Operational Assessment of eir's Regulatory Governance Model

REDACTED FOR PUBLICATION

7 July 2017

Prepared for:

Commission for
Communications Regulation

Version History

Version	Date	Author	Changes	Distribution	Approval
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Confidentiality

This is a non-confidential version of the report. Redactions are marked in black.

Copyright

Contents

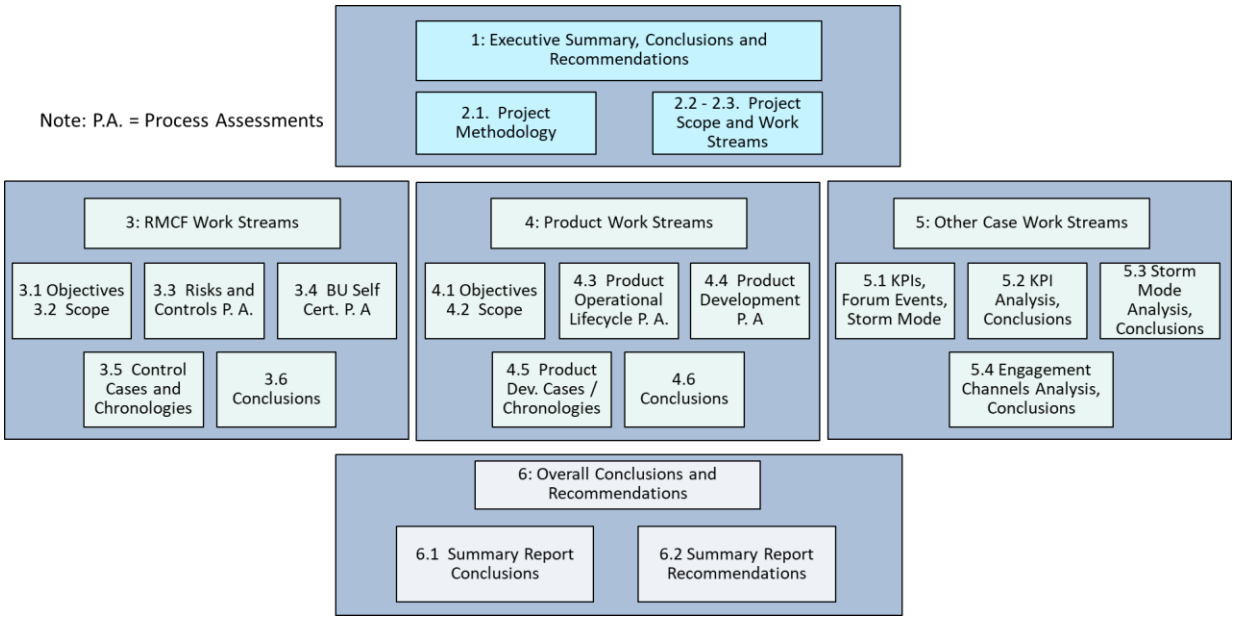
List of Figures

List of Tables

Document Framework Overview

This report is presented in the sections as shown in the figure below. The section numbers and headers are listed for each of the sections in this document.

Figure 1. Document Organisation



Section 1 provides an overview of the project, together with the summary conclusions and recommendations. These are supported by the Work Stream analyses documented in sections 3 – 5.

Section 2 covers the project methodology and scope, as well as the regulatory context of the project.

Section 3 focuses on processes, and the quality of the controls in the Risk Management and Control Framework (RMCF[1]).

Section 4 focuses on Product Processes, covering Product Development, and Product Lifecycle processes[2]. Both sections 2 and 3 follow a common document structure, beginning with objectives and scope sections, then sections documenting Cartesian's assessments, and lastly, the conclusions drawn from the assessment.

Section 5 covers three separate assessments, on Key Performance Indicators (KPI), Storm Mode operations, and operator and eir downstream account channel activities. Each of these process assessments follow the same organisation structure as used in the previous two sections.

Section 6 presents the overall conclusions by process area, and the overall recommendations.

[1] The Risk Management and Control Framework (RMCF) consists of the set of processes used to identify risks, and develop and operate controls. It includes the self-certification process, and its management and assurance.
[2] Product Lifecycle processes are defined to include: checks on customer information and product availability (pre-order), placing of orders (ordering), provisioning of orders, service and repair, and lastly, management of changes.

Section 7 (not shown in the figure above) contains reference materials that support the findings, or provide additional information and clarifications. A Lexicon of the terms used throughout the document is provided here. The observations that have been made throughout the assessments in sections 3 – 5 have been linked to the conclusions in each of the areas, then to the summary conclusions and finally, the recommendations. These links are documented in this section as well.

1. Executive Summary

Since October 2012, eir has, on a voluntary basis, been implementing a series of measures to provide assurance that regulated products are delivered in compliance with its regulatory obligations. Collectively, these measures are referred to as its Regulatory Governance Model (RGM).

The RGM contains three main strands, as follows[3]:

1. A Group Wide Code of Practice (CoP) dealing with eircom's Access and Non-Discrimination Obligations;
2. A Business Unit (BU) Process Compliance review programme to ensure the day-to-day processes are compliant with the CoP by implementing the necessary Regulatory Controls, the output of which are Statements of Compliance (SoCs);
3. Compliance reporting to the eir Board, ComReg and to the Industry.

To support the BU Process Compliance review, a Risk Management and Control Framework (RMCF) was implemented. This consisted of risk management and assurance processes supported by eir BUs, Internal Audit (IA) and Regulatory Compliance and Equivalence (C&E) functions, and utilising a Risk and Control Matrix (RACM). The purpose of the RMCF is to ensure that risks of eir not meeting its regulatory obligations are identified and controls that mitigate those risks are developed and effectively operated.

In December 2015, ComReg decided to conduct a review of the scope and quality of Eir's regulatory governance structures and the operation of the associated processes and procedures, including but not limited to eir's RGM. The review was tendered as two lots in March 2016.

In May 2016, Cartesian was appointed to perform the Operations Review and KPMG was appointed to perform the Governance Review. These lots, while distinct, were inter-related and Cartesian and KPMG worked closely throughout the review to manage any potential gaps or duplication in the reviews.

The Governance review comprised an assessment of the suitability for regulatory purposes of the macro structural, governance and control environment within which the operational risk and control framework operates. The review addressed such issues as eir's legal and management structure; the role of eir's main board and senior management; the independence and governance arrangements for its wholesale arm, open eir; the existence and quality of independent oversight; and the existence of suitable codes of conduct together with related HR matters such as training and disciplinary arrangements.

The Operations review comprised of an assessment of the adequacy of the control environment within eir as it applies to operational business processes, including product development. This included an assessment of the risk management and control environment throughout the eir organisation as it pertains to its regulatory obligations. It also assessed the completeness and quality of process documentation, the documentation and management of reports, information flows and sample transaction testing of the operation of controls, and the accuracy of source documentation.

The adequacy of the control environment as it applies to operational business processes is dependent on the reliability and repeatability of these processes. These include day-to-day business operational processes, processes for dealing with access requests from operators, processes for the management of

[3] Regulatory and Compliance Audit report, May 2015. The RACM emerged from the process compliance reviews and the SoC process to provide assurance to ComReg. The RMCF, including self-certification, was required to support the RGM BU compliance and reporting.

regulatory risk and independent assurance processes. For a process to be reliable and repeatable it should be clearly documented, have clear ownership and be supported by an adequately resourced and trained organization. In addition, there should be defined performance standards and tolerances.

Cartesian assessed these processes to determine their adequacy for identifying risks of non-compliance to regulatory obligations, and applying controls in a consistent manner. The assessment did not consider the efficiency or effectiveness of the processes in carrying out their functions. This assessment used the principles of ISO9001 for process quality, CMMI for process capability and maturity, and Sarbanes-Oxley for controls sustainability. These process attributes ensure that a process is reliable and repeatable.

Using these principles, Cartesian addressed four questions, in line with the scope of our engagement as outlined in the Invitation to Tender (ITT):

- Are the foundations of good process management, as it applied to the Risk Management and Control Framework, in place? (Process management)
- Are access requests from operators dealt with in a timely, transparent and non-discriminatory manner? (Product Development)
- Are regulatory risks identified, appropriate controls developed and effectively operated? (Operation of Controls)
- Is there effective oversight to ensure Risk and Control Management achieves its objectives. (Effective assurance)

In addressing these questions, Cartesian had intensive engagements with eir, and would like to thank the staff who attended interviews, dealt with information and follow up requests. We acknowledge that this posed a considerable burden on a number of people.

Cartesian's findings with respect to each of these questions are as follows;

1. Process Management

1. Product Lifecycle processes, consisting of Pre-Ordering / Ordering, Provisioning, Service Repair and Reporting, and Change Management, are reliable and stable.
2. Risk management processes, at the operational, management and assurance levels were not well-documented. Process owners were not clearly identified. There were no process standards, tolerances nor documented escalation processes.
3. There were no standards for risk identification and assessment in terms of probability, impact and timeframe. This meant that mitigation development could not be prioritised.

2. Product Development

4. The prioritisation process for RAP Development was opaque.
5. There was a lack of evidence of decision making by senior management for the cases Cartesian reviewed. This, and the opacity of the prioritization process, made it impossible to determine how key decisions were made. It was unclear the extent to which consideration was given to eir's regulatory obligations.
6. There were wide differences in the elapsed times of the product development cases examined by Cartesian, which were not explained by the complexity of the development work. There were no

controls on the timeliness of product development, even though there were timeliness obligations for a number of cases examined.

7. There was no formal process for dealing with operator requests and actions from the various forums. There were no project plans nor milestone management for tracking progress of requests.

8. The computer programs which were developed for the production of KPIs did not have specifications or test plans. They had not been independently assessed to verify that they performed as intended and generated results per the Decision requirements[4].

9. There was no proof that all records for the KPI metrics were included in the calculations.

3. Operation of controls

10. The Self-Certification process, which is a fundamental basis for the RMCF, was not reliable enough, nor consistently applied, to assure the successful operation of the Regulatory Governance model. The certification process had significant deficiencies and lacked effective assurance oversight.

11. Control defects existed in a high percentage of the controls reviewed over an extended period. There were sufficient cases where defects occurred over several quarters, either contiguously or continually, that it raised concerns about whether any tracking, escalation and corrective measures were enforced.

12. There were no company-wide standards to guide BUs in the operation of controls and the retention of evidence.

13. Aside from the initial development of a control, there were no processes for ensuring that the controls mitigated risks.

4. Assurance

14. Coordination between Compliance & Equivalence and IA was unclear with respect to operational tasks and accountability for regulatory assurance. This resulted in gaps and overlaps of assurance reviews.

15. The RGM Assurance reviews were carried out on a scheduled basis. However, there were overly long intervals between reviews.

16. Evidence of control operation and their outcomes was not consistently maintained. There were no central repository, standardised format nor standard access mechanisms for control evidence.

17. Several controls failed consistently from cycle to cycle; no process existed to identify consistently failing controls.

18. The tools that were used for managing risks and controls were limiting and cumbersome. Information necessary for the effective management of controls were missing.

Summary Conclusions

Cartesian reviewed the operational, risk management control and assurance processes to establish if they were sufficiently mature, robust and reliable to enable regulatory risks to be identified and controls

[4] Decision D05/11, Document 11/45, 'Response to Consultation and Decision on the Introduction of Key Performance Indicators for Regulated Markets', 29 June 2011.

to be applied and maintained in a consistent manner. Controls and the RMCF processes were examined to assess whether risk mitigation was effective. These processes are key elements in the overall Regulatory Governance Model, which eir uses as the basis for assuring compliance with their regulatory obligations. Past product development cases were examined to understand whether eir was at risk of not being in compliance with its Regulatory Obligations.

Our review findings highlighted significant deficiencies in the Risk Management and Control Framework. Examination of the RMCF supporting the operation, management and assurance of the RACM revealed significant flaws that call into question their overall effectiveness. The RMCF does not reliably mitigate risks, due to the inconsistent operation of controls. This is compounded by poor evidence maintenance, infrequent assurance, and a lack of trending and escalation mechanisms for dealing with defects in controls.

The product case analyses and product development chronology analyses have further highlighted process deficiencies and differences in elapsed time between products being developed for eir's downstream businesses and those of other operators.

The conclusions drawn from the assessment of how the KPIs were developed and operated raises concerns about the accuracy of the KPI reporting.

The responsibilities of C&E and IA were unclear regarding the ownership of operational tasks and accountabilities for regulatory governance assurance.

In the context of these findings, it is Cartesian's view that the Regulatory Governance Model is not sufficiently robust and reliable to enable regulatory risks to be assessed and controls to be applied in a reliable and consistent manner.

Key Recommendations

Process Improvement

1. Document business operational, product development and risk management processes and standardise risk management and control operations within BUs

Develop detailed documentation for each of the risk management processes identified, based on eir's regulatory obligations. Ensure well-defined criteria for evaluating and assigning risk impact, probability and risk exposure timing.

2. Develop process standards, escalation criteria, and exception tolerances

Create standards for critical processes, such as for defining exceptions[5] and escalations, and accepting new products for development. This will ensure that all groups carry out their tasks consistently, and that external stakeholders understand the criteria used for making decisions

3. Develop a transparent process for handling operator requests

[5] Exceptions are events in a process that are unexpected or abnormal. An exception can only be defined when tolerances for that process are first defined. An example of a tolerance setting would be the maximum time taken to complete the process under normal circumstances (e.g., all the process inputs are also defined, and they must fall within given ranges defined as 'Normal'). A request to complete this faster than the defined interval then becomes an exception. Such a request would require a re-prioritisation of process work and rescheduling. An implication of a capable process is that it is adequately staffed, or if automated, the system has sufficient capacity to handle the changes in process volume that could occur from day-to-day.

Create a transparent and fair process for managing Operator requests that will avoid protracted development delays, identified in several of the product cases reviewed. This process should be based on clear and objective standards, well-defined stakeholders and roles, milestone points and entry criteria. There should be strong independent oversight of the management of product development, which is required to ensure transparency and fairness to all operators, including eir. This should be supported by adequate evidence retention.

4. Increase visibility of the RAP prioritisation process

Implement a RAP prioritisation process that includes detailed documentation, clear assessment and decision criteria with decision milestones identified in the product development process.

5. Reduce dependency on forums to progress projects

Review the current industry engagement models to streamline the operation of various channels, including account management for industry and downstream eir. Introduce a project management discipline and standards on all industry participants.

Consider creating an independent operational role for establishing standards and the scope of topics across all channels. This scope should include all issues or enquiries raised by either other operators, or eir's downstream BUs. This role should ensure that a project-based approach is taken for all activities so that workloads, tasks, task ownership and deliverables can be independently planned and tracked till completion.

Risks and Controls

6. Design controls for simplified and comprehensive management

Design controls to simplify evaluations and improve assurance. Reporting of control operations and outputs should be standardised to simplify tracking of control operation, and assurance reviews.

7. Trend control results

Develop a process for trending of control evidence results to identify consistently failing controls. Implement escalation processes for failed controls, increase standardisation and oversight into BUs, and define roles of IA and C&E.

8. Maintain visibility of all KPI-reported transaction records

Maintain an audit trail for the processing of all the transaction records for KPI reporting, to ensure that all records are accounted for. This will ensure a clear understanding of which records were excluded from the calculations in the KPI reports, and the reasons for such exclusions.

Assurance

9. Implement independent oversight over critical processes and outputs

Because of the nature and extent of the deficiencies in the operational governance of Regulated Access Products (RAP) development and RMCF, Cartesian believes there should be robust, independent, competent oversight of these and the operation of all regulatory matters covered by this report. The provision of oversight will require operational support of an independent, adequately resourced, proactive regulatory assurance capability.

2. Scope and Context

2.1. Project Methodology

Cartesian organised the project into 15 work streams. These covered the following:

- business process assessments;
- analyses of past product development and other cases, and;
- assessment of controls and how they were operated and assured.

The business processes covered product development, product lifecycles and risk identification, assessment, and control lifecycles[6]. Cartesian examined these processes in terms of operations, management and assurance functions. These functional areas are described in Figure 2, below. Cartesian interviewed process owners and executors and reviewed supporting evidence provided by eir

Business processes were assessed to see if these were stable, repeatable and had reliable metrics such that regulatory risks could be identified and controls applied in a consistent manner. These are the attributes of high-quality, capable processes.

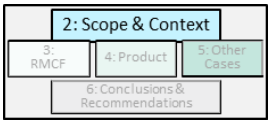
A high-quality[7] process will produce consistent outputs for a given set of inputs. The process should also be able to handle some pre-defined exceptions. Such processes are well-understood by staff who can then execute the process consistently. They are generally supported by detailed process documentation and proactive staff training.

A capable process starts with a well-defined and documented process, with clearly-defined exception conditions and how these exceptions are handled. Quantitative tolerances for the process must also be established, which then guarantee conformity in their handling[8]. Processes must be able to scale to handle the workloads up to a defined point, and are not dependent on specific individuals, but on teams. The skills to operate a process should not be dependent on specific individuals, but can be acquired through a standardised training regime.

Therefore, a high-quality, stable process has certain attributes; as listed:

- Standardised processes are formalised through documentation, and are therefore not subject to individual interpretation. The lack of such documentation indicates a lack of transparency and could result in discriminatory execution, since there is no standard to assess one execution of the process against another.
- Process owners who maintain process documentation and ensure the process is executed as it was documented is a requirement. Accessibility in a regulatory context cannot be reliably demonstrated without documentation, since it would be difficult to consistently communicate how a process is operated.

[6] Control lifecycle refers to the design of a control to mitigate a risk, to when it is retired because the risk has been permanently removed or mitigated sufficiently. A control may also be merged with another control,that control now being responsible for continued mitigation of the risk.
[7] 'High Quality' is narrowly defined to mean a stable, repeatable process that is well-documented, but does not necessarily imply that the process is efficient, or effectiveness in accomplishing its outputs. Section 7.2 describes the method.
[8] As an example, a process could be defined to complete within 2.5 to 3.5 business days 99% of the time, this being the process interval tolerance. Any order that is requested to complete faster than 2.5 days would require an exception process to handle it, e.g., *expedited process*. Similarly, if the process took longer than 3.5 days, it would go into an *escalation process* that would try to complete the process as quickly as possible. Without tolerance definitions, it would not be clear when orders were to follow an expedited process path, nor which orders needed escalation.



- Quantitative standards and tolerances must be established to ensure that exception conditions are well-understood and handled in a consistent manner, leading to non-discriminatory outcomes.
- Process capability ensures that even when work volumes change from day-to-day, similar inputs generate similar outputs in a predictable timeframe. Exceptions will also be handled consistently, thus assuring non-discrimination.

In summary, high-quality, capable processes enable different users to have equivalent outcomes (same inputs generate the same outputs). Since this also means that processes are well-documented, it increases transparency and accessibility to the processes.

Cartesian reviewed the quality and capability of processes and assessed them in the context of regulatory risks and their controls. The risks and associated controls examined were those identified in the following groups (overlaps exist between these groups);

- eir's Risks and Controls Assessment completed in June 2014,
- risks and controls owned by three BUs (BU)[9], and
- some others discussed in the May 2015 Regulatory Compliance and Audit Report[10].

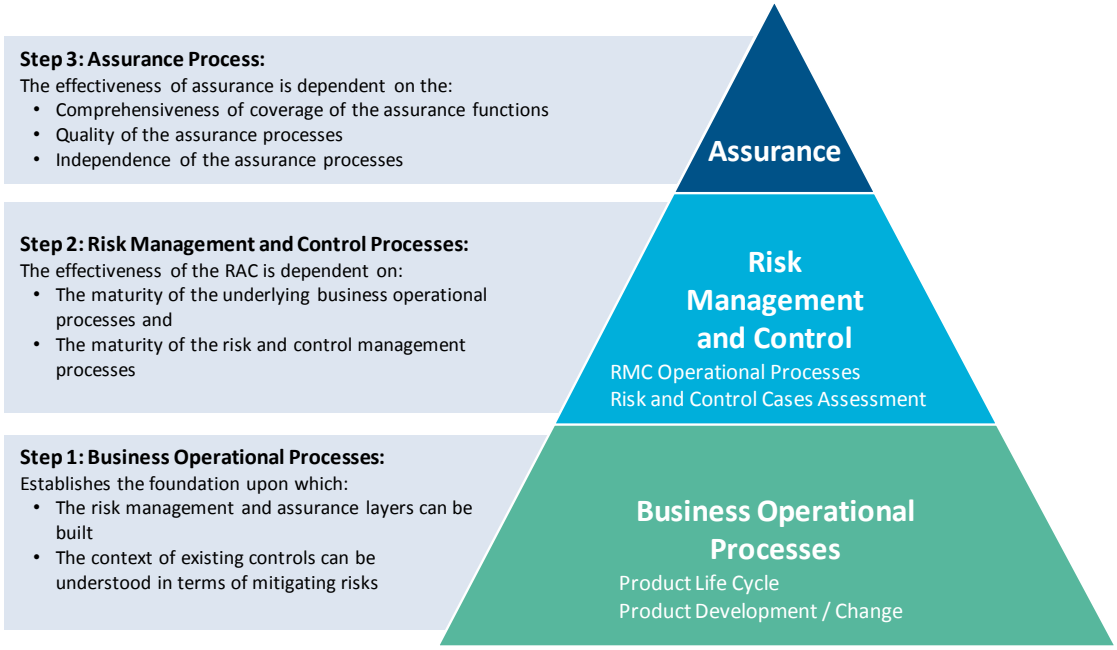
Specific examinations were made on historical product development cases, and the operational lifecycle for some of the controls. These included the processes associated with the Business Process Reviews and Self-Certification, and publishing of findings in the redacted Regulatory Compliance and Audit Reports issued twice-yearly.

