RIPE	Unlikely	Major	
Data custodians provide data feeds that are non-compliant with supplied data dictionary	Unexpected data causes functionality and performance issues with Alert SA	• Closely monitor data feeds • Disable notifications as required	RIPE	Unlikely	Major	
The root cause may have been misdiagnosed meaning the remediation plan and review has not addressed/ assessed the actual root cause	Functionality and performance issues with Alert SA	• RIPE Intelligence to monitor and report on Alert SA performance and delivery of expected functionality and respond quickly where issues are noted (e.g. disabling notifications where required) in line with SLA's	RIPE	Unlikely	Major	

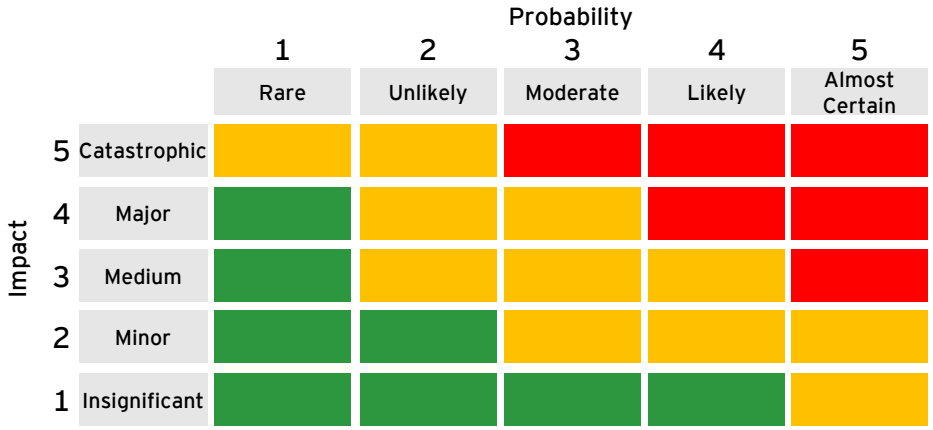
*** Refer to risk assessment framework overleaf**

Risks (cont.)

Risk description	Consequence	Control	Responsible	Likelihood	Impact	Rating*
Application functionality/performance negatively impacted by additional bug fixes being included in deployed software	Unforeseen issues arise in production that impact the functionality and/or performance of Alert SA	• Testing of the additional bug fixes and upgrades have been scheduled separate to the remediation fixes and have tested successfully • 100% of functionality is being tested in UAT. SAFECOM have engaged additional test resources to test Alert SA thoroughly • Roll back or fix issues in production based on severity • Extensively monitor in production post release	SAFECOM	Rare	Major	

* Refer to risk assessment framework below

Risk assessment framework



Risk evaluation scale & risk acceptance matrix summary

Impact * Probability	Risk Rating	Action	Adequacy of control
1 - 4	LOW	Monitor risk	Adequate controls required
5 - 14	MEDIUM	Management attention required	Clearly defined, strong controls required
15 - 25	HIGH	Urgent management attention required	Only acceptable with excellent controls in place

Interviews conducted

SAFECOM & EY

Friday 10th November 2017
Teleconference
1 hour 15 minutes
In attendance: Fiona Dunstan, Matthew Aitchison, Kendall Richardson, Michael Kinnane
Dialled in: Rahul Parkhe, Jenny Lewis

Tuesday 21st November 2017
Meeting
2 hours
In attendance: Matthew Aitchison, Michael Kinnane, Rahul Parkhe, Jenny Lewis

Thursday 23rd November 2017
Meeting
1 hour
In attendance: Malcolm Jackman, Fiona Dunstan, Matthew Aitchison, Kendall Richardson, Michael Kinnane, Jenny Lewis

Wednesday 15th November 2017
Meeting/Teleconference
30 minutes
Dialled in: Matthew Aitchison, Michael Kinnane, Rahul Parkhe, Jenny Lewis

Wednesday 22nd November 2017
Meeting
2 hours
In attendance: Fiona Dunstan, Matthew Aitchison, Kendall Richardson, Rahul Parkhe, Jenny Lewis

RIPE Intel & EY

Wednesday 15th November 2017
Teleconference
1 hour 15 minutes

Dialled in: Luke Corbett, Tarron Newman, Michael Kinnane, Rahul Parkhe, Jenny Lewis

Friday 17th November 2017
Meeting/Teleconference
2 hours 30 minutes
In attendance: Luke Corbett, Tarron Newman, Rahul Parkhe, Jenny Lewis
Dialled in: Michael Kinnane

