



# Advisory Circular

TCAA-AC-GEN015A

February 2020

## GUIDANCE ON SAFETY RISK ASSESSMENT AND MITIGATION

### 1.0 PURPOSE

This Advisory Circular (AC) provides guidance to service providers on safety risk assessment and mitigation.

### 2.0 REFERENCES

The Civil Aviation (Safety Management) Regulations, 2015

### 3.0 BACKGROUND

#### 3.1 Regulatory Requirements

The Civil Aviation (Safety Management) Regulations require service providers to develop and maintain a formal process that ensures analysis, assessment and control of the safety risks of the consequences of hazards during the provision of its services. This advisory circular provides guidelines to enable service providers to conduct safety risk assessment and mitigation in compliance with regulatory requirements. The safety risks of each identified hazard shall be analysed in terms of probability and severity, and assessed for their tolerability. The service provider shall define safety controls for each safety risk assessed as tolerable.

#### 3.2 Safety Risk Management

Safety risk management is a key component of a safety management system. The term “safety risk management” is meant to differentiate this function from the management of financial risk, legal risk, economic risk and so forth. The fundamentals of safety risk includes the following:

- a) a definition of safety risk;
- b) safety risk probability;
- c) safety risk severity;
- d) safety risk tolerability; and
- e) safety risk management

#### 3.3 Definition of Safety Risk

Safety risk is the projected likelihood and severity of the consequence or outcome from an existing hazard or situation. While the outcome may be an accident, an intermediate unsafe event or consequence may be identified as the most credible outcome. Provision for identification of such layered consequences is usually associated with more sophisticated risk mitigation software. The safety risk mitigation worksheet illustrated in Appendix 2 to this Advisory Circular also has this provision.



# Advisory Circular

TCAA-AC-GEN015A

February 2020

## 3.4 Safety Risk Probability

The process of controlling safety risks starts by assessing the probability that the consequences of hazards will materialize during aviation activities performed by the organization. Safety risk probability is defined as the likelihood or frequency that a safety consequence or outcome might occur. The determination of likelihood can be aided by questions such as:

- a) Is there a history of occurrences similar to the one under consideration, or is this an isolated occurrence?
- b) What other equipment or components of the same type might have similar defects?
- c) How many personnel are following, or are subject to, the procedures in question?
- d) What percentage of the time is the suspect equipment or the questionable procedure in use?
- e) To what extent are there organizational, managerial or regulatory implications that might reflect larger threats to public safety?

Any factors underlying these questions will help in assessing the likelihood that a hazard may exist, taking into consideration all potentially valid scenarios. The determination of likelihood can then be used to assist in determining safety risk probability.

**Table 1** below presents a typical safety risk probability table, in this case, a five-point table. The table includes five categories to denote the probability related to an unsafe event or condition, the description of each category, and an assignment of a value to each category.

It must be stressed that this is an example only and that the level of detail and complexity of tables and matrices should be adapted to be commensurate with the particular needs and complexities of different organizations. Also, it should be noted that organizations may include both qualitative and quantitative criteria that may include up to fifteen values.



# Advisory Circular

TCAA-AC-GEN015A

February 2020

**Table 1: Safety Risk Probability Table**

<b>Risk Probability</b>	<b>Meaning</b>	<b>Value</b>
<b>Frequent</b>	Likely to occur many times (has occurred frequently)	5
<b>Occasional</b>	Likely to occur sometimes (has occurred infrequently)	4
<b>Remote</b>	Unlikely to occur, but possible (has occurred rarely)	3
<b>Improbable</b>	Very unlikely to occur (not known to have occurred)	2
<b>Extremely improbable</b>	Almost inconceivable that the event will occur	1

### 3.5 Safety Risk Severity

Once the probability assessment has been completed, the next step is to assess the safety risk severity, taking into account the potential consequences related to the hazard. Safety risk severity is defined as the extent of harm that might reasonably occur as a consequence or outcome of the identified hazard. The severity assessment can be based upon:

**a) Fatalities/Injury.**

How many lives may be lost (employees, passengers, bystanders and the general public)?

**b) Damage.**

What is the likely extent of aircraft, property or equipment damage?