Cartesian also examined the chronologies involved in product development work carried out by eir, and the lifecycles of all the controls, to provide further support for its findings. Figure 2 illustrates the relationship between business operational processes, product development processes, risk management and risk and control assurance processes.

The figure below also shows the order in which the analyses were done. The business operational processes[11] were examined first to establish whether they were stable, capable, repeatable and had reliable metrics such that regulatory risks could be identified and controls applied in a consistent manner and mitigated the risks. Once that was established, management and assurance processes were examined, as well as the risks and controls.

[9] eir Wholesale RAP Markets, eir Enterprise and Government Markets, eir Fixed Access Operations
[10] A redacted version of the May 2015 'Regulatory Compliance and Audit Report' was published as the Aug 2015 'Industry update on Eircom's Regulatory Governance Model'
[11] Section 7.4, definitions of Business Operational, Management and Assurance processes

Figure 2. Process Hierarchy



2.2. Project Scope and Work Streams

Cartesian organised activities into 15 work streams under three broad headings: (a) Risks and Controls, (b) Product Development and Product Lifecycles and (c) other work-streams. The processes and cases examined under each of these headings covered processes involved in all layers in the Process Hierarchy – operational, management and assurance. These were examined to identify and understand any issues with these processes that could affect eir's ability to meet their regulatory obligations and also test the robustness of the Regulatory Governance Model.

a. Risks and Controls

Cartesian examined risks and controls covering a period from Q2 2013[12] to Q3/2016. The RMCF processes were examined by Cartesian in the H2 2016, based on interviews with key participants, and documentation of the risks and controls.

All the assessments were appraised in terms of eir's ability to meet their regulatory obligations, and how risks of non-compliance were mitigated.

The RMCF assessments looked at the Operational, Management and Assurance Processes[13] used to manage the Risks and Control lifecycle. The lifecycle consists of the following process areas;

- identification of risks and design of controls
- Control merges and retirement

[12] Quarter dates refer to calendar quarters, rather than eir's fiscal reporting quarters.
[13] **Error! Reference source not found.** provides a description

- BU Self-Certification processes
- eir's assurance and reporting processes.

Past instances of self-certification, risk and controls management and assurance were also examined.

The effectiveness of selected controls was examined, as was the means used for handling any exceptions that were identified.

There were three work streams within Risks and Controls.

- Work Stream 1 and 2: Risk and Controls Lifecycle processes covered the following areas;
  - Initial risk identification and assessment, design and development of controls and risk closure and control retirement and the publication of the Statement of Compliance.
  - Self-certification in BUs. Cartesian reviewed Control execution and Self-Certification sign-off in 3 BUs.
  - IA and C&E processes used in the assessment of BUs' controls includes the processes and tools used to manage and assure the Self-Certifications
  - BU processes used to manage exceptions, either in the operation of the control, or when exceptions were encountered in the results produced by the controls.
  - Examination of specific controls (including those identified as Gaps and Equivalence issues in the Regulatory Governance Reports[14]), to understand their effectiveness in mitigating risks of non-compliance, and the quality of their operation, management and assurance, over the control's lifecycle.
- Work Stream 3: This covered the chronological analysis of all controls, utilising logs that eir has used to track risks and controls through successive review cycles. This analysis was used to understand trends in the quality of the controls, the quality of the assurance process itself, and any patterns in the operation and type of controls.

The assessments carried out in this section overlapped with the product lifecycle examinations, as new product developments require the identification of risks, and the implementation of appropriate controls. These are described and assessed in item b, Product Development and Product Lifecycle, below.

b. Product Development and Product Lifecycle

Cartesian examined new product development and change management processes for RAP and product Lifecycle processes, covering pre-ordering / ordering, provisioning, service assurance and change management. These processes provide the foundations that enable risks to be reliably identified and reliable controls to be consistently applied.

Six historical development cases were also included in the scope of analysis to understand h they were handled in the context of the RGM.

[14] These are the 6-monthly reports issued by C&E. The report names have changed over time, with earlier reports called Regulatory Governance Reports, later changing to Regulatory Compliance and Audit Reports. Some name changes may be due to different version of the same report, with different distributions and levels of redaction.

The six cases examined covered a period ranging from 2010 to June 2016[15].

- Work Stream 4: Processes used for receiving requests for products or changes to products, from the current in-situ 'informal' request, through the various stages including eir internal processes, leading to the release of a RAP. Process steps used to identify risk have been included in this section, although the steps used for designing, implementing and operating the controls for these risks are covered in the previous section (a) above.
- Work Stream 5: Processes used in the customer-product lifecycle, including pre-order / order, provisioning, service assurance and change management were reviewed. The operational processes were evaluated primarily to understand their capability for risk identification and mitigation through controls.
- Work Streams 6 - 11: Six specific product development cases were examined from a historical perspective. This was to understand the sequence of milestones, elapsed times and decisions made, that resulted in the commercial deployment of the products.
- Work Stream 12: A chronological analysis of development projects was undertaken to understand the major process steps and decision points (project stages or gates) associated with these product developments. This analysis was designed to also allow an assessment of trends and patterns in development times and the nature of the projects.

c. Other Work Streams

Three additional detailed assessments were made into Key Performance Indicators, Storm Mode, and open eir's handling of actions arising out of forum and account management channels.

- Work Stream 13: The processes used for designing, developing, operating and reporting of KPIs were examined. Cartesian examined what measures were taken to minimise risks to compliance with eir's regulatory obligations, which were mandated through Decision D05/11[16]. The KPIs covered were (i) service fulfilment intervals, (ii) fulfilment quality, (iii) fault repair intervals and (iv) fault repair quality. The examinations covered the processes in operation in Q4 2016, and included a review of all available documentation.
- Work Stream 14: Cartesian examined the entry conditions, operations under Storm Mode, and the exit conditions. The assessment covered the processes in operation in Q4 2016, and included a review of all available documentation. The declaration of Storm Mode requires one condition to be fulfilled, namely an abnormal increase in the level of faults, such as triggered by unseasonably bad weather.
- An abnormal increase in faults is defined as when carry-over faults for a day are twice the normal level for that time of year and where normality cannot be restored within one week. Once Storm Mode is declared, a Storm Response Plan is activated.
- Work Stream 15: Cartesian examined open eir's management of actions arising out of forum and account management channels, to understand what operational, management and assurance processes were used, their degree of formality and their effectiveness in ensuring that eir's obligations were discharged.

[15] The elapsed time for two of the cases (Duct Access and SLA development) commenced before the establishment of the RGM. The development time for all cases continued after the establishment of the RGM in 2012.
[16] ComReg Document number 11/45, Response to Consultation and Decision on the Introduction of Key Performance Indicators for Regulated Markets, 29/6/2011. This document described the markets that required key performance indicators, and the type of metrics required.

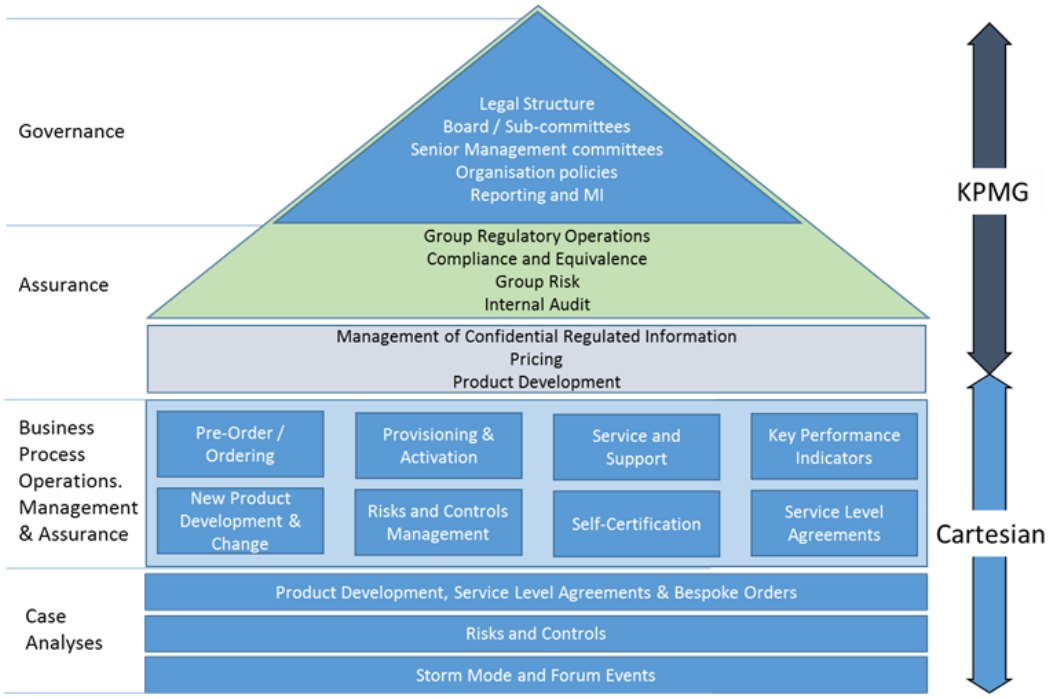
2.3. Scope in conjunction with KPMG

Since October 2012, eir has been implementing a series of measures to provide assurance that regulated products are delivered in compliance with regulatory obligations. Collectively, these measures are referred to as its RGM.

In December 2015, ComReg decided to conduct a review of the scope and quality of Eir's regulatory governance structures and the operation of the associated processes and procedures, including but not limited to eir's RGM. The review was tendered as two lots in March 2016.

In May 2016, KPMG was appointed to perform the Governance Review and Cartesian was appointed to perform the Operations Review. These lots, while distinct, were inter-related and KPMG and Cartesian worked closely throughout the review to manage any potential gaps or duplication in the reviews. The high-level scope of the two reviews delivered by KPMG and Cartesian is illustrated in the diagram below.

Figure 3. Assessment Scope Coverage



The Governance Review performed by KPMG comprised:

- An assessment of the scope and quality of eir's regulatory governance structures and the operation of the associated processes and procedures, including but not limited to eir's RGM;
- Consideration of eir's structure and organisation in the context of their potential impact on the effectiveness of eir's governance arrangements and therefore eir's ongoing compliance with its regulatory obligations; and,
- The implications of the issues raised in the August 2015 report and the information provided in this and other internal eir reports.

2.4. Regulatory Context

The purpose of this section is to provide an overview of the linkages between Cartesian's assessment methodology and eir's regulatory obligations.

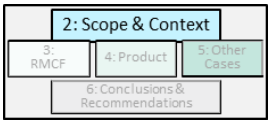
The effectiveness of the RGM is dependent on the quality and reliability of its supporting processes. Cartesian has assessed these processes to determine if they were robust, stable, and capable, and had reliable metrics such that risks of non-compliance to regulatory obligations could be identified and controls applied in a consistent manner.

Cartesian assessed each process against a number of process attributes which are listed in the table, below. Each of these process attributes were comprised of several elements (also listed below) and considered in the context of eir's Regulatory Governance Model.

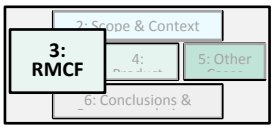
Table 1 below summarises various process attributes and their potential effect on eir's obligations to Non-Discrimination, Access and Transparency. This is a guide to understanding the importance, from a regulatory perspective, of having each of the process elements in place. For instance, having a defined process that is well documented with clear ownership and under change control, provides a stable and visible reference that enables risks to regulatory obligations to be identified and controls applied and maintained consistently. Conversely, the lack of a defined process means that regulatory risks may be unstable and controls cannot be consistently applied.

Table 1. Process Implications of Regulatory Obligations

Process Quality and Implications for Regulatory Obligations				
Processes should be robust, stable, capable, repeatable, and have reliable metrics such that risks of non-compliance to regulatory obligations can be identified and controls applied in a consistent manner.				
Attributes	**Elements**	**Elements substantially in existence with evidence**	**Elements substantially or partially not in existence**	**Obligations potentially impacted**
• Elapsed time for development (Product Cases only)	• Reasonable elapsed time from change request from operator to delivery of solution	• Demonstrate that product developments have been done in a timely manner.	• Main indicator that product development timeliness obligation has not been adhered to.	• Access • Non-Discrimination • Timeliness
• Process Quality - Formal Process	• Defined process • Clear Ownership • Formal documentation • Change control & current • Process adhered to	• Predictable process outcomes • Provides a stable and visible reference that enables risks to regulatory obligations to be identified and controls applied and maintained consistently. • Visibility to the process	• Lack of Transparency • Risk of unstable process leading to: • Unstable risks • Unreliable controls	• Access • Non-Discrimination • Transparency • Timeliness



Process Quality and Implications for Regulatory Obligations				
Processes should be robust, stable, capable, repeatable, and have reliable metrics such that risks of non-compliance to regulatory obligations can be identified and controls applied in a consistent manner.				
Attributes	**Elements**	**Elements substantially in existence with evidence**	**Elements substantially or partially not in existence**	**Obligations potentially impacted**
• Process Capability (Formal Process a prerequisite)	• Repeatable process • Adequate staff • Standards and tolerances • Escalation paths • Process metrics • Formal training • Single Process Path	• Enables predictable outputs for the same inputs • Risks remain the same over time • Enables effective controls to be implemented • Ability to handle exceptions consistently	• Variable risks and ineffective or unreliable controls • Inconsistent outputs for the same inputs • Loss of transparency	• Access • Non-Discrimination • Transparency
• Transparency of decisions and decision makers	• Defined decision making process • Clear rules on decision making • Clear criteria for decision making • Defined decision makers	• Enables demonstration of equivalence • Visibility to the operation of controls and their outcomes	• Inability to demonstrate equivalence • Limited visibility to control operation and outcomes	• Access • Non-Discrimination • Transparency
• Supporting Documentation (Pre-requisite – Transparency)	• Documentation available for inspection • Documentation of key decisions and how / who made them	• Maintain evidence of the rationale for decisions made and stakeholders	• Loss of transparency • Inability to prove equivalence • Cannot prove control operation or remediation	• Access • Non-Discrimination • Transparency
• Independent Assurance of processes	• Organisational independence • Effectiveness of controls to mitigate the identified risk	• Provides an independent assessment that regulatory risks are identified and controls are operating as designed and that they mitigate the risks	• Lack of confidence in results of the effectiveness of controls and mitigation	• Access • Non-Discrimination • Transparency



3. RMCF Assessment

3.1. Objectives

eir is required to ensure that its RAP development and lifecycle processes are compliant with Regulatory Obligations. eir's means of ensuring and demonstrating this compliance is through a framework which eir refers to as the RMCF.

Cartesian reviewed eir's RMCF as it applied to business operational processes. The primary purpose of the review was to ensure that the RMCF was effective in identifying regulatory risks and, through controls, mitigated them consistently.

3.2. Scope

The review examined the scope and design of the RMCF, its implementation, and how it was operated and managed. eir's industry updates on the implementation of its Regulatory Governance Management (RGM) framework were also within the scope of the review[17].

Our overall approach involved examining how compliance risks, including gaps and difference issues[18] were identified, and whether the controls satisfactorily mitigated these risks. The importance of this assessment is underlined by the fact that two of the RGM's three strands are based on reviewing and reporting on its compliance[19]. These two strands in turn utilise the set of controls tracked in the RACM, and the processes examined below, to manage risks to its regulatory obligations.

Cartesian assessed:

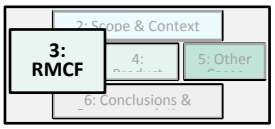
- the adequacy of eir's control environment as it applies to operational business processes;
- the reliability of the risk assessment process, and processes used for implementing, operating and reporting on the controls and;
- the processes used for handling issues discovered in the execution of the processes, and the assurance over all of these processes.

The assessments were carried out through three work streams, each of which covered different aspects of the RMCF.

The first work stream, detailed in section 3.3, examined the following processes:

1. Risk Assessment
2. Control Design
3. Risk Closure & Control Retirement
4. RACM Control Execution
5. RACM Assurance Process

[17] Cartesian has carried out its assessments in view of the obligations that include Access, Non-Discrimination, and Transparency, as described in the relevant ComReg Decisions.
[18] Regulatory Compliance and Audit Report, May 2015, page 29. We have used the term 'non-equivalence' as well as difference
[19] Regulatory Compliance and Audit Report, May 2015, page 7, details the three strands of the RGM.



6. Statement of Compliance (SoC) Publication

The processes were examined in terms of the work carried out by C&E, IA and open eir functions. Cartesian carried out interviews and examined documentation, to assess the quality and capability of these processes.

The second work stream is detailed in section 3.4. This examined the Self-Certification processes owned by, and executed by the BUs. Similar to section 3.3, Cartesian carried out interviews and examined documentation, to assess the quality and capability of these processes. As part of the assessment, Cartesian examined the controls that were owned by the BUs, to assess the effectiveness of these controls in mitigating the risks, over their lifetimes. This entailed examining the history of each control, from the point where the risk was identified, through the end of the Cartesian evaluation period (end Q2 2016), or to when the control was retired. This utilised data from the Self-Certifications, IA and C&E reviews, and from the 'snapshot' records described in the next work stream below.

The third work stream utilised the 'snapshot' records that formed the database on which the RMCF was based. IA maintain a set of Excel spreadsheets, which record the status of the complete set of controls at specific points in time[20]. Cartesian assembled these snapshots into a database which allowed an analysis of the history of the complete set of controls, and trending of the status of the controls. From this, we could evaluate statistical trends and overall quality of the control effectiveness, and the extensiveness and quality of the record-keeping of the control information. For example, it was possible to understand systematic trends in the types of issues, and their durations, across the entire body of controls. This study was essential in understanding the overall effectiveness of the controls and their tracking and management.

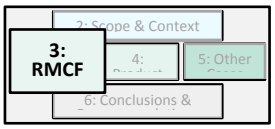
To understand the effectiveness of the controls in mitigating risks, it was important to understand the primary attributes of risks. These include:

1. The probability of a risk occurring, and becoming an issue;
2. Whether the severity of the impact is quantifiable;
3. The imminence of a risk so as to enable prioritisation of the development of mitigation;
4. The risk exposure duration. This period starts when a risk or issue is identified and assessed, and ends when mitigation is implemented;
5. Whether the occurrence of a risk can be detected with a known degree of reliability;
6. Whether a plan for dealing with issues exists;
7. Whether assurance processes have been developed to ensure that the risk identifications can be done consistently.

Controls have several attributes that are vital in ensuring their effectiveness, including:

8. Whether assurance is in place to ensure that controls are operated effectively, and the requisite reporting is accurate and timely;

[20] Cartesian has referred to these as 'snapshots'. The first of such snapshots examined was recorded as of 25/9/2014, and the last file as of 16/06/2016. There were 14 such files, recorded at unequal intervals. The snapshots are managed by IA, and are recorded in Excel files named generically as 'MOA vx.x.xlsx', where x.x is the file version number. The first version examined by Cartesian was 0.2, and the last by Cartesian was version 2.9.



9. The effectiveness of mitigation in terms of its ability to decrease the likelihood of a risk, and / or decrease the severity should it occur.