Points of contact

SAFECOM

Malcolm Jackman
Chief Executive Officer
malcolm.jackman@sa.gov.au

Fiona Dunstan
CFS Manager of Information Operations
fiona.dunstan@sa.gov.au

Matthew Aitchison
Manager Public Information and Warnings
matthew.aitchison@sa.gov.au

Kendall Richardson
Principal Procurement Advisor
kendall.richardson2@sa.gov.au

RIPE Intelligence

Luke Corbett
Director
luke@ripeIntelligenceinfo

Tarron Newman
Director
tarron@ripeIntelligenceinfo

EY

Mark Stewart
Engagement Partner
mark.stewart@au.ey.com

Michael Kinnane
Engagement Director
michael.kinnane@au.ey.com

Rahul Parkhe
Manager
rahul.parkhe@au.ey.com

Jenny Lewis
Senior Consultant
jenny.lewis@au.ey.com

Documents provided

- AlertSA_Test Plan v1.2.pdf
- AlertSA_Network_Design_v3.0 (A428450).pdf
- NotificationDelay_NonDelivery_1.0.pdf
- OVERVIEW OF SERVICES_Alert SA.docx
- Alert-SA-website-app_Default-settings_Business-Rules-v3.6 (A656313).docx
- Test Cases_Alert SA_ACM.xlsx
- SLA with RIPE 1.0 (A471384)
- Alert SA Change Management Process.doc
- Alert SA Change Request Process_Internal (A491368).doc
- Updated UAT Schedule 15.11.17
- ASA_logic_v2.0.23.pdf
- WZCandidateTestScenarios.pdf
- 21b-1510637941.pdf
- 54c-1510624801.pdf
- cd2-1510637881.pdf
- server_record.pdf
- safecomalertSA_Runsheet_v1.1.mpp
- Various email correspondence
- NotificationDelay_NonDelivery_2.0.pdf
- AlertSA_monthly_report_201710.docx
- Fire Danger Rating XML Feed Data Dictionary v6.docx

Our understanding of the incident

Through review of supplied and requested documentation and interviews conducted, we have outlined our understanding of the incident and validated this with all involved parties. Recommendations throughout this report will be based on this understanding.

Impacts from the incident

The incident that occurred on two separate days, Friday 27th October and Sunday 29th October, impacted the Alert SA application end users in the following ways;

- Short periods of downtime
- Delayed notifications
- Non-delivery of notifications

The incident caused the following impacts to the Alert SA backend solution;

- Increased server load leading to server capacity increases
- Empty caching caused by the temporary gateway lock from the traffic overload on the single proxy

Following the incident, impacts continued to occur to the service including;

- No Country Fire Service (CFS) Total Fire Ban (TFB) / Fire Danger Rating (FDR) notifications are being sent to users
- All Bureau of Meteorology (BoM) warning notifications were meant to be blocked, however certain notifications continued to be sent

Root cause of the incident

Immediately following the incident, the root cause was identified as unexpected data from a BoM feed and corresponding remediation plans were focused on resolving this issue. Through further investigation, the root cause changed and was identified as CFS data feeds, from an isolated server, containing anomalies such as duplicated events with inconsistent conditions and out of the ordinary, frequent (every 60 seconds) new data feeds being received and processed. The solution was programmed to check for new data from this particular feed every 60 seconds therefore should have been able to handle a scenario in which the data was updated every 60 seconds regardless of whether it was not characteristic of this data feed. Therefore, the root cause of this incident can be deemed a combination of the problematic data feed and shortcomings of the solution.

The issue relating to the unexpected data from the BoM was degraded to a contributing factor of the incident but not deemed the root cause based on analysis conducted by RIPE Intelligence. Through investigation of the root cause of the incident, the following additional potentially contributing factors were also identified to be remedied:

- Inefficient/un-optimised queries and function processing
- Single proxy traffic route was not sufficient to handle peak traffic loads
- Limited documentation from data custodians such as data dictionaries with accompanying business rules and direction for use

Has adequate root cause analysis been done?