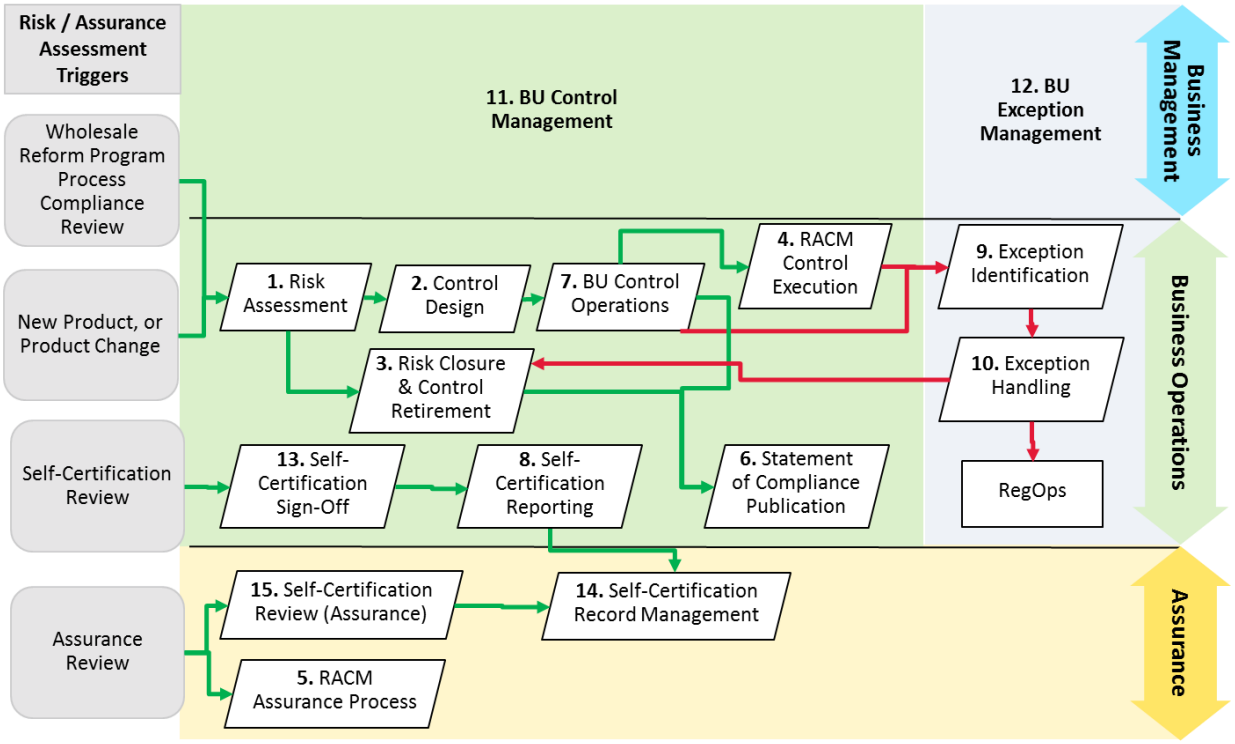
Because eir operates in a regulated framework, the factors above must be demonstrable, through transparency of the processes, the documentation kept, and the traceability of the processes leading to the documented results.

3.3. Operational, Management and Assurance Processes for Risks and Controls Processes

The figure below shows the relationship of the processes that support the RMCF. The numbering of the process boxes and areas correspond to the numbering of the process areas described in sections 3.3 and 3.4.

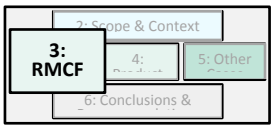
The assessment covered the three process layers, as described in Figure 2 Process Hierarchy, namely, Business Operations, Risk Management and Assurance processes.

Figure 4. Risks and Controls Processes and Triggers



Notes: Green arrows denote normal work-flows, and Red arrows denote exception work-flows[21]. Each process box contains the section and name of the process that has been reviewed below. BU Control Management (11) and BU Exception Management (12) are the management processes overseeing these operational processes.

[21] An exception event is where an unexpected event has occurred.



Process Quality and Capability Scoring [22]

The scoring methodology outlined here was used for each of the processes assessed in this section, and in section 4. Cartesian assessed each process from the perspectives of quality and capability, the elements of which are outlined in the Table 1.

For example, process quality comprises five elements: (1) documented process, (2) with clear ownership, (3) under change control, (4) that is current and up to date and (5) operated as documented. Each element could score 100%, 50% or 0%, depending on the extent to which the element met the criterion. The process score is made up of the average of the scores for the five elements.

If an element fully met the criteria, then the process would score 100%. If the element partially met the criteria, then the process would score 50%. If the element did not meet any the criteria, then it would score 0%. The same scoring methodology applied for Process Capability, which had eight elements.

Risks and Controls Processes

This is an assessment of the processes associated with Risks and Controls Management. These are considered separately from the Self-Certification processes, which are addressed in the following section.

The RACM include the following processes:

1. Risk Assessment

This process ensures that product requests are checked to see if they are RAP. If so, then checks are made for compliance risks, so that mitigations can be developed. The risk assessment process is completed when the risk has been documented.

When the Wholesale Reform Programme was implemented, reviews were conducted of the business processes supporting eir Wholesale Regulated Access Products, and the downstream BU processes used to offer RAP-based products. The risks identified through these reviews, and the associated controls, formed the initial base of the Risks and Controls documented in the RACM.

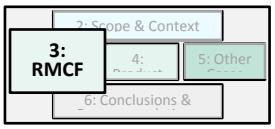
Subsequent to the reform programme, new RAP, and changes to existing RAPs, require an initial risk assessment to identify risks to compliance with eir's regulatory obligations pertaining to RAP.

Observations

O 1: The initial Wholesale Reform Programme Business Process Reviews of risk identification were well-documented. Following those reviews, evidence was not well-maintained to show the subsequent review processes, and standards used for formal investigations.

O 2: Decisions with respect to a risk are made by a team (C&E, Regulatory Operations, Solution Architects and Product Management) based on expert product and regulatory knowledge.

[22] The methodology is fully documented in the presentation, Eir Process Walkthrough v2.pptx



However, decisions are made without documented decision criteria and therefore there is a low level of process reliability.

O 3: The C&E function participates in the risk identification process. C&E also subsequently checks the operation of the process. Therefore, there is no formal independent assurance process[23].

O 4: No quantitative criteria exist for the evaluation of risk likelihood and severity were it to occur, nor of the potential impact timeframe.

O 5: Qualitative criteria for risk likelihood and severity are used, however not all risks are assessed and there is a risk of inconsistent treatment. Only 45% of risks had a qualitative Risk Impact and Risk probability value assigned in the last RACM examined (June 2016). These values used were 'H', 'M', and 'L', but there are no definitions for what these values meant or how they are to be assessed.

Cartesian Process Quality Score: 30% Cartesian Process Capability Score: 31%

2. Control Design

This process step follows from the Initial Risk Assessment, and covers the design of controls to mitigate the risk to an acceptable level, through to its implementation by a BU. The controls may be temporary or permanent, generally involving manual processes or reports, or a longer-term remediation, such as changes to a computer system. In some cases, both a temporary solution was designed to mitigate the risk quickly, while awaiting a longer term permanent remediation. Each BU is accountable for the design of a control, with support as needed /requested from C&E and / or Wholesale RAP.

Observations

O 6: The design of some controls did not result in the mitigation of the risk. For example, some controls required the generation of reports that did not provide information needed to determine whether the risk had occurred[24].

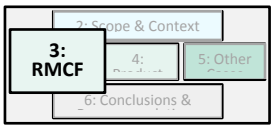
O 7: Inadequate documentation and a lack of independent assurance are also issues for the design of mitigation processes. No standards exist for assessing the acceptable degree of risk mitigation, exacerbated by the fact that there are no standards for assessing risk likelihood and severity.

O 8: Control design decisions are made by a team (RAP, C&E, and Product Management) based on expert knowledge, but without documented decision criteria. Therefore, there is a low level of process reliability and repeatability.

O 9: C&E participate in the design decision-making. They are also responsible for checking the operation of the process to ensure that the design meets the control requirements. This may lead to a conflict of interest.

Cartesian Process Quality Score: 30% Cartesian Process Capability Score: 44%

[23] Since 2016 C&E are no longer involved in business as usual process for identifying risks and controls.
[24] NGAWBA_CRM_031, WRP_CRM_063



3. Risk Closure & Control Retirement

These processes are initiated primarily by the BUs. Occasionally, C&E or IA may recommend the merging of a control with another similar control, as part of their reviews. A control may be retired for two reasons:

- The risk has been mitigated satisfactorily through a remediation (generally through a change to OSS[25] / BSS platforms), and / or
- The control has been merged with an equivalent control.

C&E and Wholesale RAP review the requests and must sign off the request before the retirement can proceed. The transaction is then recorded by IA[26].

Observations

O 10: While the process for Risk Closure and Control retirement is documented, there is no means to ensure that it is followed consistently by the BUs. The assessment of the mitigation by C&E is informal, and no standards exist for carrying out the assessment consistently.

O 11: The process works well from an operational perspective. Controls have been merged and retired, with C&E reviews carried out to validate these merges and retirements. C&E utilise a documented procedure for carrying out reviews of the RACM. However, there are no standards or evaluation criteria to assure that controls are retired or merged in a consistent manner, especially by different BUs, nor is there evidence of the assurance steps taken during the progress of the requests through to the conclusion.

O 12: The overall risk posed by retirement and merging of controls is low. Controls reviewed by Cartesian that had been merged or retired were appropriate, even though the review process was informal.

Process Quality Score: 20% Cartesian Process Capability Score: 50%

4. RACM Control Execution

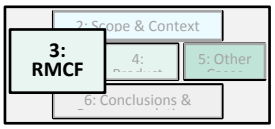
This process is initiated through the Self-Certification notification by IA. The BUs execute the controls according to the control procedure (see section 3.4 item 7 below) listed in the RACM, and report the self-certification back to IA using the process listed in section 3.4 item 8 below. The scope of this process review covers the work done by IA as the trigger and receiver of the Self-Certification.

Observations

O 13: Each control is operated and managed by the BU owner. There are no common process guidelines, no established standards for escalations, nor non-compliance consequences with procedures. There are no audit trails within the BU Self-Certification mechanism that BUs are required to follow. The only requirements are that:

- the BU owner must certify that the control executed satisfactorily. If the control did not operate per the procedure, the BU owner will note this in the certification.

[25] OSS – Operational Support System, BSS – Business Support System
[26] The process is documented in 'Operation of the RACMs and Controls within eircom', Version 1, dated 26/11/2014.



- evidence is placed in the location specified in the Control Evidence field of the RACM. The BU owner must note any discrepancies during the Self-Certification process.

O 14: High defect rates in the execution of controls were identified through Self-Certification, and by eir's internal reviews. These were documented in eir's Regulatory Compliance and Audit Reports, and associated IA HIA Summary Reports[27].

Cartesian Process Quality Score: 40% Cartesian Process Capability Score: 38%

5. RACM Assurance Process

Both the IA and C&E teams carry out periodic reviews of the controls independently. They use different criteria for selecting controls for review, and utilise different assessment criteria, as described below.

Internal Audit Review Criteria and Scope

IA carry out a 'Desktop Walk-Through' of controls on a Business Area basis. IA have defined 7 business areas. The reviews are carried out one at a time, on a 6-monthly schedule done on a best-efforts basis. This means that, at best, the same BU controls will only be reviewed once every 4 years.

IA noted control exceptions if; (a) the control had not been implemented, it was termed 'aspirational', (b) the control procedure was incomplete or unclear and (c) the control evidence storage location was not clearly documented.

IA do not assess the severity of the issues, nor do they make any recommendations for next actions in the Wholesale Reforms Committee HIA Summary report.

Compliance and Equivalence Review Criteria and Scope

Each C&E control review cycle will review all the controls that cover one of the product lifecycle stages. There are 2 review cycles per year, timed to coincide with the issuance of the 6-monthly Regulatory Compliance and Audit Report. There are 4 product lifecycle stages;[28]

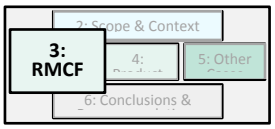
- Change Control
- Pre-Ordering / Ordering
- Provisioning
- Fault Report / Repair

These reviews are done on a best-efforts basis.

The C&E evaluation methodology for Change Management Controls, was reviewed and described in the May 2016 Regulatory Compliance and Audit Report. The primary review methodology was a walk-through of the Change Control Logs. The review was both qualitative and quantitative, and included the following:

- Quantitative identification of instances not reported or logged correctly, or where evidence was not retained or available;

[27] Wholesale Reforms Committee HIA Summary Report. These are carried out by Internal Audit on an approximate 6-monthly cycle, and added as an appendix to the Regulatory Compliance and Audit Report, where it is referred to as the 'Internal Audit report'.
[28] The Regulatory Compliance and Audit Report, May 2015, Page 97, lists the review areas by C&E.



- Qualitative reviews of the logs to identify whether the sequence of control procedure events was complete, and whether the right decisions were made on the evidence provided.

A list of issues found in the report is maintained, as is a set of recommendations for next steps.

Observations

O 15: The risk and control review cycles are too infrequent. IA completes a review cycle in 3.5 years. Therefore, the same group of controls will not be reviewed again till 4 years later. For C&E, a review cycle completes in 2 years, so the same control group is only reviewed every two and a half years. These are done on a best endeavours basis. There is nominally one individual in each group that is tasked with this, and they have other tasks that they are supporting as well.

O 16: There is no evidence of consistent follow-up. While both groups record the outcomes and schedule follow-up meetings, these appear to be informal, and there is no escalation criteria and path for outstanding issues. Without severity criteria, escalation timeframes, nor documented escalation procedure, there cannot be any reliable escalation of defects with the controls. Several examples of such defects occurring for extended periods exist.

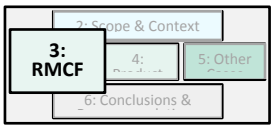
O 17: The recording of the controls in the RACM tool has improved over time, with a steady reduction in inconsistencies, incorrect or blank required field values, and the recording of change events. However, the tool requires a significant degree of manual cross-checking and validation, and does not allow a direct comparison with prior versions, meaning inconsistencies will be hard to eliminate.

O 18: The RACM that is maintained by IA is used to track the status of controls. It also drives the Self-Certification reviews and the IA and C&E reviews. The RACM are maintained as a series of versions over time. Key change events to controls, such as the initiation dates of a control, merges, change of control stakeholders and departments, product families, etc., are not reliably tracked. The mechanism used within the spreadsheet to track this is insufficient. Only a single change date and change event type can be assigned in a RACM version, yet several change events could have taken place between versions, with different event types and dates, which are thus lost.

O 19: The RACM, which tracks the status of every control, does not include the dates IA, C&E and Self-certification reviews, nor the outcomes of these reviews. There are no other tools or processes for tracking defects and analysing them over time. C&E explained that they reviewed the past period's reports prior to beginning a new review cycle, but this is not effective, as controls do not get reviewed again for at least 2 years, and follow-up was not mandatory. The fact that controls can stay defective for several quarters indicates the ineffectiveness of any trending and escalation.

O 20: The reviews showed significant percentages of defects, some of them indicating the control had either not been run, run incorrectly (and were therefore ineffective), was aspirational, or that no evidence had been preserved. These findings are deemed very significant, as the controls had high defect rates; in some cases, less than half the controls were effective within a review area. The types of issues identified were severe[29]. In several cases, even if the control had operated, it would not have mitigated the risks.

[29] Regulatory Compliance and Audit Report, May 2015, Page 103-104.



Cartesian Process Quality Score: 80%[30] Cartesian Process Capability Score: 50%[31]

6. Statement of Compliance (SoC) Publication

When a new product is developed, or changes made to an existing product, eir is required by regulatory obligation to issue a SoC. In summary, the SoC must demonstrate how eir remains in compliance with its regulatory obligations. The SoC is produced by the L1[32] of the BU to certify that the RAP has been designed appropriately, and that the operational processes covering the product lifecycle are compliant with the obligations for its respective Regulated Market.

Observations

O 21: An established but informal process exists that is dependent on a small number of subject matter experts to operate reliably

O 22: There is an established but undocumented process for creating the SoC, which is initiated by the product manager.

O 23: There is no official role for the coordination of the sign-offs when multiple SoCs are required.

O 24: There is no formal independent review internally, only informal SME reviews.

O 25: The various internal review approvals preceding the issuance of the SoC are done informally; the evidence in most cases is an email reply to the original request for a review.

Cartesian Process Quality Score: 40% Cartesian Process Capability Score: 56%

3.4. Business Unit Self-Certification Processes

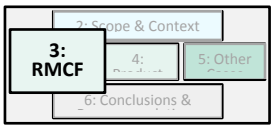
The Self-Certification Process in conjunction with the Governance processes, are the foundation for the RMCF, and are used by eir to attest to ComReg that it is in compliance with its Regulatory Obligations. Therefore, any weaknesses in the Self-Certification process can significantly risk eir's ability to comply with its Obligations.

Cartesian examined three BUs to understand how they operated the Self-certification processes. The BUs were:

- eir Wholesale RAP Markets
- eir Enterprise and Government Markets
- eir Fixed Access Operations

These processes were categorised into specific process layers, from operational processes, the management processes overseeing these operations, and lastly, the assurance processes carried out by separate BUs in eir.

[30] C&E review of Operation of Controls. The scope of the quantitative scores did not include the evaluation of the follow-up processes.
[31] C&E review of Operation of Controls
[32] The L1 signifies the 'Level 1' manager for the department, thus the senior-most member of the department.



Operational tasks were carried out by the BUs at regular intervals, primarily driven by the triggering of the Self-Certification process by IA. The operational processes include the following areas listed from Items 7 to 15.

7. BU Control Operations

The control operations process[33] from initiating the operation of a control, through to its reporting was examined from the perspective of the BUs that owned the controls. Control operations are triggered by an email request from IA, which contains a list of controls the Business owns.

Observations

O 26: BUs do not have a common standard process for tracking and managing control execution exceptions. There are no documented requirements or standards for BUs to manage and rectify exceptions, nor how they are to be prioritised. For example, there are no standards that defined that an exception of a given severity level must be rectified within a certain period. No standards exist to define severity levels across BUs.

O 27: There is no consistent process that all BUs follow for operating their controls, and logging the operation of the controls. Only the entry and exit points are defined.

O 28: An escalation process for dealing with problems in running the controls does not exist. There is limited ability to identify recurring problems from quarter to quarter. There are several cases where missing evidence of operations, or self-certification of non-operation of a control, has continued for several reporting quarters.

Cartesian Process Quality Score: 40% Cartesian Process Capability Score: 38%

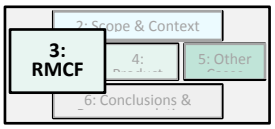
8. Self-Certification Reporting

The Self-Certification Reporting process covers the generation of the approved self-certification report to the submission to IA, and storing of any necessary documents within the specified storage locations. Evidence storage management is discussed separately. Reporting also covers any exception issue reporting.

Observations

O 29: The formality of the process where the Control Owner confirms that the self-certification can be signed off varied extensively across BUs. There are no standards established for what checks are required, aside from the control procedure itself and the two questions posed in the RACM. For example, there are no checklists for the control owners[34] to ensure that the executors accomplish their tasks correctly. There are several recorded instances where the control procedure has not been executed properly[35].

[33] The process is documented in 'Operation of the RACMs and Controls within eircom', Version 1, dated 26/11/2014.
[34] Control owners are accountable for the definition, operation and results of a control, and ultimately, the risk mitigation.
[35] Self-Certification Reviews, IA and C&E reviews.



9. Exception Identification, and 10. Exception Handling

These two processes are dealt with together. When controls are operated, exceptions may be encountered, consisting of:

Exceptions reported in the control reports. These are issues that the control reports were designed to expose (controls generally require a report to be generated, which highlight exceptions that the control is designed to reveal), and generally, there are procedures documented in the controls as to how these are handled and reported.

Exceptions in the operation of the controls. These are issues encountered when the controls were run (i.e., the control procedure did not run as documented, or could not run as documented). As an example, the control procedure could be found to be incorrect, or missing steps.

These processes should clearly define the approach to identifying and handling control exceptions. Some types of exceptions covered anything out of the ordinary, whereas others could have different degrees of severity. This process deals with the identification of all the above exceptions.

Observations

O 30: There is no standard for identification and research into any exceptions, nor what evidence of this research needs to be maintained. There is wide variability in the knowledge of the control owners and executors on maintaining the evidence. In one case, both the control owner and executor were unaware how, by whom, or what was stored, and where.

O 31: None of the BUs maintains a formal, documented escalation handling process that covered exceptions outside, where it existed, the definitions within the control procedure. None of the BUs maintains any formal, documented standards and criteria for issues that required escalation. In many cases, the control procedure definition of exception events is unclear.

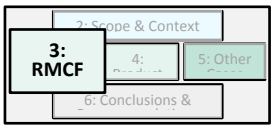
O 32: Some BU controls had escalation processes for control failures. However, the process was not always adhered to.

O 33: Exceptions either in the execution control procedure, or the results of the control operations are noted in the Self-Certification. These are also noted by IA, but the process for managing and tracking these is informal. There is no escalation path within IA for ensuring that such exceptions are dealt with and resolved within a given time frame. As such, it is possible, and cases have been noted, where the same self-certification failures have occurred over several self-certification cycles with no resolution.

O 34: Several controls were not operated at all, operated incorrectly, or there was no supporting evidence that the control had been operated. (This includes cases where the location of the evidence was inadequate.)

O 35: Some controls are 'Aspirational'[36], which means that there is a mitigation plan, but it had not been implemented yet. This term was used by IA, and Cartesian has used the same definition. These controls typically required computer systems to be changed. Most of these

[36] 'Aspirational' was used and described in the WRC HIA Summary report, November 2014 onwards.



remediations did not occur on time, and some of them had no mitigations in effect while awaiting the permanent remediation.

A differentiation has been made between Self-Certification process operations and the management of these processes. BU Management functions are broken out into the processes listed in this section.

11. BU Control Management

The purpose of BU Control Management is for ensuring that controls are operated when required, and follow correct procedure. They should ensure that the procedures and results are properly documented, accurate and can be operated.

Observations

O 36: There are no standards to guide the Business Owners on how to undertake a thorough investigation before signing that the control operates as specified. Documentation for the procedure exists, there are, however no standards associated with the process.

O 37: Failures are not consistently documented in the control reports. Processes are not documented, and it is left to each individual owner to follow up on the resolution actions. The question the control owners must respond to, "Is this control effective", does not describe what is meant by "effective", and is left to the interpretation of each control owner.

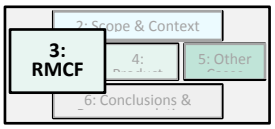
12. BU Exception Management

Exception management covering all types of exceptions, should ensure that required decisions are made, and provide oversight of control operations to ensure that the correct course of action is followed. This process should include exception risk verification and mitigation. A distinction should be made between handling the exception and managing them. In the cases examined, this distinction did not exist, as exception handling itself was done by the managers themselves.

Exceptions include control operation issues, incorrect control documentation, Control effectiveness, Change Requests, and retirement requests. Change Requests are evaluated for any changes to the risks and thus the controls.

Observations

O 38: There are no standardised criteria for evaluating exception events such as retirement, or merging of controls. This would ensure consistency of the standards used for deciding on these and ensuring that they are comprehensive and assessed reliably and consistently.



13. Self-Certification Sign-Off

The BU manager (L1[37]) is required to validate the controls and exceptions, before the Self Certification sign-off. The process starts with the presentation of the data set to the manager, who checks and investigates any discrepancies, and when satisfied, signs and submits the certificate to IA.

Observations

O 39: There is no 'audit trail' that provided assurance that the L1 sign-off is confirmed by verifications with the control executors[38] and L2 managers that own and operate their set of controls.

O 40: There is no clear separation of duties; those doing the certification in downstream BUs are often involved in non-RAP activities as well.

14. Self-Certification Record Management

The purpose of Self-Certification Record Management is to ensure that the set of reports, including any exceptions, are maintained per the documented procedures specified in the RACM, and that the evidence is intact and retained for the appropriate periods.

Observations

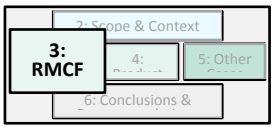
O 41: Each control's documentation, even for the same control owner, could vary significantly because no standards or organisation requirements were developed for managing them.

O 42: Each BU has its own document management and storage structures and locations. Various controls' evidence could be stored differently.

O 43: The RACM does not maintain a clear evidential trail for the controls and their risks. A common occurrence is when remediations are involved. Key dates are not consistently maintained in the RACM, nor are key milestones, such as the date a remediation became operational. Target dates, especially confirmed ones after the remediation had been accepted into development, are not visible. In many cases, there is no documentation of the Planview ID[39] provided, so even if it was desired to cross-check details in the Planview system, it was not possible to do so reliably. The ability to obtain dates for the origination of a risk, deployment of a control, and when a control was retired or merged is inconsistent.

O 44: In many cases, several controls relied on the same software fixes to remediate the risk. These controls did not record the same remediation dates when provided, even when they referred to the same Planview ID. The effective dates when controls were remediated are unclear.

[37] 'L1' refers to the senior-most, or 'Level 1' manager in a BU in eir. 'L2' refers to the managers who report directly to the L1.
[38] Control executors are defined as eir staff who are responsible for the execution of the control procedures, with the control owners being accountable for this work. The control owner is typically the 'L1' - senior-most member of the department.
[39] The Planview ID is the identification number used to register and track projects within eir's Portfolio and Programme Management tool.



O 45: Many controls were reported to lack control evidence in the Self-Certifications, or through IA and C&E reviews. Added to the low frequency of independent reviews, this is a serious issue that calls into question whether some controls are being operated at all[40].

O 46: There is no documentation on, or standards for the preservation of evidence that controls operated correctly, nor how it was carried out. System controls are not tracked to ensure they are delivered on time (the Regulatory Compliance and Audit Report reports on implementations, but not timeliness, consistently). There are no tools or processes being used to maintain an understanding of gaps caused by delays in remediations.

Assurance capabilities over the operations and management of the self-certification processes was also investigated. The organisations within eir responsible for this included IA and C&E.

15. Self-Certification Review (Assurance)

This assessed the assurance done as part of the overall self-certification process, and the interactions between IA / C&E and the BUs who operate and manage the controls and self-certification processes. The process completes when the self-certification is reported to IA and accepted by them.

Periodic reviews by IA and C&E of the controls is covered in the Risks and Controls Assessment in the previous section.

Observations

O 47: IA's review is designed to ensure that the control procedures have been followed, and that the control evidence is correct in what is specified to be provided, and where it is held. However, it does not assess the control's ability to mitigate risk. Investigations of control evidence issues may be escalated to C&E.

O 48: C&E's review is focused on the evidence to assure that the results generated were dealt with correctly, which also means that the evidence is correct. This also verifies that exceptions are correctly identified, and that the corrective actions are listed, but does not verify whether a control mitigates the risk adequately.

O 49: There are no corporate standards for self-certification within BUs, nor for the maintenance of evidence for BU certification. There were high control failure rates when reviews were carried out.

O 50: Although the IA Charter gives them access rights to all evidence, IA and C&E do not have automatic rights to access control evidence, and must specifically request access to the evidence when the review begins.

3.5. Cases and Chronology

The entire set of Controls that have been developed, implemented and operated were examined to understand the history of each of the controls, and the quality with which they were operated and managed through their lifecycle. Cartesian also examined the self-certification results of these controls,

[40] Cartesian requested control evidence for many controls, but only received a small number within the research timeframe.

where documentation was available. Thirdly, assurance reviews by IA and C&E were examined. Lastly, a subset of about 100 controls[41] were reviewed in detail, which covered all the Equivalence / gap issues listed in the May 2015 Regulatory Compliance and Audit Report, plus a significant number of others. This was done to understand the effectiveness of the controls in mitigating the risks for which they were designed, and how well they had been operated historically.

Additionally, issues with how controls are documented and tracked, and their ability to provide the information needed to understand their effectiveness, were examined. Much of the control evidence requested by Cartesian were not provided within the research timeframe, despite multiple requests.

Change Management controls were reviewed by C&E in the May 2015 Regulatory Compliance and Audit Report[42]. Cartesian examined the effectiveness of the controls throughout their active life histories, their related controls, based on IA, C&E and Self-certification review results, as well as our analysis of the controls. We assessed whether they were effective in mitigating the risks, and where possible, the risk exposures that existed due to non-functioning or delays in implementation of the controls.

Sixty-three controls were reviewed in open eir, fifteen in Fixed Access Operations, and two in the Enterprise and Government Markets BU. These provided close to 100% coverage of the active and retired controls for each of these BUs as of the June 2016 timeframe.

Observations

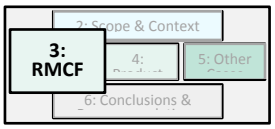
O 51: In one case, there was no named control executor, only a title name, which does not match the title of the actual proxy control executor. This individual became aware of the need to execute these controls because he was executor for some other controls, and assumed that these controls also had to be executed. This was also based on experience. More importantly, the chain of responsibility became unclear for audit purposes.

O 52: There was one case where the control was operated incorrectly. Rather than identify exceptions and report their outcome, the control report was used to eliminate exceptions. After the exceptions were cleared, the report was run again, to show that no exceptions occurred and none were left to report. This contradicted the control procedure, which required that the exceptions be reported, the reasons why, and the corrective actions.

O 53: [redacted][43].

O 54: There are some ineffective controls. For example, one is to ensure that non-standard orders[44] are reviewed by RAP. The only control check is for orders that are marked as non-standard. Therefore, non-standard orders marked as standard would never be examined by this control. (The risk impact is low, as these incorrectly-marked orders would be subsequently inspected

[41] The reviews generally consisted of a primary control and a subset of related controls, either through merges, or common risks. These complicated the count of controls reviewed in detail, as some of the related controls were fully reviewed as well, based on the investigation results.
[42] 'Change Management' is one of the four classifications of process areas. Each of these areas is reviewed by C&E in a review cycle.
[43] [redacted]
[44] 'Standard' orders consist of all RAP order components. 'Non-standard' means that an order has non-RAP components included, which may include a build element,



by an engineer team, who are also required to review and mark the order as standard or non-standard through a separate control.)

O 55: Risks were not appraised properly for Impact and Likelihood. The percentage of these fields that were populated was very low, and where there was a value, there was a large percentage of non-valid values. Only 45% of risks had a qualitative Risk Impact and Risk Likelihood value assigned in the last RACM examined (June 2016)[45]. These values were 'H', 'M', and 'L', but had no definitions for what they meant, nor how they were to be assessed.

O 56: The definition of 'Risk' was not clearly used. Instantiated risks, or issues, versus risks were not delineated. Combined with the lack of a proper risk impact and likelihood analysis, this meant that compliance exposure could not be properly assessed using the information in the RACM.

O 57: The RACM did not contain any information on the results of Self-certification, nor any of the reviews by IA and C&E. eir has pointed out that the RACM was not designed to track the results of self-certification. However this is critical information that shows the status of a control and it is not captured in a single place.

O 58: While record-keeping quality in the RACM improved over time, it was still inconsistent, and not maintained to a sufficient standard for audit records, as some critical data fields were not consistently populated and certain critical events were not recorded.

O 59: The two key roles responsible for Self-Certification are the Control Executor and the Control Owner. IA stated that if either of the Title field or the name field was populated, it would be sufficient to determine who these individuals were. However, good record keeping practices dictate that these fields should always be populated. The Self-Certification contained the signature and title of the accountable Control Owner, but there was no indication of the executor and thus there would not have been any responsibility trail extending to the executor.

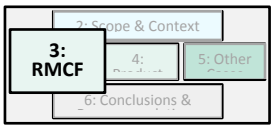
O 60: There are other issues, although not prevalent, that persisted over long periods. These included related controls that they were dependent on to be effective, but the related control had been parked since the control was created[46]. A control was 'parked' when no further activity was carried out to implement the control.

O 61: There did not seem to be any effective escalation mechanism in place. Issues that occurred with controls could persist over several quarters, as listed in the previous observation. It was reported by both C&E and IA that they followed up with the control owner to check whether anything had been done. While it is acknowledged that this check was probably done, no escalation occurred to ensure that action was taken to rectify the situation. The evidence was in the persistence of the same issues for the same controls across several quarters.

O 62: There was no tool or mechanism in place to provide a status view of the trending in the operations of the controls. It was not possible to understand from the RACM whether a control was defective, as there were no records included for Self-Certification reporting (except "Signed Off" under "Management Status"), nor for IA and C&E reviews. It required

[45] In MoA 2.9, 'Impact' had 13 Blanks, 32 'H', 35 'M', 7 'L' and 76 'NA' values, for a total of 163 active controls. 'Likelihood' had 13 Blanks, 19 'H', 14 'M', 41 'L', 48 'NA' and 28 that had a value of 'Risk' assigned. Blank, 'Risk', 'NA' were considered invalid.

[46] Control ID WRP_CRM_132: Other controls indicated they had defects for several quarters continuously, such as WRP_CRM_056, NGAWBA_CRM_011



relatively complex analysis, as executed for this assessment, to understand quality trends and to obtain a historical view of a control.

O 63: It is noted that record-keeping has improved over time. Additionally, the captured changes to Controls recorded in the RACM had improved. However, issues still remain with the quality of the record keeping.

3.6. RACM Summary Conclusions

C 1: There are significant gaps in process documentation for the risk and control management processes, at the operational, management and assurance levels. There is also a lack of defined process owners, and management standards. There are no process standards (tolerances), criteria, nor documented escalation processes.

C 2: There are no standards for risk identification and assessment in terms of probability, impact and timeframe, leading to an inability to prioritise controls development, and the level of mitigation necessary. Such standards are also required to assess whether the implemented control was sufficient to mitigate the risk.

C 3: Defects occurred in a very high percentage of the reviews, over an extended period, demonstrated through self-certification, and IA and C&E reviews. Cartesian's review of selected controls also found defects with several of them. A significant percentage of the controls reviewed are defective in one or more ways. There are sufficient cases where defects occurred over several quarters, either contiguously or continually, that it raises concerns about whether any tracking and corrective measures are enforced[47].

C 4: There are no processes for ensuring that the controls mitigated the risks, aside from what is done during the initial development for the control (There is no assurance testing in these developments). The process used in design for identifying and assessing risks is informal. There are no criteria nor checklists covering what needs to be checked for, by assessment area. Eir has pointed out that it previously had a process but Cartesian found no evidence of one being currently operated.

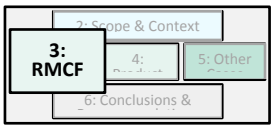
C 5: The Self-Certification process is not reliable enough, nor consistently applied, to assure the successful operation of the Regulatory Governance model. The Certification process has several serious deficiencies and lacks effective assurance oversight.

C 6: Evidence of control operation and their outcomes are not consistently maintained. There is no central repository, standardised format, nor reliable and consistent access mechanisms for control evidence.

C 7: Trending of controls to identify consistently failing controls is not undertaken, and no standardised escalation process is in place to handle such situations.

C 8: The tools (RACM spreadsheets) that are used for managing risks and controls are limiting and cumbersome, with missing information that is necessary for the effective management of

[47] Examples include: November 2014 IA review indicated that up to 100% of the 57 controls reviewed were defective in one way or another. The IA review of December 2015 report indicated that up to 39 controls out of 48 reviewed were defective (the number cannot be determined accurately, as some controls could have more than 1 defect. Non-defective issues, such as unnecessary details, were not included). In the same report, the Self-Certification process revealed 26 defects in 168 controls. C&E's review reported March 2016 Regulatory Compliance and Audit report indicated that only 8 out of 16 controls reviewed operated effectively.



controls. Control defects identified by Self-Certification, and C&E and IA reviews are not tracked in any single tool, nor trended over time. It required a significant amount of manual analysis to create a chronological view of control lifecycles, to determine what periods it was to be in effect and operated correctly.

C 9: Mitigation controls require the use of instructions to follow a process, such as for certain groups of staff not to access particular information as part of their job. Many such risks that use this type of control were issues (the risk had materialised), with known instances of violation. Cartesian believes that instructions to employees not to use tools or documentation to access non-equivalent information provides inadequate safeguarding.

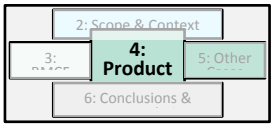
C 10: Assurance cycles by IA and C&E are carried out too infrequently. The inspection schedules were 4 years, and 2 years, respectively.

C 11: The identification of stakeholders and their roles is not consistent in maintaining a continuous tracking of the Control Owners and Executors. There were a few cases where either the department name, or the stakeholder name, were found to be missing.

C 12: C&E perform two roles: guidance in the design of controls to mitigate risks, and assurance that controls are operated as designed. This may lead to an inadequate separation of duties.

C 13: Coordination between Compliance & Equivalence and IA is unclear regarding assurance tasks and accountabilities for regulatory governance assurance. For example, both groups carry out different, but somewhat overlapping inspections of controls, but neither party formally confers with the other in reviewing the results of the inspections, (excepting one escalation process from IA to C&E_)

C 14: Staffing of C&E and IA appears to be inadequate to properly execute all responsibilities at frequencies that are desirable (all controls inspected at least annually). Several functions are entirely dependent on one or two people to perform, leading to increased sustainability and reliability risks in the long run.



4. Product Work Streams

4.1. Objectives

Processes covering the operations for Product Lifecycle and Development, their management framework and the assurance framework were reviewed.

This review was undertaken to assess product life cycle processes against the criteria in Table 1 on process quality, and capability, and to further test if all users had the same experience of using the processes. As previously stated, Cartesian tested the processes under consideration to assess if they were stable, capable, repeatable and had reliable metrics such that regulatory risks could be identified and controls applied in a consistent manner.

In this context, the objectives of the assessments were to:

- Understand operational process steps where risks can occur;
- Assess potential variability in a process and identify where it may occur;
- Assess whether risks associated with a process are stable and therefore whether controls can be implemented and their effectiveness measured;
- Assess a risk in terms of impact on the process.

4.2. Scope

The analysis of Operational Processes consisted of Product Life Cycle processes, Product Development processes and SLA development.

Product Lifecycle processes covered Next Generation, Current Generation, and Passive Infrastructure products. Cartesian interviewed key stakeholders in product and change management, and reviewed materials provided by eir for this assessment.

This section contains:

- A process review;
- A process or case walk-through; and,
- A chronology analysis. The chronology analysis was to test if conclusions arrived at during the process analysis and walk-through reviews were reflected in the overall population.

4.3. Product Operational Lifecycle Processes

The typical customer lifecycle for a product includes these five major functional areas:

1. Pre-Ordering processes include product availability determination, lead time determination, pre-requisites. Ordering covered Customer and product information capture, and order orchestration.
2. Provisioning covers services configuration and activation, and billing set-up.
3. Fault reporting and repair includes the initiation of a fault repair request through the resolution of the fault.

4. Change Management covers the initiation of requests, consideration and outcome, leading potentially to product development.

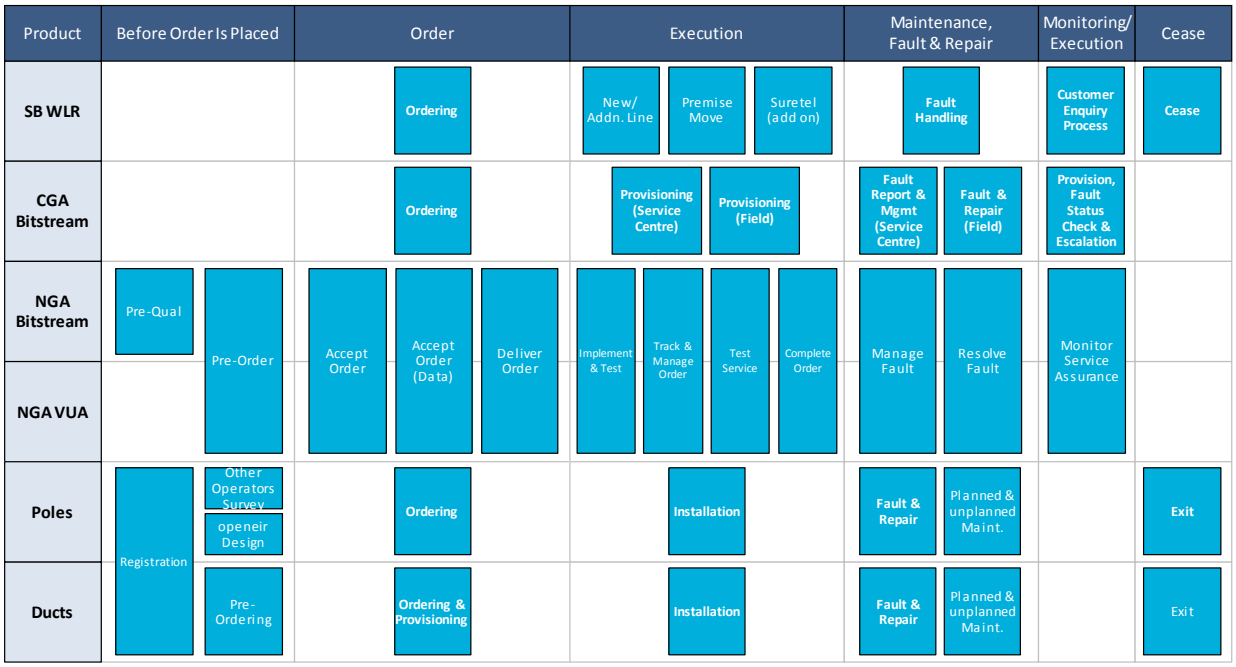
The products for which these processes were examined included;

1. SB-WLR
2. CGA Bitstream
3. NGA-Bitstream+
4. NGA VUA
5. Poles
6. Ducts

The stakeholders impacted by these processes were other operators, eir Product Management, eir Wholesale Customer Contact Centre Management, eir Systems Architects, and ComReg. The key stakeholders were interviewed and relevant documentation such as process documentation, Statements of Compliance, Industry Process Manuals (IPM) and Product Descriptions were reviewed and assessed.

The assessment of common processes used across the various products' lifecycles is illustrated in the diagram below.