Observations

Our observations outlined below are based on information provided during interviews with key stakeholders and documentation provided by SAFECOM and RIPE Intelligence:

- The root cause was initially identified as unexpected data contained in the BoM data feed which was later retracted as the root cause and deemed a contributing factor for the incident, with the root cause being the problematic CFS data feed
- The root cause determination by RIPE Intelligence was conducted through monitoring the behaviour and restoration of the solution in response to disabling the problematic CFS data feed. Further detailed analysis of the problematic CFS data feed was also performed to identify the anomalies presented in the data set. RIPE Intelligence are confident that the root cause determination was the primary reason for the slowing of the system which caused the incident
- The problematic data feed historically changes up to a maximum of three times a day although the solution was programmed to check for a new feed for processing every 60 seconds. The reason for the 60 second processing frequency configuration was to minimise the delay between when the data changes at the source and when it is updated in the solution. Through this process, load is only caused to the system when there is a new feed to be processed. Considering the configuration of the system, there was an expectation that the system could handle new CFS TFB/FDR data feeds processed every 60 seconds without causing any impacts to the solution, however through the review process it has been determined this was not the case, nor was it contractually stipulated
- RIPE Intelligence have not explored whether the CFS data in question has been included in any other data feeds over the history of the solution due to limited time and resources
- SAFECOM have engaged a third party to ingest the problematic BoM data feed and a clean successful data feed from prior to the incident to determine whether this data was the root cause as per the initial determination

Assessment

- Considering the contributing factors and unknowns on the days of the incident the testing undertaken by the third party as to whether this data was in fact the root cause of the incident will provide an indicative result but will not be 100% conclusive
- A more definitive determination of the root cause could have been achieved through comparison of data sets from incident days to successful days, given more time and resources as remediation strategies were prioritised over root cause analysis
- If data ingestion intervals are set at 60 seconds, it is reasonable to expect the solution to handle the scenario where new data is imported every 60 seconds without causing any performance impacts
- Due to time and resource constraints, the scale of the parties involved and prioritisation given way to remediation and preventative measures, it is unrealistic to expect a more detailed and definitive root cause analysis to have been completed in this timeframe

Is the remediation plan to mitigate against further reoccurrence of this incident sufficient?

Observations

Our observations outlined below are based on information provided during interviews with key stakeholders and documentation provided by SAFECOM and RIPE Intelligence:

- Focus and pressure has been placed on development and deployment of the remediation plans within the set out timeframe
- The remediation plans by SAFECOM and RIPE Intelligence address strategies to mitigate against and solve the reported root cause and also address management of problematic data as best as possible
- The remediation plan from RIPE Intelligence has a strong focus on improvement of the contributing factors identified
- Further, undocumented remediation plan strategies by RIPE Intelligence relating directly to solving the root cause have been captured through interviews including;
    - Tighter safeguards around data acceptance including rejection of duplicated inconsistent events
    - CFS TFB FDR data feed import frequency increased to 30 minute intervals to address server load issues
- The remediation recommendations by RIPE Intelligence that have been actioned by SAFECOM include data governance strategies with data custodians such as refreshed and redistributed data change request process and requesting of data dictionaries with business rules and directions of use. These strategies are focused on preventing the reported root cause
- SAFECOM have identified a gap with transparency in and ability to monitor the solution and are considering engaging a third party monitoring service to improve their detection strategies
- Both SAFECOM and RIPE Intelligence were relying on each other to provide direction in relation to data handling however, at the time of the incident, no one party had taken responsibility of this area. Responsibility has now been assumed by SAFECOM
- The majority of the data presented in the solution is sourced from publicly available records. The remediation plan focuses on mitigation of the issues caused from the reported root cause and the successful import and display of this data. The data custodians are responsible for ensuring that the data provided accurately reflects the conditions reported and meet the agreed data standards

Assessment

- As the root cause is due to problematic data provided combined with shortcomings with the solutions ability to handle such data, it is possible that associated issues experienced from this root cause could re-occur if the CFS TFB FDR data feed is not adequately remediated or if it were to revert back to the problematic state. Efforts to remediate against this will not completely eliminate the risk of issues being experience with the CFS TFB FDR data feed but will reduce the impact to the solution in the event of reoccurrence
- The remediation plans proposed by SAFECOM and RIPE Intelligence will mitigate against reoccurrence of the reported root cause and are sufficient to best manage and limit the impact of associated issues if the reported root cause was to occur again

Is testing by RIPE Intelligence and SAFECOM adequate to deem remediation successful?