Figure 5. Product Operational Lifecycle Processes



In general, these processes were well documented, robust and mature, and covered the range of in-life product operational processes from pre-ordering through provisioning to service assurance. However, while Pole and Duct Access processes were well documented, there was no customer uptake and process capability was not subjected to in-life operational tests [redacted]

4.4. Product Development Lifecycle Processes

The product development process has four phases:

1. The process from receipt of a change request to its inclusion in the Product Change Request Log (PCRL). This is highlighted as the 'preamble' stage in Figure 6, below;
2. The Product Change Request Phase;
3. The end-to-end technology development and RGM Phase; and,
4. The Product Development Council Phase.

1. Preamble Phase

The preamble process consists of the raising of a change request by an OAO or eir downstream business unit, to this request being logged in the PCRL. This is a critical first step, during which an initial assessment is made prior to inclusion on the PCRL. This process starts with discussions between the requesting entity (OAOs and eir downstream business units), and open eir product management and technology engagement specialists. These discussions can continue beyond the Preamble Phase. The channels used for these include account management channels and industry forums.

2. Product Change Request Phase

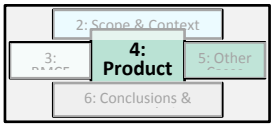
This phase considers whether a request has RAP implications and decides on the submittal of the request to Ideation. Ideation is the first step in the technology development process.

3. End-to-end technology development and RGM Phase

This includes an initial assessment of a request in terms of a technical solution and associated resource requirement through to deployment. There are a number of defined gates in the process. The Technology End to End process is the process, through which all projects requiring IT scoping and development resources, are progressed. The rate at which the overall portfolio of projects progress is determined by the availability of resources and Capex at key stages in the process. The Portfolio Board coordinates the flow of projects through the process. KPMG reviewed the structure and governance of the Portfolio Board.

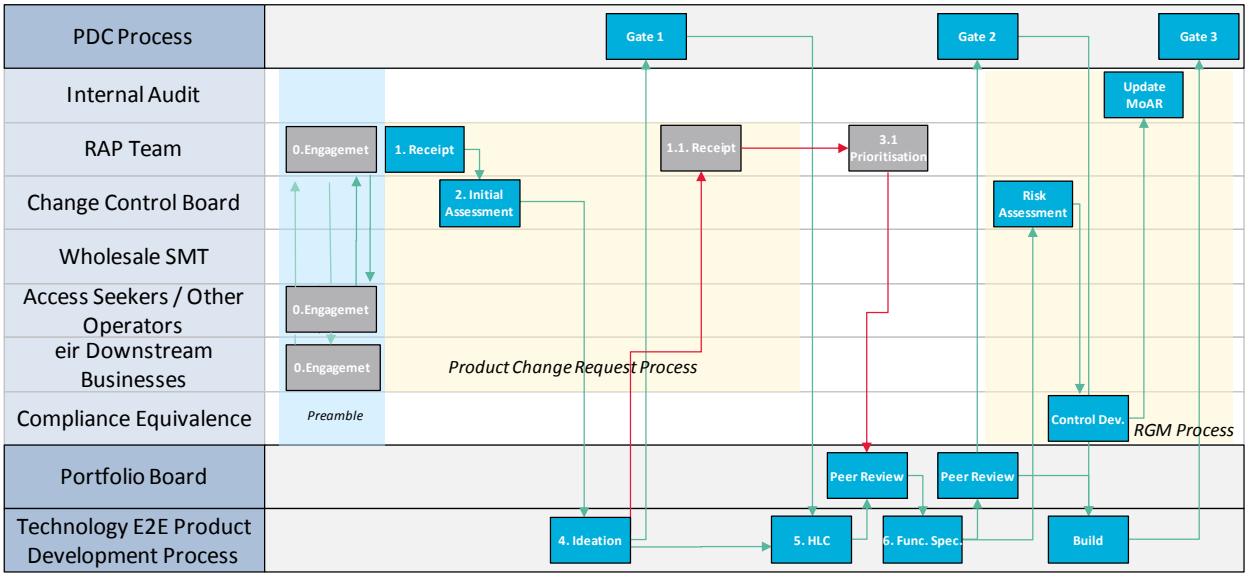
4. Product Development Council Phase

This step formally approves projects to move through key stages in the end-to-end technology development process. Central to this process are three approval gates – Gate 1: approval to proceed to



detailed technical consideration stages; Gate 2: approval to proceed to technical development and Gate 3; approval to launch.

Figure 6. Product Development / Change Process Flow



Note: Process block item numbers are referred to in the process explanations that follow. Green lines / arrows indicate the normal process flow; red indicates the handling of an exception event.

Process Quality and Capability Scoring

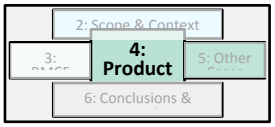
An explanation of the scores associated with each of the process descriptions below were provided in section 3.3 above

0. Preamble Process

This is the entry point for requests to be processed as part of the Product Development process. It is a process that includes dialogue between the requesting entity (account management channels, industry forums, eir downstream business units), open eir product management and technology engagement specialists. It also is the point where actions from the above channels come together and should be dealt with as part of a single process.

There are a number of participants in the process, internal and external to eir, operating with varying modes/degrees of interaction and formality. Because of the variety of channels and modes of interaction, it is particularly important to have a robust and transparent process in order to minimise the risk of non-discrimination by open eir in the treatment of requests from all participants.

Observations



O 64: There are no formal processes, standards or performance metrics for dealing with requests, nor was evidence found of any controls over this phase. As outlined above, this is of particular concern in the context of the risk of non-discrimination.

Cartesian did not score this as it was not identified as a formal process but crystallised during the product development case and engagement channel analyses. These analyses are dealt with later in this report.

1. Initial Receipt of RAP Change Request

This process starts with the receipt of a change request or product development request and the initial scoping and logging into the PCRL[48]. The requested change is assessed by the Change Control Board to determine whether it involves a Regulated Access Product and is therefore subject to regulatory compliance risk assessment.

Observations

O 65: This is documented and is a well understood process from the point of final receipt of a RAP change proposal. Product requirements are also well-documented. The process has a clear RACI[49] matrix for each of the process steps.

O 66: Formal ownership of the process needs to be clarified.

O 67: There is a clear separation of duties, insofar as this is done by a separate team.

Cartesian Process Score Quality: 70% Cartesian Process Score Capability: 69%

2. Initial RAP Assessment and Progression to Gate 1

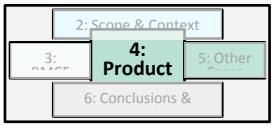
This process determines whether a proposed product change is RAP or has RAP elements, in order to consider whether it should be submitted to Ideation. The process is undertaken by a group that includes Product Management, Regulatory Operations, and Technology Engagement. If the proposed product change is considered a RAP change, it is then reviewed by the RAP Product Development Council (PDC) at Gate 1, which is the first step in the end-to-end technology product development process.

Observations

O 68: There are no documented assessment criteria to determine if a request has RAP implications. While not documented, the process was well-understood by the participants.

O 69: Decisions are made by the group, as described above, based on their expert knowledge of the Code of Practice[50] and understanding of Regulated Markets[51]. The process depends on a small number of people and there is a risk to the sustainability and repeatability of the process in the event these persons should leave the organisation or are otherwise indisposed.

[48] PCRL is the Product Change Request Log, which registers all requests for changes or new product requests for RAP.
[49] 'RACI' stands for Responsible, Accountable, Consulted and Informed, and is a methodology used to document the roles of staff involved in a process.
[50] The Code of Practice (CoP) was introduced in April 2013 to drive improved governance, by helping employees and contractors understand how to comply with eir's Regulatory Obligations. This is one of the three stands of the Regulatory Governance Model.
[51] Regulated Markets are those in which ComReg has deemed eir to have Significant Market Power (SMP).



Cartesian Process Score Quality: 40% Cartesian Process Score Capability: 25%

3. Prioritisation of RAP Requests

This process handles the prioritisation of non-RAP and RAP requests, and between requests within the RAP category. The process involves decision-making about the priority/order in which product change requests are initially submitted and progressed through the product development process. Central to this process should be a set of decision-making criteria which is commonly understood by all users.

Observations

O 70: This process is central to the operation of a transparent and reliable Product Development / Change process. However, there is no documented process with assessment criteria. There is no evidence of how decisions were made, and lack of transparency in prioritisation.

O 71: No evidence has been produced of independent organisational assurance of the decision-making process and outputs. This process step is not included in the published process documents[52].

Cartesian Process Score Quality: 20%. Cartesian Process Score Capability: 44%

4. Product Change Request Assessment - Ideation

This is the first stage in the generic IT development process. It starts with the initial, high level assessment, by IT Solution Architects, to identify potential solutions and estimate the required development effort. The evaluation capacity is constrained as this is determined by the availability of solution architects, system architects, business analysts and other downstream development resources. The output of this process step is a Rough Order of Magnitude resource assessment.

Observations

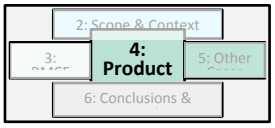
O 72: This is a robust process which meets its objectives of providing Rough Order of Magnitude resourcing estimates of each proposal. No evidence has been produced of independent organisational assurance of the decision-making process and outputs.

Cartesian Process Score Quality: 40% Cartesian Process Score Capability: 75%

5. Product Change Request Assessment – High Level Concept (HLC)

The High-Level Concept stage in the overall Product Development / Change process is designed to establish resourcing needs of each of the proposals submitted and to ensure that all proposals going to Functional Design will fit into the established resource constraints. The output of this stage is a high-level resource and cost assessment.

[52] RAP Product Development Process. V2 - Internal



The Portfolio Board reviews the output of this stage. This process meets its primary objective of ensuring the optimum utilisation of system architect and development resource.

Observations

O 73: This is a well-documented and mature process which meets its objectives of ensuring a smooth flow of work to technology development units. It does not guarantee an equitable sharing of resources between RAP and non-RAP. However, Cartesian has identified a control to monitor the timeliness of RAP and non-RAP through the technology development process.

Cartesian Process Score Quality: 70%. Cartesian Process Score Capability: 75%

6. Product Change Request Assessment – Functional Design

The Functional Design stage in the overall Product Development / Change process is designed to establish more accurately the delivery resource implications of each of the proposals submitted and to ensure that all proposals going to Delivery will fit into the established resource constraints. The outputs of this stage are detailed business requirements, a functional specification and a solution assessment which contains cost and resourcing impacts.

The Portfolio Board reviews the output of this stage. The BU takes the output to the Capex Committee for final approval. This process meets its primary objective of ensuring a smooth flow of work to the established development resources.

Observations

O 74: This is a well-documented and mature process which meets its objectives of ensuring a smooth flow of work to technology development units

Cartesian Process Score Quality: 70%. Cartesian Process Score Capability: 75%.

4.5. Product Development Case Assessments

At ComReg's request, Cartesian reviewed a sample set of product development requests to determine the approach taken by eir in dealing with these .and to assess how Eir ensured compliance with its regulatory obligations. These reviews focused on whether formal processes for the development of these product cases existed and were sufficiently robust to demonstrate that eir identified risks and applied controls, to ensure it could comply with its regulatory obligations. These reviews were undertaken in the context of the RGM and focused on the existence, quality and capability of processes and whether relevant controls were operated by eir.

There are several distinct process phases in the development of a product or change request. Our case analysis involved a review of the end to end process, from an initial request to final deployment for each of the cases. Comments in this section deal exclusively with the processes from initial request / mandate to logging in the PCRL and general decision making processes. The early phase of the process – from the formal logging of a change request in the Product Change Request Log through the IT development stages – is reviewed section 4.4, item 1, Initial Receipt of RAP Change Request, and therefore not specifically commented upon here.

The reviews included a detailed analysis of the key milestones and elapsed times from the date on which a request was made (or product mandated by ComReg) to the date of final deployment[53]. They also include assessments of the key decision points for each case, and the processes and documentation used to arrive at these decisions.

This assessment reports on the elapsed times, process quality, key decisions/decision makers and supporting documentation.

- Elapsed time is the main indicator of timeliness of product development. Elapsed times will vary depending on the complexity of the requested development. For instance, developments with complex IT elements in the solution can be expected to take longer than requests which only involve process change. We summarized the elapsed times and we have attempted to reflect these differences in our comments.
- Process Quality involves the existence and quality of documentation and the organization which is dedicated to supporting the process. A documented process, supported by sufficient organisational resources is essential to enable regulatory controls to be applied in a consistent manner and to provide transparency of the processes which were followed. Access to the processes can only be consistent if documentation is available.
- Transparency of the decision-making process, including nominated decision makers, decision making criteria and supporting documentation, is necessary to demonstrate that regulatory obligations were considered and acted upon.

4.5.1. Product Development Cases

The following are summary descriptions of each of the product cases together with key observations for each.

1. Duct Access

[redacted]

Observations

O 75: [redacted][54] [redacted][55] [redacted][56].

O 76: [redacted][57].

O 77: [redacted]

[53] The elapsed time for two of the cases (Duct Access and SLA development) commenced before the establishment of the RGM. The development time for all cases continued after the establishment of the RGM in 2012.

[54] [redacted]

[55] [redacted]

[56] [redacted]

[57] [redacted]

[redacted]

O 78: [redacted]

O 79: [redacted]

2. SLA Development

Cartesian examined the development and publication of SLAs for (a) Single-Bill Wholesale Line Rental (SB-WLR) and Local Loop Unbundled (LLU), (b) Next Generation Access (NGA) and (c) the Universal Gateway (UG).

All Current Generation Access (CGA) products had an existing SLA and NGA products and UG had new SLAs developed. Many of these had been in existence for a long period. Drivers for updates to SLAs include product changes, such as those due to improved systems supporting a product. There were also operators' requests for SLA refreshes.

Observations

O 80: The SLA development process inputs and requirements were driven through the forum meetings with no formal process for vetting and collating requirements and there was a lack of performance metrics against which controls could be implemented. There is a general access obligation for dealing with operator requests in a fair, reasonable and timely manner. There are no controls governing SLA development that demonstrated eir's consideration of regulatory obligations.

O 81: The ten SLA versions examined took between 160 and 1,190 days to develop (an average of 516 days each). The average development time for LLU SLA versions was 411 days, SB-WLR was 819 days, NGA was 417 days and UG took 614 days. The time taken to develop a new version of an SLA raises concerns whether risks to its regulatory obligations were being managed.

O 82: SLA topics that could affect multiple SLA areas are discussed across different forums which can then make decisions on these topics. Currently, the same members tend to attend all the forums. However, there is a chance that over time, this may start diverging, and may lead to some members not being aware of these decisions.

O 83: The onus for the timeliness obligations lies with eir, but there was no evidence of adequate overall project management managing to a timeline, keeping tabs on tasks and responsibilities, and keeping stakeholders focussed on their tasks.

O 84: Waiting until after a trend for the performance of any SLA metric had been reliably achieved before developing and agreeing financial penalties significantly sped up the development of

SLAs, by removing a major point of contention, whilst ensuring fairness to all parties. However, time limits should be set to ensure that the penalties can take effect in a timely manner, since these are mandatory for completion of an SLA.

3. Regional Handover

[redacted]

Observations

O 85: [redacted]

O 86: [redacted]

4. Address Matching

[redacted]

Observations

O 87: [redacted]

O 88: [redacted]

[redacted]

5. Enhanced Provisioning Process

This was a product/ process initiative originating within eir which was designed to improve the process for changing customer appointments by open eir customer service agents, when a customer had missed an appointment. It required open eir personnel making direct contact with other operators' customers for rearranging appointments.

Observations

O 89: This product moved rapidly through specification and development stages. The overall elapsed time, from initiation to deployment, was 612 days of which 183 days was spent on developing a functional specification, 282 for the development of the product and the remainder for the formal notification period during which there were some Operator trials.

O 90: There was a lack of transparency regarding some decisions; there was no formal decision making criteria and poor documentation. A Statement of Compliance, which outlined eir's consideration of its regulatory obligations, was produced.

6. Bespoke Bid - Virtual Managed Service for an Operator

[redacted]

Observations

O 91: [redacted]

O 92: [redacted]

O 93: [redacted]

4.5.2. Product Development Chronological Analysis

Elapsed time is the main indicator of timeliness of product development. Elapsed times will vary depending on the complexity of the requested development. For instance, developments with complex IT elements in the solution can take longer than requests which only involve a process change.

Cartesian did not find controls being operated that mitigated risks to timeliness for any of the cases that were externally generated (requests from operators).

The elapsed times for all the product development cases are compared in the table below

Figure 7. Elapsed Days for Product Development Cases [58]

	Duct Access	SLA Development	Regional Handover	Address Matching	Enhanced Provisioning	Bespoke Bid
Total Elapsed Time (days)	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

It is Cartesian's view that the differences in the elapsed times of the product cases above were not explained by the complexity of the IT development work [redacted] However, there was a significant difference in the elapsed time, which was not fully explained by the IT development time.

One of the purposes of analysing product development timelines was to identify whether there was any risk of bias in the time taken to develop regulated products for eir's downstream businesses versus OAOs.

Cartesian reviewed all projects, from March 2012 to October 2016, that were listed in eir's Product Change Request Log and their technology product development tracking system[59]. Elapsed times were ascertained for every project through every development gate, from the preamble stage through to deployment. These were summarised by product category and by originating source. Comparisons were then done and subjected to tests for statistical significance.

Data was sourced from eir's IT project tracking system and spreadsheets used by the Regulated Access Products team to track product changes through from initial logging to final deployment. The final cleansed number of projects was 785.

Of the 785 final cleansed projects, 358 progressed through all development stages. These were used as the basis for our comparative analysis.

There were 35 projects identified as being directly requested by OAOs, and 227 projects being sourced from open eir, some of which could have benefited other operators as well. The remainder were from eir's other BUs, including its downstream businesses. Our analysis showed that the average duration of OAO projects reaching Deployment date was 655 days. This exceeded the average for Open eir by 178

[58] The elapsed times include the periods of notification to ComReg, prior to products being launched.
[59] Eir utilise a Portfolio and Programme Management (PPM) application, Planview.

days, and for eir Retail by 236 days. The sample sizes were large enough for these differences to be significant. The criteria for the analysis was based on the requester for the development only.

There was a significant difference in elapsed time, from an initial request being raised to it being logged as a valid request, between eir's BUs and those of the OAOs of 160 days. This appears to be the result of the different levels of engagement for the respective businesses. The interaction between downstream businesses and TED is informal and frequent, whereas the OAO interactions with TED are more structured, and operate more infrequently.

The following table highlights the differences in durations for each of the project phases and in total.

Table 2. Summary of Projects Duration (days) by Customer Category up to Deployment Date

Category	Overall		Open eir			eir Retail			Other eir			OAO		
Project Phase	Count	Avg.	Count	Avg.	Diff.	Count	Avg.	Diff.	Count	Avg.	Diff.	Count	Avg.	Diff.
Avg. Project Duration	358	488	*71*	*477*	*-2%*	*130*	*419*	*-14%*	*139*	*537*	*10%*	*18*	*655*	*34%*
Avg. Project Duration (excluding IRD)	358	477	*71*	*475*	*0%*	*130*	*417*	*-13%*	*139*	*529*	*11%*	*18*	*511*	*7%*

Note:

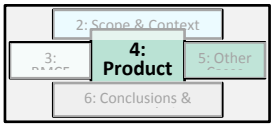
- IRD – Initial Requirements Definition.
- Count indicates the number of projects analysed for the same period, from March 2012 to October 2016, for all projects, then Open eir, eir Retail, Other eir and OAOs separately.
- Avg. indicates the mean number of days taken for the projects within that category.
- Diff. indicates the percentage difference in the number of days for that category group, compared to the average of all projects.
- The elapsed times include the requisite ComReg review period and Industry Notification periods.

An examination of the table above shows that OAO projects take 34% longer to complete compared to the overall average (all eir groups and OAOs), when the time taken for completing the initial requirements definitions is included. A direct comparison between OAO versus all eir projects (open eir, eir Retail and other eir projects) has a larger difference of 37%, and excluding IRD, 8% longer durations. The sample size for OAO projects while small, was still statistically significant.

4.6. Product Summary Conclusions

The end-to-end product development process consisted of a number of distinct parts, as outlined above. The first part can be referred to as the 'Request Preamble', which starts with the raising of an informal request by an operator, and ends with the registration of the request in the PCRL.

The second part, RAP Development, starts with the registration in the PCRL, and completes on commercial deployment.



C 15: In the Request Pre-amble, there are no formal processes, standards or performance metrics for dealing with Operator requests (including IT support or technical requests related to RAP), nor was evidence found of any controls over this phase, giving rise to a risk of discrimination.

C 16: The second part of the process which includes the end-to-end Technology Development process is well documented and has high process reliability. There are controls for monitoring risks.

C 17: The prioritisation process for both the Request Pre-amble and the RAP Development is opaque, resulting in a lack of confidence in its impartiality among key stakeholders.

C 18: There is a lack of documented assessment and decision making criteria covering prioritization of product development requests and a number of decision processes including initial RAP Assessment and BU Exception Management for the operation of controls.

C 19: There is a lack of evidence of decision making by senior management in open eir for the product development cases Cartesian reviewed. This, combined with the opacity of the prioritization process, made it impossible to determine with accuracy how key decisions were made. It is unclear the extent to which consideration was given to eir's regulatory obligations in its decision making.

C 20: There are wide differences in the elapsed times of the product cases that were analysed which are not explained by the complexity of the required development work. There are no controls on the timeliness of product development, even though there are timeliness obligations for a number of the product cases examined.

C 21: An analysis of product development requests since 2012 has indicated that OAO projects took significantly longer than eir downstream business products to progress both from initial request recording to deployment of products. While controls existed to monitor the RAP Development phase, none existed to monitor the Request Pre-amble period prior to that.

C 22: There is no formal process for the development of SLAs, nor is there a formal process for tracking the development of an SLA, such as gating processes, project plans, and milestones. There was no evidence of a control that would ensure that SLAs were developed in a timely manner.

C 23: It was noted that the responsibility for covering specific SLA topics migrated between forums. Hence, SLA principles and metrics may be discussed and agreed in multiple forums, leading to the potential for confusion and delays. This has been minimised by the fact that the forum participants are the same; but this may not always be true.

C 24: Operational Product Life-cycle processes were found to be mature and robust, as were the end-to-end technology development processes. These processes are essential for the day-to-day operation of the business.

C 25: The process for the Initial receipt of RAP proposals is well documented with a clear RACI matrix for each of the process steps. However, there is not a clear process owner.

C 26: There is an over-reliance on the forums to move OAO projects forward, on an issue-by-issue basis, in lieu of proper project management. This prolongs the time for the delivery of product and process improvements.

5. Other Cases

5.1. KPIs, Engagement Channels and Storm Mode Assessments

Cartesian was requested to assess KPIs, various channels through which operators and eir downstream BUs engaged with open eir, and Storm Mode in more detail.

eir has a regulatory obligation to produce KPI reports at regular intervals. They are an extension of some of the controls that have been implemented to ensure that all operators received non-discriminatory service and quality.

The functioning of forums, focusing on eir's management and handling of forum requests, and requests emanating from account management channels, was examined to understand how eir processed these requests, and how responses were provided. In many of these requests, eir had an obligation to ensure timeliness in handling requests, in addition to other Regulatory Obligations.

Storm mode is a status triggered by an increase above a threshold level of faults due to bad weather. The declaration of Storm Mode does not in itself result in the suspension of SLAs. However, this declaration, if the result of a Force majeure event, may result in the temporary suspension of SLAs and the triggering of the Storm Response Plan. Eir's current LLU and SB-WLR SLA facilitates the exclusion of a fault on an individual circuit from the payment of an SLA where that fault arises from or is otherwise caused or contributed to by a force majeure event (storms, flooding fire or lightning). Cartesian was asked to assess the processes, trigger point and operation of Storm Mode.

5.2. Key Performance Indicators Analysis

ComReg Decision D05/11 mandates that eir produce the KPIs in a 'true and accurate manner'. The purpose of the assessment was to determine whether there were risks to eir's ability to meet this regulatory obligation. Cartesian examined the processes used to design the tools and processes used for KPI generation, as well as the processes used in the generation of the metrics, for a subset of the Key Performance Indicators.

5.2.1. Scope

The processes supporting three KPI metrics were selected for analysis, covering the open eir and Downstream product equivalents:

- Wholesale SB-WLR / WLA versus eir Consumer PSTN; and,
- open eir Bitstream versus Consumer Broadband[60].

The stakeholders involved in the design, implementation, operation, and publication of KPIs for these product families were the same. Cartesian did not assess nor analyse the production metrics for accuracy, nor trace the total set of source records and how their eligibility in the final metrics were accounted for.

[60] Decision D05/11, Document 11/45, 'Response to Consultation and Decision on the Introduction of Key Performance Indicators for Regulated Markets', 29 June 2011, Appendix 2, Table 1 describes the scope of the products.

The analysis considered the KPIs reported in the Regulatory and Compliance Audit reports for May 2015, and March 2016.

These KPIs metrics covered the supply and repair of RAP services:

a. Service Connection time, where the service physical infrastructure was in place (electronic enablement of services[61]). The KPI consisted of the percentage of such orders being completed within 2 working days over a fixed period.

b. Service Connection time, where work requires new line install. The KPI consisted of the percentage of such orders being completed within 10 working days over a fixed period.

c. Service Connection Quality, calculated as the percentage of orders that did not have a fault reported within 28 days of the completion of the order.

d. Fault repair percentage completed within 2 working days. There is a control[62] that is specified to mitigate the risk of non-equivalent service, in addition to the KPI report.

e. Fault Repair Quality, calculated as the percentage of fault repairs that did not have another fault reported within 28 days of the completion of the last repair.

It was noted that an assessment of the KPI Fault Metrics Production Business Process Review[63] (referred to in this document as the KPI Fault Metrics Production Review) had been carried out by an external party in the June to July 2015 timeframe. Cartesian's assessment included some of the same processes for Fault Metrics to understand what improvements had been made. However, Cartesian did not include Line Share and ULMP/GLUMP products which were in the scope of the earlier review.

The processes examined by Cartesian covered the development of the KPIs, including its operation, reporting, management and assurance, as listed below.

a. KPI Tool and Process Design: Cartesian did not review this process in the KPI Fault Metrics Production Review. However, the tools and processes must be designed to ensure that KPI reports can be produced that meet the requirements of the ComReg Decisions. The processes should cover the analysis of the specifications and the design and implementation of the tools and procedures used to operate and manage the production of the reports. It should also include the design of, and definition of the standards for the operational use for the tool.

b. Transactional Data Generation: These are the processes such as service requests and fault reports that result in the data reported in the KPIs. This assessment is needed to understand how the transaction records that the KPI is designed to report on are generated, and provide a reference framework for understanding data variables and operational data that affect the KPIs. The process was analysed at a high level to develop an understanding of how the data originated.

[61] Electronic enablement is defined in Annex 1, Pages 28 and 35, of ComReg Decision D05/11, Document 11/45, 'Response to Consultation and Decision on the Introduction of Key Performance Indicators for Regulated Markets', 29 June 2011.
[62] NGNE_CRM_019
[63] eircom KPI Fault Metrics Production – Business Process Review, June/July 2015, prepared by IBM.

c. Reference Data Management: This includes processes and stakeholders involved in managing and authorising any changes to the parameters and variables (reference data, e.g., fault codes, close codes, product codes and time periods) that control the selection and filtration of the data used in the KPIs. This assessment was done to understand how decisions are made in the definition of these parameters / variables and the impact assessments that are done to understand their effects on the KPIs, prior to and after changes are made. It includes processes defined in the KPI Fault Metrics Production Review such as:

   - Refresh
   - KPI Fault Data Process

d. Report Generation and Production: These programs extract data from the production systems, or from data warehouses, such as eir's CDW system. Cartesian examined how raw data records are extracted, then cleansed and transformed, to be loaded into the data sets used to generate the reports. This process area was not included in the KPI Fault Metrics Production Review.

   A set of programs and processes produce the KPIs, and generate, distribute and archive the reports. The KPI Fault Metrics Production Review-defined processes include;

   - Generate KPI Repair Report Process
   - Generate SB-WLR Repair Clock Hours KPI Report Process

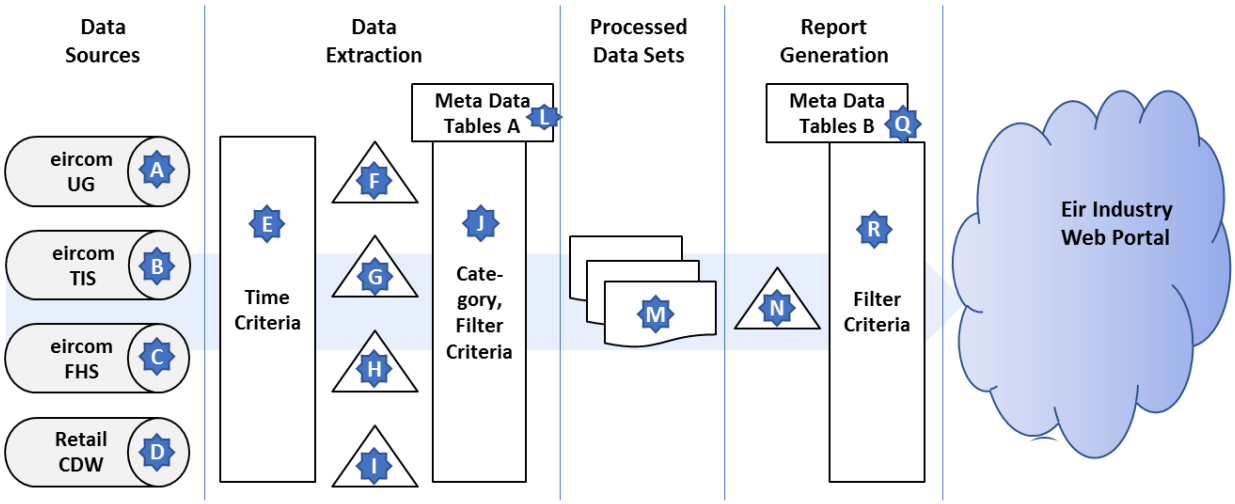
e. Quality Assurance: The processes assess the quality of the reports, manage changes to them and assure their accuracy and dissemination. This is carried out by the management in the departments that own the KPI reporting processes. Cartesian has included Quality Management in each of the sections above, as this is also carried out by the teams who own or operate those processes.

Cartesian examined the degree to which independent processes and teams are used to assure reporting accuracy, timeliness and quality, as well as to assure compliance to the KPI Requirements from the Decision Instruments.

For each of the process areas listed above, separate assessments were done for Service Connection Time and Quality and for Fault Repair Time and Quality. The figure below shows the overall view of the processes used to generate and publish the KPI reports[64].

[64] KPI reports here refers generically to all the periodic reports specified in ComReg Decision D05/11, Document 11/45, 'Response to Consultation and Decision on the Introduction of Key Performance Indicators for Regulated Markets', 29 June 2011.

Figure 8. KPI Operational Processes



Note: The labels above will be used as references in the observations.

A brief examination of the fault management processes was made. These processes generate the data records the KPIs are designed to measure, namely the Fault Records. This examination provided the context for how these records were produced, and how they were selected.

5.2.2. KPI Processes

The assessment does not include examination or validation of the computer programs and associated algorithms used in any of the programs required to generate the KPI metrics.

Two sets of programs are used to generate the KPIs for the Service Connection Time and Quality, and the Repair Time and Quality metrics.

The first set of programs (Items F to I in Figure 8 above) extract information from the computer systems which generate provisioning, and fault repair (Systems A to D) records. These programs extract information for the correct time periods, and apply filtration rules to categorize the data into different data sets, based on product classes. Separate programs are used for different products, and for fault versus service connection metrics.

The second set of programs (marked by Item N in Figure 8 above) utilise the collated data from the first set of programs and generate the metric reports. Other programs are used to generate similar reports for other products. These were not examined.

5.2.3. Observations

Please note that item letters below refer to Figure 8 above.

The first set of programs extract information from the computer systems where the KPI data has been generated during operational work, whether provisioning, or fault repair (Systems A to D). One

exception is the eir consumer CDW computer data warehouse, which holds Retail information that is extracted from other operational systems.

A set of criteria are used to select the data for the time period to be reported on (Time Criteria E).

O 94: Programs F – I which extract data from the source systems A – D (see Figure 8), are not well-documented. There are no formal test plans for these programs. The current operators and owners are not aware whether they had been tested to ensure that the programs extracted the correct set of data for the KPIs. There is no independent assurance for these programs, and no specifications or test plans which can be used as a basis for assurance reviews.

O 95: The selection of the records for the given time interval to be reported works as planned[65].

O 96: The report generation programs, N, are well documented for the in-scope products. However, there are no design specifications, test specifications and plans that are known to the owners and operators. There have been no assurance reviews of these programs known to the program owners and operators.

The following findings refer to programs F to I.

O 97: Reference Data are not consistently managed across all the programs.

O 98: The processes that were reviewed are well-documented documented by the operator or owner of the process. These were maintained to a high standard.

The findings below refer to programs N.

O 99: There is a procedure manual which explains the use of the reference data. The reference data is complete, based on the sample inspected.

O 100: One sample of a SQL code description was provided. The code can be used in debugging. However, it cannot replace proper documentation of the functional specification of the code, or be used to design test scripts, as it does not contain working parameters, input nor output specifications.

O 101: Some of the files provided were not dated, nor contained an owner name or department, version number, or valid dates for the data. However, we determined from interviews, that there were owners for some of the files, but these were not always documented.

O 102: There is a centrally-managed process to ensure that all the reference data required to run the programs is available and consistent, for the products examined. However, the complexity and number of separate tables that need to be synchronised increases the risk of inaccuracy. The other product KPIs were not examined, and there is a possibility that other processes and tables are needed to manage all the KPIs.

The observations below refer to Fault Repair.

O 103: There is no process or system for reconciling the total number of transaction records received from Service Request or Fault Management systems. The number of records that are

[65] Based on a process review; no quantitative analysis done of the reference data set.

excluded from the KPI calculations and the reasons why, (filter rules) are not tracked and accounted for.

O 104: The teams and individuals who run the programs do not carry out any detailed checks on the correctness of their processes, or on the outputs generated. No verification is made that all data that should have been included in the KPI metrics was actually used in the calculations.

O 105: The Programs and processes (item N in the figure) specifically for SB-WLR, LLU and WLA KPIs, are supported by a KPI Reporting Process manual. This manual is version-controlled and dated. It contains information about the overall process, as well as detailed step-by-step instructions for operating the programs.

O 106: The programs or scripts used for the generation of Service KPIs require many manual steps to execute correctly. There are many external reference values that must be selected individually and many steps that need to be run separately. While this is much improved compared to manipulation of Excel files, it is still prone to error.

O 107: The monthly operations used to generate the Service provisioning quality data does not include any quality checks nor assurance beyond visual inspection. There are no accounting checks to confirm any fall-out of the source records used in the KPI metrics.

5.2.4. KPI Analysis Conclusions

C 27: The programs developed for the in-scope products do not have any test plans or specifications. They have not been independently assessed to verify that they perform as required to generate results per the Decision requirements.

C 28: There is no accounting for the handling of the source data records for any of the KPIs; hence there is no verification mechanism to ensure that all valid records are being included in the KPI reports.

C 29: The overall processing environment is still highly manual and relatively complicated, with only one set of programs that are well-documented. There are different processes and sets of programs required for the different KPI metric sets. These increase the chance for errors. The lack of formal results validation increases the probability that errors, if made, would not be discovered.

C 30: The quarterly KPI reports are reviewed by C&E. However, this review examines the KPI metrics reported, but does not verify the accuracy of the report generation process itself. No formal checks are made to confirm that the results produced are correct, and that all valid records were included in the calculations.

5.3. Storm Mode Analysis

Storm Mode is declared once there is an abnormal increase in the level of faults, such as that due to unseasonably bad weather. An abnormal increase in faults is defined as when carry-over faults for a day are twice the normal level for that time of year and where normality cannot be restored within one week.

Once Storm Mode is declared by the Director of Fixed Access Operations, a Storm Response Plan is activated under the direction of the Head of Fixed Access Service. This plan is developed on a regional basis and involves the tiered use of additional resources as follows:

a. Extended hours from business as usual repair teams

b. National Response Team to deal with local pressure points

c. National Build team for larger remediation work

d. Additional numbers of apprentices

e. External contract resources, (which may be re-allocated from provisioning teams)

The target is to return to normal fault rates within one month and there is daily communication with stakeholders.

5.3.1. Scope

The scope of this review was to assess the process used in declaring Storm Mode, eir's operations under that mode, and exit. Storm mode is a status triggered by an increase above a threshold level of faults due to bad weather. This declaration, if the result of a Force Majeure event, may result in the temporary suspension of SLAs and the triggering of the Storm Response Plan. Eir's current LLU and SB-WLR SLA facilitates the exclusion of a fault on an individual circuit from the payment of an SLA where that fault arises from or is otherwise caused or contributed to by a force majeure event (storms, flooding fire or lightning).

The review was done through interviews and assessing the documentation provided by eir. This included:

- Records of decisions to invoke Storm Mode and the criteria used;
- Daily operational decisions on resourcing and prioritisation under the mode; and lastly,
- The return to business as usual operating practices.

5.3.2. Observations

O 108: The Storm Mode process is well-documented, with clear ownership and defined roles and responsibilities. The documentation is under change control and is current. The process is managed with defined tolerances and escalation paths.

O 109: The key decision maker is the Director of Fixed Access Operations, supported by the Storm Response Group which has a defined mandate, as outlined in the process documentation.

O 110: There are clear decision criteria for declaring and maintaining Storm Mode. The declaration of Storm Mode, in the case examined, was triggered by a storm. Once storm mode was declared, it remained in operation until the level of faults declined to within the quantitative normal working parameters for Fixed Access operations. The duration of Storm Mode was not based on the period of storm conditions. The length of this period is influenced by the severity of the storm, the nature and extent of the faults, and the overall state of the network plant.

O 111: Cartesian noted that ComReg Decision 17/08[66] included that eir should put in place a comprehensive set of terms and conditions governing the circumstances and the process by which faults are excluded from the payment of Service Credits (SC) due to force majeure. We note that this determination is under appeal.

O 112: There is adequate supporting documentation[67], last updated on 04/01/2016

5.3.3. Storm Mode Analysis Conclusions

C 31: The processes associated with Storm Mode are sufficiently well documented to allow risks to be assessed and controls to be applied in a consistent manner. Operational teams deal with faults based on the severity of impact on network elements, which are not linked to any particular operator. No risks have been identified, nor are there any controls for Storm mode processes.

5.4. Engagement Channels

The purpose of this review is to establish if a formal, structured process existed for dealing with actions that arise out of the various engagement channels, including industry fora and account management channels, in the context of eir's regulatory obligations. These account management channels include those for operators and eir's downstream businesses. Engagements, and tasks arising out of the various industry channels can cover a wide range of issues including the development of SLAs, product development requests, requests for technical / operational information, and other day-to-day operational issues. The specific focus of this section is to review the process within eir for dealing with actions which originate from the various channels.

As stated, above, in the product development preamble section, there are a number of stakeholders, internal and external to eir, involved in these channels which operate with varying modes/degrees of interaction and formality. Because of the variety of channels and modes of interaction, it is particularly important to have a robust and transparent process in order to minimise the risk of non-discrimination by open eir in the treatment of requests from all participants. Risk of discrimination in this context can relate to timing of developments, sharing of information, richness and quality of engagement as between the various channels.

The work stream examined the process for the capture and management of requests (Requests for Information, clarifications, new product / product change, and other changes) made by all operators, to open eir for resolution or follow-up. The purpose was to understand the following and to assess whether effective regulatory governance could be applied:

a. How these requests are tracked and processed within open eir,

b. Decision points and criteria used to assess these requests,

c. Stakeholders involved in the process of managing forum requests and actions

d. Other mechanisms that could be or are used either by downstream eir operators, or other operators, and how these may differ.

[66] ComReg Document number 17/08, Final Determination in a Dispute between (i) BT Communications Ireland Ltd., Magnet Network Limited, Sky Ireland Ltd., and Vodafone Ireland Ltd. and (ii) Eircom Ltd.
[67] Eir document, 'Storm Response Plan V2.0, 26/10/2016 & open eir Network Infrastructure', issued on 04/01/2016.

5.4.1. Scope

The purpose of this review was to establish if a formal process existed within eir for dealing with actions and requests that arise out of the various engagement channels, including industry forums. The working of various forums was reviewed as part of the work-stream analysis dealing with the development of SLAs and the respective product development case analyses. The focus of this section is to review the processes within eir for dealing with actions arising from the various engagement channels.

Cartesian has used its process assessment method to review the process under the headings of Process Quality, and Process Capability.

a. Documentation gathering, all sources, analysis (sources, validation carried out, versioning, stakeholders)

b. Process analysis – types of processes, e.g., new and change product requests, requests for information, etc.

c. Quality and Assurance processes – types of KPIs, SLAs, and any other metrics used for the assurance over the forum processes and documentation.

d. Findings and Recommendations – Completeness of request types coverage in interactions between eir and all operators (based on forum objectives and goals), quality of the interaction, completeness of documentation, and recommendations thereof.

5.4.2. Observations

O 113: There is no formal process, standard documentation or performance metrics. Each eir manager deals with their respective actions in a manner deemed most appropriate by them.

O 114: Decisions are made by each product manager and there is a weekly review of the actions arising out of the various forums with regulatory operations. There is no consolidated log of actions or coordinated management of actions. There is no assurance process to report on the rate at which actions are dealt with.