Observations

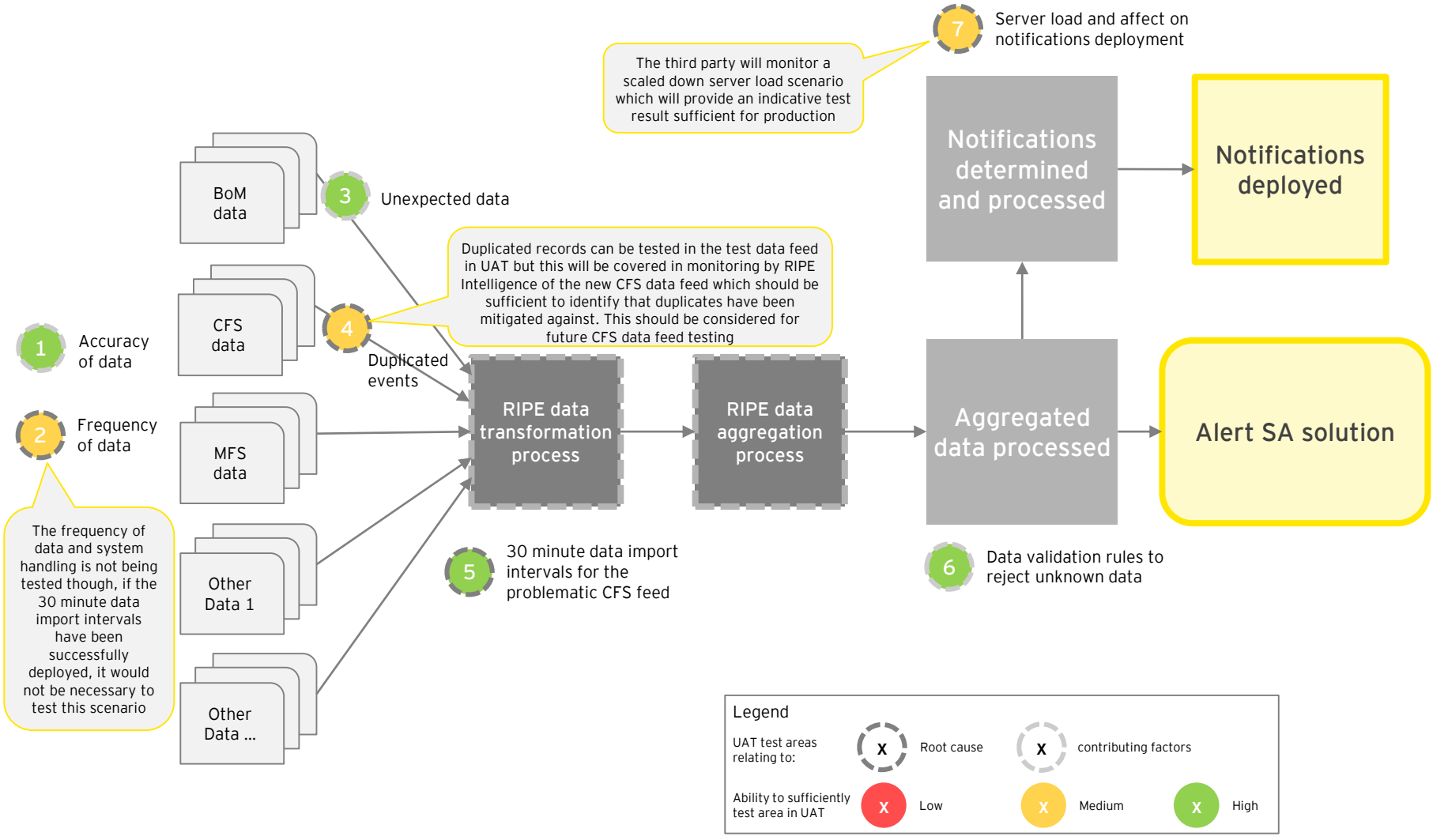
Our observations outlined below are based on information provided during interviews with key stakeholders and documentation provided by SAFECOM and RIPE Intelligence:

- Remediation testing by RIPE Intelligence was focused on testing the fixes against simulations of the root cause and monitoring the response and outcome of the solution to those fixes to determine whether testing was successful
- Remediation testing by RIPE Intelligence was deemed successful once RIPE Intelligence were convinced that the issue had been resolved through monitoring of the response of the solution to the fixes being tested
- Remediation testing by SAFECOM was focused around recreating multiple scenarios in the root cause environment (or as close to this as possible) including processing of successful and erroneous data feeds and monitoring the fixes against these scenarios
- Remediation testing by SAFECOM was deemed successful through assessment by SAFECOM of the UAT report with accompanying feedback from the engaged third party relating to the simulated BoM data scenarios. A SAFECOM scale for defect management was applied to determine whether the testing was successful
- SAFECOM invited RIPE Intelligence to monitor the results of UAT to support their testing strategy and provided them with the detailed test schedule
- Testing relating to the root cause of the incident was performed with other scheduled bug fixes and upgrades which were been consciously separated out in scheduling to ensure accuracy in test results
- The test environment was not an exact replication of the production environment as the number of servers were scaled down due to the intended usage of the environment and the cost implications therefore, it was unable to provide 100% assurance of performance and load testing results. However, proportionate performance load testing to the production environment was performed during UAT by the third party which provided indicative results as to the success of the UAT
- Regression testing of the full suite of functionality of the application was also performed

Assessment

- RIPE Intelligence's testing approach will adequately provide a conclusive result as to whether the fixes have remediated against the reported root cause.
- As the testing environment cannot be identically replicated, the testing can only be deemed successful against the environment tested and cannot be related back to the exact environment in which the incident occurred – the result obtained will provide an indicative result as to whether the testing was successful
- The testing environment is the best possible environment that can be achieved given the constraints on time and resources
- Further work into replicating the production environment in testing for future performance load related UAT should be explored to ensure more accurate results and outcomes
- No test results from RIPE Intelligence have been seen
- SAFECOM shared the UAT test results at completion of testing which showed no critical defects, therefore passing the SAFECOM quality management criteria for release to production

Our understanding of the data flow and processing and associated areas of UAT



Deployment assessment

Based on the information provided when undertaking this review, the remediation works and subsequent testing conducted by SAFECOM and RIPE Intelligence appear to address the key issues identified through the root cause analysis.

A number of risks have been identified in relation to the remediation, testing and deployment of the updated Alert SA app that mean SAFECOM cannot with 100% certainty guarantee that issues similar to those previously experienced will not be reoccur, however these risks are no greater than a typical software upgrade of this nature and should not prohibit deployment provided the controls defined in this report are effectively implemented.

Conclusion

Our conclusions outlined below are based on information provided during interviews with key stakeholders and documentation provided by SAFECOM and RIPE Intelligence:

- The reported root cause is outside of SAFECOM's control to directly remediate against as they, like RIPE Intelligence, do not have control over the data integrity from data custodians. Furthermore, SAFECOM do not have control over programming of the solution as this is under the control of RIPE Intelligence who are able to directly remediate against this element of the root cause
- Effort has been made to reduce known data anomalies from being imported prior to updating the associated data validation rules. RIPE Intelligence have directly addressed the inability to process the problematic feed in the nominated frequency by adjusting the frequency interval to an achievable level which will mitigate against reoccurrence of the reported root cause in the future. Additional strategies have been developed in the remediation plan focusing on limiting the impact to the service if this scenario were to reoccur
- Due to the CFS TFB FDR data being available for public use SAFECOM are not in a position to dictate to the CFS and data custodians of other publicly available data feeds how they should structure their data in order to suit the Alert SA solution. SAFECOM need to continue working closely with data custodians to maintain clear and regular lines of communication and to gather and maintain data dictionaries, business rules and accompanying instructions in relation to their respective data feeds
- It is SAFECOM's responsibility to provide RIPE Intelligence with any changes or updates to data feeds or structures, where SAFECOM have the responsibility with the data custodian, so RIPE Intelligence can proactively prepare and test for these changes instead of working in a reactive manner after the event
- It is important to note that 100% assurance cannot be provided as to whether the remediation plan will in fact prevent reoccurrence of the incident in question due to the unconfirmed determination of the root cause of this incident. The remediation plan by SAFECOM and RIPE Intelligence will reduce the impact experienced in the event that the reported root cause were to reoccur
- It is also important to note that the original remediation plan and associated test plans were developed when the known root cause was initially misdiagnosed as the BoM unexpected data. The remediation plans were updated to also mitigate against the data anomalies in the CFS feed and additional measures and strategies have been added to the original plan
- Given the short timeframe, prioritisation has given way to prevention strategies over a detailed root cause analysis. There is a risk that further issues not identified through the root cause analysis may exist however this risk is controlled to a degree by SAFECOM's extensive testing of the new version of the application
- The communication and escalation process between RIPE Intelligence and SAFECOM requires improvement to avoid future delays in notification of issues to SAFECOM