O 115: Actions can arise in one industry forum and get transferred to another and delays can occur for several legitimate reasons. Operators, as well as eir, expressed frustration to Cartesian about the length of time eir takes to deal with actions.

O 116: Operators have observed that when an action arises in the context of a clearly defined open eir project plan, they are dealt with in a reasonable timeframe. However, when actions arise as general issues, timelines are extended, causing operator frustration.

5.4.3. Engagement Channels Conclusions

C 32: There is no formal process, standard documentation, nor performance metrics. There is a high degree of variability in elapsed times. There is a high risk that requests/actions from different channels (industry forums, account management, eir downstream businesses) may be treated differently. Cartesian has not identified a control to deal with this.

C 33: There is no consolidated list of actions with owners and formal status monitoring. Cartesian did not identify controls relating to the timeliness of responses to actions arising from the various industry forums and other industry channels.

6. Overall Conclusions and Recommendations

The Summary Report Conclusions below have been repeated from the Executive Summary Conclusions for the reader's convenience. The Summary Report Recommendations contain more detail than in the Executive Summary Recommendations.

6.1. Summary Report Conclusions

Cartesian reviewed the operational, risk management control and assurance processes to establish if they were sufficiently mature, robust and reliable to enable regulatory risks to be identified and controls to be applied and maintained in a consistent manner. Controls and the RMCF processes were examined to assess whether risk mitigation was effective. These processes are key elements in the overall Regulatory Governance Model, which eir uses as the basis for assuring compliance with their regulatory obligations. Past development cases were examined to understand whether eir was at risk of not being in compliance with its Regulatory Obligations.

Our review findings highlighted significant deficiencies in the Risk Management and Control Framework. Examination of the RMCF supporting the operation, management and assurance of the RACM revealed significant flaws that call into question their overall effectiveness. The RMCF does not reliably mitigate risks, due to the inconsistent operation of controls. This is compounded by poor evidence maintenance, infrequent assurance, and a lack of trending and escalation mechanisms for dealing with defects in controls.

The product case analyses and product development chronology analyses have further highlighted process deficiencies and differences in elapsed time between products being developed for eir's downstream businesses and those of other operators.

The conclusions drawn from the assessment of how the KPIs were developed and operated raises concerns about the accuracy of the KPI reporting.

The responsibilities of C&E and IA were unclear regarding the ownership of operational tasks and accountabilities for regulatory governance assurance.

In the context of these findings, it is Cartesian's view that the Regulatory Governance Model is not sufficiently robust and reliable to enable regulatory risks to be assessed and controls to be applied in a reliable and consistent manner.

6.2. Summary Report Recommendations

<u>General</u>

R 1. Operationalise the Code of Practice

The principles of the Code of Practice should be translated into Methods and Procedures for respective BU processes, thus helping to avoid misinterpretation or oversight. Undocumented processes should be documented, and the rules ensuring compliance with the code of practice should then be embedded in the process steps.

R 2. Develop Process Standards, Risk and Escalation Criteria, and Exception Tolerances

Process management standards, including process tolerances and escalations should be developed and maintained. These should include the frequencies with which some of the assurance processes are executed. Standards should include the following items:

a. Checklists of risk areas and risk types (more detailed than just Product Lifecycle, including, but not only information security, timeliness, exception management, etc.) and assessment points for risk identification;

b. Quantitative assessment standards for risk impact, likelihood and timeframes on impartiality;

c. Standards for acceptable risk mitigation, based on (b), and escalations;

d. Escalation criteria by type of escalation, such as, but not limited to, control defects in control operations and control operation results, product development and control implementation changes and delays;

e. Standards for control retirement and merges;

f. Operations acceptance criteria for new controls (equivalent to Operational Readiness tests in software development);

g. Control operations acceptance (approval standards for the periodic operations of the controls);

h. Self-Certification standards for accountability and responsibility, reporting and assessment of the functioning of controls need to be established at a corporate level to ensure consistency across the RACM in different BUs;

i. Process documentation and maintenance standards.

R 3. Maintain records to provide evidence needed to demonstrate that Regulatory Obligations have been met

The rules relating to the retention of evidence should be documented and the evidence retained.

R 4. The roles for Regulatory Operational, and Assurance functions should be clarified

The roles of IA, C&E and Regulatory Operations need to be clarified. The resourcing of the functions should be sufficient to enable it to undertake its duties reliably and consistently in accordance with predetermined schedules. The schedules for reviews should ensure that a comprehensive review of each control is done annually, at a minimum.

R 5. Implement Independent program management oversight over critical processes and outputs

Because of the nature and extent of the deficiencies in the operational governance of RAP development and RMCF, Cartesian believes there should be robust, independent oversight of the operation of all regulatory matters covered by the recommendations below, and in this report. The provision of oversight will require support of an independent, adequately resourced, proactive assurance function, incorporating a programme management capability.

R 6. Implement project management for RAP development, to ensure eir's Regulatory Obligations are met

Eir should implement project management with clear plans, action items and responsibilities across all stakeholders (including OAOs), where the onus lies with eir to ensure that timeliness and other obligations are met. Eir currently has project management for aspects of such developments, but a full, end-to-end project plan and management covering all stakeholders, was found to be lacking. These projects should fall under the programme management recommendation in R 4. To avoid doubt, a clear escalation path to programme management should be defined for risks and issues outside of eir's control.

Such a capability will also enable more precise records to be maintained about project status, gating, decisions made and progress.

RMCF

R 7. Document RMCF Processes and standardise BU RMCF operations

Detailed documentation should be developed for the risk management processes, based on eir's regulatory obligations. These should have well-defined criteria for evaluating and assigning impact, likelihood and risk exposure timing.

R 8. Ensure that controls mitigate risks adequately

A formal, independent validation of controls should be implemented periodically to ensure that risks are mitigated adequately. The validation should be based on documented standards for risk assessment.

R 9. Implement a fit-for-purpose Risk and Controls Management tool

The information stored and managed using the current RACM documents is inadequate. A fit-for-purpose tool would track, manage and report risk and control milestones, (e.g., planned / actual implementation dates and software development tracked in eir's PPM tool, Planview should be incorporated), and review dates and outcomes (Self Certification, and assurance reviews). It would also enforce data quality rules, such as mandatory fields and data validation. These requirements imply a capability to track the full history of the lifecycle of risks and their controls.

R 10. Standardise Control and Control Operations Evidence Management and Storage

A company-wide standardised repository should be created for control operations evidence and the output / results of control operations such as KPIs.

R 11. Design controls for simplified and comprehensive management

Controls should be designed to simplify evaluations and improve assurance. Reporting of control operations and outputs should be standardised to simplify tracking of control operation, and assurance reviews.

R 12. Trend control results

A process for trending of control evidence to identify consistently failing controls should be developed. Standardisation and oversight into the BU, and coordination between IA and C&E should be implemented.

R 13. Implement an escalation mechanism

An escalation process should be implemented to enable follow-up on defective controls. This process should be well-documented, with clear stakeholder roles and evidence.

R 14. Rank risks based on likelihood, impact and timeframes

Every risk should be evaluated in terms of the likelihood, impact and timeframes so that the most important mitigations can be prioritized.

R 15. Assess aggregate risks in RAP processes, BUs and RAP markets

Different groupings of risks should be analysed to understand the total risk impact against that area. Three major areas should be evaluated for aggregate risk exposure on this basis:

- Product Lifecycle Processes – pre-ordering / ordering, provisioning, service assurance and change;
- Business Units – Open eir (Wholesale and Networks), Consumer, eir Business Solutions;
- RAP by product category - While assessments are currently done according to the first two groupings, the aggregate risks are not appraised and quantified.

Product Development

R 16. Develop a transparent process for handling operator requests

A process should be created to manage operator requests that will avoid protracted development delays, as identified in several of the product cases reviewed. This process should include clear and objective standards, well-defined stakeholders and roles, including technical support [68], and well-defined milestone points and entry criteria. There should be strong independent oversight of the management of product development (including pre-amble), which is required to ensure transparency and fairness to all operators, including eir.

R 17. Increase visibility of the RAP prioritisation process

A RAP prioritisation process that includes detailed documentation, clear assessment and decision criteria with decision milestones, should be developed.

R 18. Provide an evidence trail

Evidence for every RAP request should be maintained to prove that eir's regulatory obligations had been considered. To ensure consistency, a checklist of compliance points should be signed and maintained for independent review.

R 19. Strengthen Life-Cycle process ownership

Clear process ownership with regular reviews should be established for each of the product life-cycle process steps.

[68] Immediate access to technical resources that will allow OAOs to fully scope their requests in a timely manner.

KPIs

R 20. Maintain visibility of all KPI-reported transaction records

An accounting audit trail for the processing of all the transaction records for KPI reporting, should be maintained so there is a clear understanding of what records were excluded from the KPI reports, and for what reason.

R 21. Independent appraisal of processes and tools

The processes and tools used for generating KPIs for fulfilment and fault management should be independently assessed periodically.

R 22. Implement periodic sample testing

KPI metrics testing should be carried out periodically. An independent audit using small samples of data records should be done to validate that the entire process results in accurate reporting of the KPIs.

R 23. Develop KPI program specifications for systems development and testing

KPI program specifications and test plans should be developed and implemented.

Engagement Channels

R 24. Reduce dependency on forums to progress projects

Forums should only be used to present status, schedule discussions for topics, and prioritise activities. ComReg's role should be to facilitate the meetings, and provide advice and clarification regarding Regulatory Obligations.

The current industry engagement model should be reviewed to streamline the operation of the various forums, including account management for industry and eir. Project management and standards, applicable to all industry and eir, should be introduced.

An independent operational role should be established for creating and maintaining standards and coverage of topics

R 25. Ensure clarity in the responsibilities and scope of every forum

The scope for each forum should be defined in more detail to prevent overlap of topics covered, especially for SLA development. This will reduce uncertainty about which forums are responsible for a given topic. For example, a clear delineation of common SLA criteria, that apply to all products, versus product-specific ones would be beneficial.

.

7. References

7.1. Project Lexicon

Acronym	Definition
(Project) Gating	This is similar to Project Stage. These is a progress point in a project where a formal review is conducted by the project sponsors, to determine whether a project should be allowed to continue, require changes, or be cancelled.
(Project) Milestone	This is a reporting and / or decision point in a project, but generally not as formal as a gate or stage.
(Risk) Impact	This is similar with Severity. Should the risk materialise, it denotes the severity that the issue causes to the project or process.
(Risk) Timeframe	This is the expected timeframe when the risk is most likely to occur.
AF	Assured Forwarding. This is a service feature.
AN	Access Node
Aspirational Control	This implies that the risk has not yet been mitigated, but that mitigations could be in any stage from discussion of mitigation options, to awaiting the implementation of a mitigation solution.
Assurance Processes	These are processes used by an independent party (not under the influence or control within the line of management for the party responsible, or accountable for the task being assured), to assure that the process functions to serve the outcome, and that all applicable standards and being met by the Business Operational processes
BAR	Business Access Review. This is a review of the accessibility to either structured or unstructured by different groups
BCS	Bitstream Connection Service
BE	Best Effort
BECS	Bitstream Ethernet Connection Service
BEREC	Body of European Regulators for Electronic Communications
BP	Bitstream Plus
BTV	Broadcast Television
BU	BU
Business Management / Risk Management Processes	These processes are owned and operated by management teams over the Business Operational processes. These processes identify risks, develop, implement and operate the required mitigations and report on their efficacy and status. They incorporate metrics, standards and tolerances to ensure business operational processes are operating acceptably. They provide corrective actions to bring operational processes back within tolerance when needed

Acronym	Definition
Business Operational Processes	Product lifecycle processes such as order, service fulfilment, fault handling etc. It also includes product development processes. These processes are a collection of related, structured activities or tasks that produce a specific service or product. They are executed by operational teams responsible for carrying out these processes, such as operating product-customer lifecycles, including product development, covering both standard operational and exception processes.
C&E	Compliance and Equivalence
Cartesian Process Capability Score	A score derived from the methodology used by Cartesian for assessing Processes
Cartesian Process Quality Score	A score derived from the methodology used by Cartesian for assessing Processes
CBYD	Click Before You Dig
CEI	Civil Engineering Infrastructure
CGA	Current Generation Access
CMMI	Capability Maturity Model Integration. An appraisal system for process maturity and capability for different types of processes.
Control Executor	The person responsible for carrying out the control procedure and is a named individual in the RACM
Control Owner	The person accountable for the control operations and risk management and is a named individual in the RACM
CoP	Code of Practice. This deal with the eir's Access and Non-discrimination obligations. Regulatory Compliance and Audit Report, May 2015 (Redacted), pages 1, 20.
CoS	Class of Service
CoW	Clerk of Works. Agent from Eircom who accompanies OAOs when visiting Eircom installations
CPE	Customer Premises Equipment
CSID	Calling Station ID
Desktop Walk-Through	A process used by Internal Audit for the inspection of controls, their operations and results
EF	Expedited Forwarding
EOI	Equivalence of Inputs
EOO	Equivalence of Outputs
ERG	European Regulators Group for electronic communications networks. The group was the EU's primary forum for exchange of best practices, benchmarking, knowledge management, education and in-depth and forward-looking discussions on current and future regulatory challenges in communications. (See BEREC)

Acronym	Definition
Exception, Exception Process	Exceptions are events in a process that are unexpected or abnormal. An exception can only be defined when tolerances for that process are first defined. An example of a tolerance setting would be the maximum time taken to complete the process under normal circumstances (e.g., all the process inputs are also defined, and they must fall within given ranges defined as 'Normal'). A request to complete this faster than the defined interval then becomes an exception. Such a request would require a re-prioritisation of process work and rescheduling. An implication of a capable process is that it is adequately staffed, or if automated, the system has sufficient capacity to handle the changes in process volume that could occur from day to day.
FACA	Fixed Access call Origination (Market 2)
FTTC	Fibre to the Cabinet
FTTH	Fibre to the Home
GLUMP	Geographic Local Unbundled Metallic Path
GPON	Gigabit-capable Passive Optical Network
GT Dashboards	Computer system for viewing Outage notifications, major faults.
HIA Summary Reports	These are reports prepared by eir Internal Audit on a 6-monthly basis, and are provided as an appendix to the C&E Regulatory and Compliance and Audit Report.
IA	Internal Audit
IGMP	Internet Group Management Protocol
Industry	Refers to wholesale customers of open eir, other than eir downstream (Government and Enterprise, Retail)
IPM	Industry Process Manual. These are documentation manuals designed to be used by eir Downstream and other eir wholesale customers. These process documents are shared with OAOs to describe the working of the RAP products
ISO9001	This is a standard issued by the International Organization for Standardization, and specifies requirements for a quality management system
ITT	Invitation to Tender. In this report, it refers specifically to ComReg's ITT for Review of Eir's Regulatory Governance Model – Operations, issued in final version on 4/3/2016.
KPI	Key Performance Indicator. In this report, it specifically refers to the set of requirements documented in Decision D05/11, Document 11/45, 'Response to Consultation and Decision on the Introduction of Key Performance Indicators for Regulated Markets', 29 June 2011
L1	The L1 signifies the 'Level 1' manager for the department, thus the senior-most member of the department.
L2	This refers to the managers who report directly to the L1.

Acronym	Definition
LLU	Local Loop Unbundled
LWI	Local Works Instruction. A low-level procedure that explains exactly how to perform a task.
MIP	Major Infrastructure Projects. Eir considers a major infrastructure programme to be one that contemplates roll-out in at least 10 exchange areas with the intention to pass at least 10,000 premises with a broadband capable service
Mitigation	Resolution of a risk.
MoA	Colloquialism – 'Mother of all Risks', otherwise known as the Risk and Control Matrix (RACM). However, there is a difference in usage within eir. The MoA refers to the filename given to a specific set of Excel spreadsheets maintained by IA. A new copy of the spreadsheet is created generally after a Self-Certification cycle review is completed, with updates to the controls and their status. Therefore, every MoA version is a historical snapshot of the controls and their status. These 'MoA' files have a standard filename, in the format of 'MOAvx.x.xlsx', where x.x is the major and minor version number. The first file was MOAv0.2.xls, dated 25/9/2014 and the last version reviewed in this project was MOAv2.9.xls, dated 16/6/2016. There were 13 files in all within this range.
MPLS	Multi-Protocol Label Switching
M-VPN	Multicast – Virtual Private Network
NGA	Next generation Access
NGA/NGN	Next Generation Access/Next Generation Network
NGA-AN	Next Generation Access
NGA-AN	Next Generation Access – Access Node
NGN	Next Generation Network
Non-Discrimination	Regulatory Obligation
NPD	New Product Development
NTP	Network Termination Point
NTU	Network Terminating Unit
NVP	
OAO	Other Authorized Operators
OLT	Optical Line Terminal
ONT	Optical Network Terminal
Operator	This is equivalent to OAOs, and is used interchangeably.
OpsSite	Computer system for viewing network performance information
OSS/BSS	Operations Support Systems/Business Support Systems
PB	POTS Based

Acronym	Definition
PCRL	Product Change Request Log
PDC	Product Development Council
PIA	Physical Infrastructure Access
PoH	Point of Handover
PON	Passive Optical network
POTS	Plain Old Telephone Service
Progressor	Wholesale billing engine
PUN	Provide ULMP new
QMS	Quality Management System
QoS	Quality of Service
RACI	RACI' stands for Responsible, Accountable, Consulted and Informed, and is a methodology used to document the roles of staff involved in a process.
RACM	Risk and Control Matrix, also referred to as the MoA
RAP	Regulated Access Product
Reference Data	In the case of KPIs, these are data parameters that are used as criteria for the selection of records for inclusion in a report, or for categorisation of such data records into reporting categories.
Regulatory Compliance and Audit Reports	These are reports published by eir Compliance and Audit internally, and in different redacted versions, for ComReg and the Industry. They are issued on a 6-monthly basis.
Regulatory Obligation	These are the various regulatory obligations specified in various ComReg Decision instruments.
RG	Residential Gateway
RGM	Regulatory Governance Model
RMCF	Risk Management and Control Framework. The framework was developed by eir as a set of processes and tools to assure eir's compliance with its regulatory obligations, supporting the Business Process Compliance Review Compliance review and the Independent Regulatory Compliance and Audit reporting which form two of the three main strands of the RGM.
RMF	Risk Management Framework
RNA	Regulated NGA Access Group
RRT	Rod, Rope and Test
SA	Standalone
SAB	Service Access Bandwidth
SAM	System for Access Management)
Sarbanes-Oxley	US standard for Accountancy, containing useful guidelines for principles for separation of duties, and transparency of process steps
SB-WLR	Single Billing - Wholesale Line Rental

Acronym	Definition
Self-Certification	A process conducted by Internal Audit every three months to ensure that the controls are operated and the results, including any exceptions are reported and dealt with as needed to meet regulatory obligations. This is a key element of the Wholesale Reform Programme.
SLA	Service Level Agreement
SLU	Sub-loop unbundling
SoC	Statement of Compliance. This is a letter issued by the L1 that states that a RAP is in compliance with its regulatory obligations specified in any applicable ComReg Decision Notices.
SOD	Segregation of Duties
SORTS	Computer system for provisioning, accessible by technicians
Springboard	Programme to bring in a new billing engine
STB	Set-top Box
TED	Technology Evolution Design
Tolerances	These are the specified limits of a process, beyond which a process is considered to have met an exception condition. Tolerances can be specified for durations in which a process should complete by, the range of inputs which is can handle normally, and the quality range of its outputs.
UG	Unified Gateway
ULMP	Unbundled Local Metallic Path
VAS	Value Added Service
VDSL	Very high bit-rate Digital Subscriber Line
VLAN	Virtual Local Area Network
VLL	Virtual Leased Line
VOD	Video on Demand
VoIP	Voice over Internet Protocol
VPLS	Virtual Private LAN Service
VUA	Virtual Unbundled Access
WBA	Wholesale Broadband Access
WEIL	Wholesale Ethernet Interconnect Link
Wholesale Reforms Committee	This committee was established to oversee the Wholesale Reform Programme
WLA	White Label Voice Access - rebranded POTs
WPNIA	Wholesale Physical Network Infrastructure Access (Old Market 4, new 3a.)

7.2. Observations, Conclusions and Recommendations Links

Work Stream	Observation No.	Description	Theme	Conclusion No.	Recommendation No.
Initial Risk Assessment	O 1	Inadequate documentation and lack of independent assurance	Inadequate documentation, No independent assurance	C 1	R 4
Initial Risk Assessment	O 2	No documented assessment criteria	No documented assessment criteria	C 2	R 1
Initial Risk Assessment	O 3	Inadequate separation of duties for C&E	Inadequate separation of duties	C 12	R 1
Initial Risk Assessment	O 4	No quantification of risk likelihood	No quantification of risk likelihood or impact	C 2	R 13
Initial Risk Assessment	O 5	No definition H, M, L in risk likelihood	No quantification of risk likelihood or impact	C 2	R 13
Design of Controls	O 6	Control did not mitigate risk	Controls did not mitigate risk	C 4	R 8
Design of Controls	O 7	Inadequate documentation and lack of independent assurance	Inadequate documentation, No independent assurance	C 1	R 4
Design of Controls	O 8	No documented assessment criteria	No documented assessment criteria	C 4	R 1
Design of Controls	O 9	Inadequate separation of duties for C&E	inadequate separation of duties	C 12	R 1
Risk Closure and Retirement	O 10	No common process guidelines, or standards for control retirement	No common process guidelines, standards or tolerances	C 1	R 1
Risk Closure and Retirement	O 11	No common process guidelines, or standards for control retirement	No common process guidelines, or standards for control retirement	C 1, C 6	R 10, R 11, R 18
Risk Closure and Retirement	O 12	Low risk due to retirement and merging of controls	N/A	NA	N/A

Work Stream	Observation No.	Description	Theme	Conclusion No.	Recommendation No.
RACM Control Execution	O 13	No common process guidelines, standards or tolerances	No corporate wide standards	C 1	R 1
RACM Control Execution	O 14	High defect rates	Inconsistent operation of controls	C 3, C 5	R 1
RACM Assurance Process	O 15	Control cycles are too infrequent	Infrequent control cycles	C 10	R 4
RACM Assurance Process	O 16	No evidence of consistent follow up	Ineffective assurance process, Poor evidence retention	C 8, C 3	R 3
RACM Assurance Process	O 17	Tool for RACM is cumbersome and limited	Inadequate tools for control management	C 8	R 7
RACM Assurance Process	O 18	No status tracking of controls in the RACM	No trending of control effectiveness	C 7	R 11
RACM Assurance Process	O 19	Insufficient evidence retention in the RACM	Poor evidence retention	C 6	R 9
RACM Assurance Process	O 20	High defect rates	Inconsistent operation of controls	C 3, C 5	R 1
Statement of Compliance	O 21	Small number of people - sustainability issue	Small number of people - sustainability issue	C 14	R 4
Statement of Compliance	O 22	No documented process	Inadequate documentation	C 1	R 1
Statement of Compliance	O 23	No role for coordination of sign-offs when multiple SoCs are required		C 1	R 1, R 7
Statement of Compliance	O 24	No independent assurance.	No independent assurance	C 4, C 12	R 4, R 1
Statement of Compliance	O 25	Informal communication of approvals	No corporate wide standards	C 1	R 7, R 10
Control Operations by BUs	O 26	No documented process - not consistent	Inadequate documentation	C 1	R 1
Control Operations by BUs	O 27	No consistent process	Inconsistent operation of controls	C 5	R 1, R 7

Work Stream	Observation No.	Description	Theme	Conclusion No.	Recommendation No.
Control Operations by BUs	O 28	No escalation process; no trending	No trending of control effectiveness, No process for dealing with exceptions and escalations	C 7	R 11
Self-Certification Reporting	O 29	No standards	No corporate wide standards	C 1, C 2	R 1
Exception Handling	O 30	No standards	No corporate wide standards	C 1, C 2	R 1
Exception Handling	O 31	No documented process	Inadequate documentation	C 1	R 1
Exception Handling	O 32	No escalation process; no trending	No trending of control effectiveness, No process for dealing with exceptions and escalations	C 7	R 11
Exception Handling	O 33	No escalation path within IA	No process for dealing with exceptions and escalations	C 7	R 1
Exception Handling	O 34	Inadequate operation of controls and location of evidence	Inadequate operation of controls, Poor evidence retention	C 6	R 3, R 10, R 11
Exception Handling	O 35	Aspirational controls, most of these did not occur on time	Controls did not mitigate risk	C 4 C 9	R 1, R 8
Control Management	O 36	No documentation or standards	Inadequate documentation	C 1	R 1
Control Management	O 37	No documented process	Inadequate documentation	C 1	R 1
BU Exception Management	O 38	No decision-making criteria for control retirement or merging	No documented assessment criteria	C 1	R 1, R 1
BU Exception Management	O 39	No audit trail verifying L1 sign-off based on confirmed reviews	Poor evidence retention	C 6	R 3
Self-Certification sign-off	O 40	No separation of duties for those doing downstream certification	In adequate separation of duties		R 1

Work Stream	Observation No.	Description	Theme	Conclusion No.	Recommendation No.
Self-certification record mg	O 41	No standards for control documentation	No corporate wide standards	C 2	R 1
Self-certification record mg	O 42	Each BU had different approaches to storage - structure and location	No corporate wide standards, Poor evidence retention	C 2	R 1
Self-certification record mg	O 43	No clear evidential trail in RACM	Poor evidence retention	C 6	R 3, R 10
Self-certification record mg	O 44	Unclear remediation dates for controls		C 8	R 7
Self-certification record mg	O 45	Lack of evidence to prove controls were operated	Poor evidence retention	C 6	R 3, R 10
Self-certification record mg	O 46	No standards for evidence preservation; inadequate tools	Poor evidence retention	C 6	R 3, R 1
Self-certification review	O 47	IA review did not check if control mitigated risk	Controls did not mitigate risk	C 4	R 8, R 15
Self-certification review	O 48	C&E review did not ensure that control mitigated risk	Controls did not mitigate risk	C 4	R 8, R 15
Self-certification review	O 49	No corporate-wide standards	No corporate wide standards	C 2	R 1
Self-certification review	O 50	IA and C&E did not have automatic access rights to access evidence		C 6	R 9
Cases and chronology	O 51	Critical information about controls not maintained consistently		C 6 C 8	R 1
Cases and chronology	O 52	Control report used to eliminate exceptions	Controls did not mitigate risk	C 4	R 1, R 1, R 7
Cases and chronology	O 53	[redacted]		[redacted]	[redacted]
Cases and chronology	O 54	Ineffective controls	Controls did not mitigate risk	C 4	R 12, R 13

Work Stream	Observation No.	Description	Theme	Conclusion No.	Recommendation No.
Cases and chronology	O 55	Risks not appraised for impact or likelihood	No quantification of risk likelihood or impact	C 2	R 13
Cases and chronology	O 56	Risks and issues were not defined	No corporate wide standards	C 2	R 1
Cases and chronology	O 57	RACM did not contain any information on results of Self-certification	Incomplete record keeping	C 8	R 7
Cases and chronology	O 58	Inconsistent record keeping	Incomplete record keeping	C 6, C 8	R 1
Cases and chronology	O 59	Key fields in the RACM not populated	Incomplete record keeping	C 11	R 1
Cases and chronology	O 60	Issues persisted over long periods of time	Inconsistent operation of controls	C 7	R 11
Cases and chronology	O 61	No escalation mechanisms in operation	No process for dealing with exceptions and escalations	C 7	R 12
Cases and chronology	O 62	No tool for trending of control status	Inadequate tools for control management, No trending of control effectiveness	C 8	R 7
Cases and chronology	O 63	Improvement in RACM over time	N/A		N/A
Preamble Process	O 64	No formal process and standards	Inadequate documentation, No corporate-wide standards	C 15	
Initial RAP Change Request	O 65	Well documented process.	N/A	C 16	N/A
Initial RAP Change Request	O 66	Process ownership needs to be clarified.	Poor definition of process ownership	C 25	R 1
Initial RAP Change Request	O 67	No independent assurance.	No independent assurance		R 4
Initial RAP Assessment	O 68	No documented assessment criteria	No documented assessment criteria	C 18	R 1, R 16
Initial RAP Assessment	O 69	Small number of people - sustainability issue	Small number of people - sustainability issue	C 18	R 4

Work Stream	Observation No.	Description	Theme	Conclusion No.	Recommendation No.
Prioritisation of RAP Requests	O 70	Lack of assessment criteria; no documentation; no evidence	No documented assessment criteria	C 17	R 1, R 16, R 17
Prioritisation of RAP Requests	O 71	No independent assurance.	No independent assurance		R 4
Ideation	O 72	Process is robust	N/A		N/A
High Level Concept	O 73	Well documented process.	E2E Technology Process well documented	C 16	N/A
Functional Specification and Design	O 74	Well documented process.	E2E Technology Process well documented	C 16	N/A
Duct Access	O 75	[redacted]		[redacted]	[redacted]
Duct Access	O 76	[redacted]		[redacted]	[redacted]
Duct Access	O 77	[redacted]	[redacted]	[redacted]	[redacted]
Duct Access	O 78	[redacted]	[redacted]	[redacted]	[redacted]
Duct Access	O 79	[redacted]		[redacted]	[redacted]
SLA Development	O 80	No formal process or performance metrics	No formal process or performance metrics	C 22	R 6
SLA Development	O 81	Long elapsed time	Wide differences in elapsed development times, Un-mitigated risk	C 20	R 16
SLA Development	O 82	No separation of common SLAs topics across forums		C 23	R 24
SLA Development	O 83	Long elapsed time	Wide differences in elapsed development times	C 20	R 16

Work Stream	Observation No.	Description	Theme	Conclusion No.	Recommendation No.
SLA Development	O 84	Separation of financial penalties		NA	N/A
Regional Handover	O 85	[redacted]	[redacted]	[redacted]	[redacted]
Regional Handover	O 86	[redacted]	[redacted]	[redacted]	[redacted]
Address Matching	O 87	[redacted]	[redacted]	[redacted]	[redacted]
Address Matching	O 88	[redacted]	[redacted]	[redacted]	[redacted]
Enhanced Provisioning	O 89	Short elapsed time	Wide differences in elapsed development times	C 20	R 16
Enhanced Provisioning	O 90	No formal decision criteria; lack of evidence of decision making	Lack of evidence of decision making by senior management, No documented assessment criteria	C 19	R 17
Bespoke Bid	O 91	[redacted]	[redacted]	[redacted]	[redacted]
Bespoke Bid	O 92	[redacted]	[redacted]		[redacted]
Bespoke Bid	O 93	[redacted]	[redacted]	[redacted]	[redacted]
KPIs	O 94	No formal process or test plans, no independent assurance	No formal process or performance metrics, No independent assurance	C 27	R 23
KPIs	O 95	Consistent time criteria for data extracts	N/A		N/A
KPIs	O 96	No specifications for report generation programs	Poor data management for KPIs, No independent assurance	C 27	R 19, R 23

Work Stream	Observation No.	Description	Theme	Conclusion No.	Recommendation No.
KPIs	O 97	Reference data not consistently managed	Poor data management for KPIs, No independent assurance	C 29	R 19
KPIs	O 98	Well documented process.		N/A	
KPIs	O 99	Procedure manual explained the reference data	Well documented process.	N/A	N/A
KPIs	O 100	Incomplete documentation of functional specification of code	Inadequate documentation, No independent assurance	C 27	R 1, R 23
KPIs	O 101	Meta-data files not dated	Poor data management for KPIs, No independent assurance	C 27	R 19
KPIs	O 102	No centrally managed process for reference data	Poor data management for KPIs, No independent assurance	C 29	R 19
KPIs	O 103	No process for ensuring all records were accounted for	Poor data management for KPIs	C 28	R 19, R 21, R 22, R 23
KPIs	O 104	No detailed checks on accuracy of outputs	Poor data management for KPIs, No independent assurance	C 28	R 20, R 21, R 22
KPIs	O 105	SB-WLR, LLU, WLA have KPI Reporting process manuals	Well-documented process	N/A	N/A
KPIs	O 106	Manual steps required to execute scripts for Service KPIs		C 29	R 22
KPIs	O 107	No detailed checks on accuracy of outputs for Service provisioning data	Poor data management for KPIs, No independent assurance	C 30	R 19, R 23
Storm Mode	O 108	Well documented process.	N/A	C 31	N/A
Storm Mode	O 109	Well documented process.	N/A	C 31	N/A
Storm Mode	O 110	Clear decision making criteria	N/A	C 31	N/A

Work Stream	Observation No.	Description	Theme	Conclusion No.	Recommendation No.
Storm Mode	O 111	ComReg Determination 17/08 on T&Cs on Service Credits		N/A	N/A
Storm Mode	O 112	Good supporting documentation	N/A	C 31	N/A
Engagement Channels	O 113	No formal process or performance metrics	No formal process or performance metrics	C 32	R 6
Engagement Channels	O 114	No formal process or performance metrics	No formal process or performance metrics	C 32	R 6
Engagement Channels	O 115	Long elapsed time	Wide differences in elapsed development times	C 33	R 24, R 25
Engagement Channels	O 116	Lack of project management discipline	Lack of project management discipline for dealing with Op. requests	C 33	R 6

7.3. Process Quality, Maturity and Capability

7.3.1. ISO9001 - Process Quality

ISO 9000 espouses seven principles , of which two are relevant specifically to the adequacy of the control environment, and its ability to identify risks and ensure the appropriate mitigation. These principles are translated into best practice as laid out in ISO9001.

The principles are:

a. QMP 4 – Process approach

Assessment of processes for their ability to provide consistent and predictable results. A better achievement in this area improves compliance capabilities. The principles list these as benefits;

- Consistent and predictable outcomes through a system of aligned processes
- Enabling the organization to provide confidence to interested parties as to its consistency.

b. QMP 6 – Evidence-based decision making

The availability of process data and information ensures that the desire results are more likely to be achieved. Cartesian use this principle to assess process quality in their ability to provide these benefits listed

The benefits listed for this principle which bear on the assessments made include;

- Improved assessment of process performance and ability to achieve objectives
- Increased ability to demonstrate the effectiveness of past decisions

The key points from ISO9001 that have a bearing on assessing eir's ability to comply with their obligations are tied to visibility of the processes that are used for operating the RAP lifecycle, including the development of RAP, and the processes used for assurance. This is manifested in ensuring that stakeholders understood how they carried out processes, that these processes were well-documented and maintained, and that the adherence to the processes could be demonstrated. They were not used to assess eir's compliance and certification for ISO9001.

7.3.2. CMMI – Process Capability

CMMI (Capability Maturity Model® Integration) principles are used to gauge the capabilities and maturity of processes. The CMMI model was useful in providing guidance in what to look for to help understand the ability of an organisation to perform certain types of functions, such as providing services, or developing product. The models help to assess the capabilities eir possessed that needed to meet the requirements set by ComReg for RAP and not to measure eir's ability to be certified for CMMI.

The model identifies facets of processes and how advanced they are, and specific models (termed constellations) exist that are focused on Development and on Services. These are the most appropriate for assessing functions that were covered in the scope of works required.

CMMI utilizes a selection of Process Area components to gauge the two aspects, capability, and maturity. Depending on the capabilities and maturity of a process area, components are added into the evaluation.

As Cartesian only used CMMI to assess eir's ability to meet compliance, only a subset of components was used. ISO9001 also cover some aspects of CMMI principles.

a. Service Model: This applies to RMCF, NPD, Bespoke Bids, NGA Bitstream, NGA VUA, CGA Bitstream, SB-WLR Pole Access and Duct Access Lifecycle processes. For Risks and Controls, processes that accompany the design and implementation processes were looked at using these principles.

b. Development Model: This was applicable to RAP development and the associated RAP cases.

The CMMI Assessment Criteria utilized consisted of some of the indices covering Capability and Maturity Levels. (In CMMI, these assessments are based on a scale of 1 – 4.)

Higher CMMI assessment levels are accompanied by lower levels of uncertainty and inconsistency in outcomes, and greater control over the processes. This translates into greater visibility of the processes, through improved metrics and record-keeping, trending and analysis of processes, all of which are helpful in improved compliance to the obligations. Process stability combined with transparency through metrics, clear decision points, process standards and tolerances, increases the probability of equivalent outputs for the same given inputs, while providing visibility to all the decisions made leading to the completion of tasks driven by the processes. Cartesian have used these constellations, their criteria and levels as guides in helping develop Cartesian's own assessment template.

7.3.3. Sarbanes-Oxley – Process Controls

While Sarbanes-Oxley Controls under section 404 apply to direct and indirect financial processes (under which some of the processes in-scope are applicable), the same principles can be used as best practice across processes dealing with regulated products. Guidelines from Section 404 that are pertinent to assuring adequate controls include:

a. Ensuring that controls are effective over time

b. Change control and risk assessments

c. Checklists for evaluation by certifying officers

d. Maintenance of evidence documentation of control results and operations

e. Evaluate controls designed to prevent or detect fraud, including management override of controls (Of interest here was the ability to override controls)

f. Assess IT-based transactions flows, both manual and automated such as to locate weaknesses that would allow for misstatements

Section 404 covers the rules used to report the scope and adequacy of the internal control structures, as well as the procedures for financial reporting. While the financial reporting aspects are not a concern, Sarbanes-Oxley 404 provides useful guidance in assessing internal control adequacy. A key driver for this Section 404 is the centralisation of controls reporting, to reduce the overhead associated with both reporting on the status of controls, but also in auditing them.

7.4. Operational Level Assessments

Cartesian assessed the processes support RAP at three levels.

a. Business Operational

These processes are a collection of related, structured activities or tasks that produce a specific service or product. They are executed by operational teams responsible for carrying out these processes, such as operating product-customer lifecycles, including product development, covering both standard operational and exception processes.

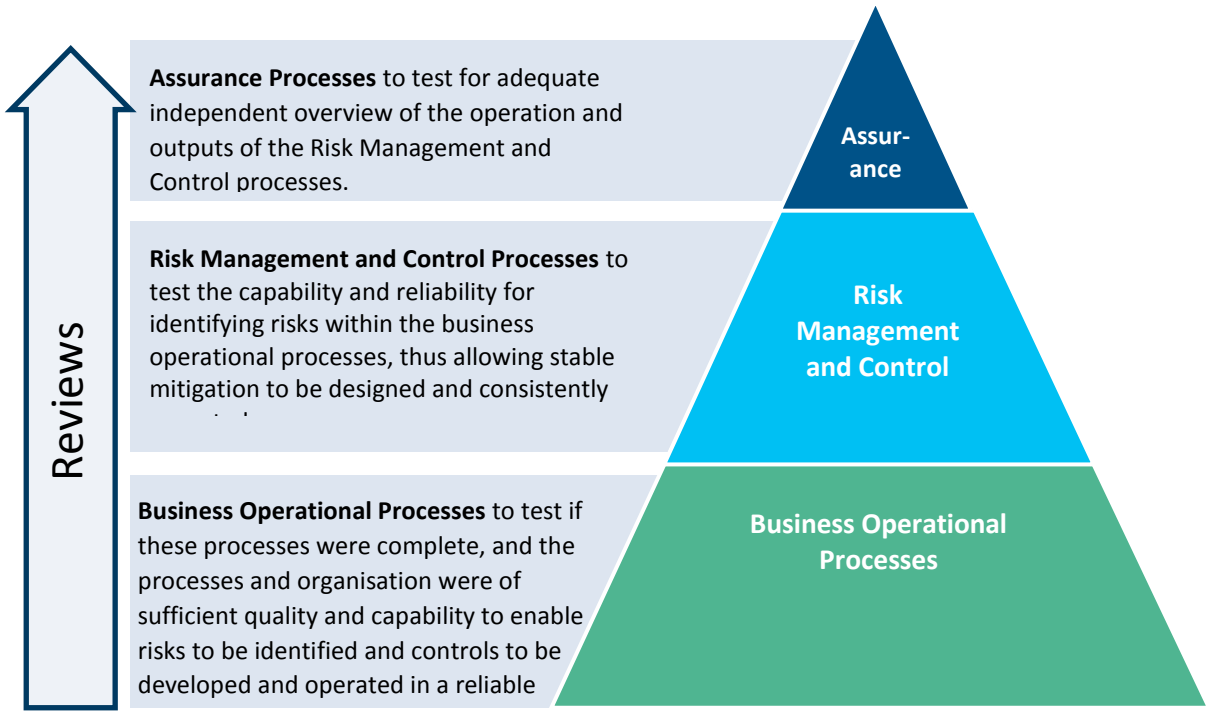
b. Risk Management and Control

These processes are owned and operated by management teams over the Business Operational processes. These processes identify risks, develop, implement and operate the required mitigations and report on their efficacy and status. They incorporate metrics, standards and tolerances to ensure business operational processes are operating acceptably. They provide corrective actions to bring operational processes back within tolerance when needed

c. Assurance

These processes are operated by independent teams to the Business Operational and Management teams. They assure that all applicable standards and being met by the Business Operational processes. They assure Management and Control are in place, and being executed to the required standards.

Figure 9. Process Area Hierarchy



Cartesian is a specialist consulting firm in the telecoms, media and technology sector. For over 25 years, we have advised clients worldwide in strategy development and assisted them in execution against their goals. Our unique portfolio of consulting services and managed solutions are tailored to the specific challenges faced by executives in these fast-moving industries. Combining strategic thinking, robust analytics, and practical experience, Cartesian delivers superior results.

www.cartesian.com

For further information, please contact us at cartesian@cartesian.com

Transformation. Accelerated.