The severity assessment should consider all possible consequences related to an unsafe condition or object, taking into account the worst foreseeable situation. **Table 2**, below, presents a typical safety risk severity table. It includes five categories to denote the level of severity, the description of each category, and the assignment of a value to each category. As with the safety risk probability table, this table is an example only.



# Advisory Circular

TCAA-AC-GEN015A

February 2020

**Table 2: Safety Risk Severity Table**

Severity	Meaning	Value
<b>Catastrophic</b>	<ul style="list-style-type: none"><li>- Equipment destroyed</li><li>- Multiple deaths</li></ul>	A
<b>Hazardous</b>	<ul style="list-style-type: none"><li>- A large reduction in safety margins, physical distress or a workload such that the operators cannot be relied upon to perform their tasks accurately or completely</li><li>- Serious injury</li><li>- Major equipment damage</li></ul>	B
<b>Major</b>	<ul style="list-style-type: none"><li>- A significant reduction in safety margins, a reduction on the ability of the operator to cope with adverse operating conditions as a result of increase in workload, or as a result of conditions impairing their efficiency</li><li>- Serious incident</li><li>- Injury to persons</li></ul>	C
<b>Minor</b>	<ul style="list-style-type: none"><li>- Nuisance</li><li>- Operating limitations</li><li>- Use of emergency procedures</li><li>- Minor incident</li></ul>	D
<b>Negligible</b>	<ul style="list-style-type: none"><li>- Little consequences</li></ul>	E

### 3.6 Safety Risk Tolerability

The safety risk probability and severity assessment process can be used to derive a safety risk index. The index created through the methodology described above consists of an alphanumeric designator, indicating the combined results of the probability and severity assessments. The respective severity/probability combinations are presented in the safety risk assessment matrix in **Table 3**.

The third step in the process is to determine safety risk tolerability. First, it is necessary to obtain the indices in the safety risk assessment matrix. For example, consider a situation where a safety risk probability has been assessed as occasional (4), and safety risk severity has been assessed as hazardous (B). The composite of probability and severity (4B) is the safety risk index of the consequence.



# Advisory Circular

TCAA-AC-GEN015A

February 2020

**Table 3: Safety Risk Assessment Matrix**

Risk probability	Risk Severity				
	Catastrophic A	Hazardous B	Major C	Minor D	Negligible E
Frequent 5	5A	5B	5C	5D	5E
Ocassional 4	4A	4B	4C	4D	4E
Remote 3	3A	3B	3C	3D	3E
Improbable 2	2A	2B	2C	2D	2E
Extremely improbable	1A	1B	1C	1D	1E

*(Colour Codes Red to denote “Intolerable”; Yellow to denote “Tolerable”; Green to denote “Acceptable”)*

The index obtained from the safety risk assessment matrix must then be exported to a safety risk tolerability matrix {Table 4 (a)} that describes the tolerability criteria for the particular organization. Using the example above, the criterion for safety risk assessed as 4B falls in the —unacceptable under the existing circumstances| category. In this case, the safety risk index of the consequence is unacceptable.

The organization must therefore:

- a) take measures to reduce the organization’s exposure to the particular risk, i.e. reduce the likelihood component of the risk index;
- b) take measures to reduce the severity of consequences related to the hazard, i.e. reduce the severity component of the risk index; or
- c) cancel the operation if mitigation is not possible.

*Note.— The inverted pyramid in Table 4(b) reflects a constant effort to drive the risk index towards the bottom APEX of the pyramid. Table 5 provides an example of an alternate safety risk tolerability matrix.*

Table 4 (a): Safety Risk Tolerability Matrix

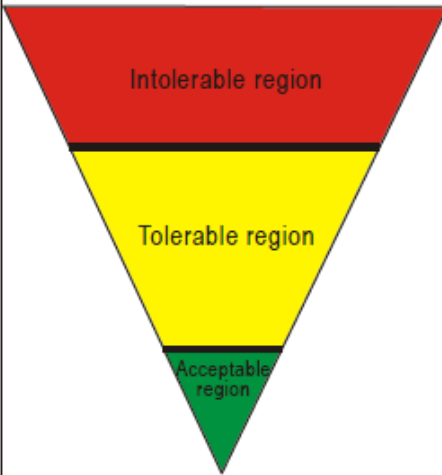
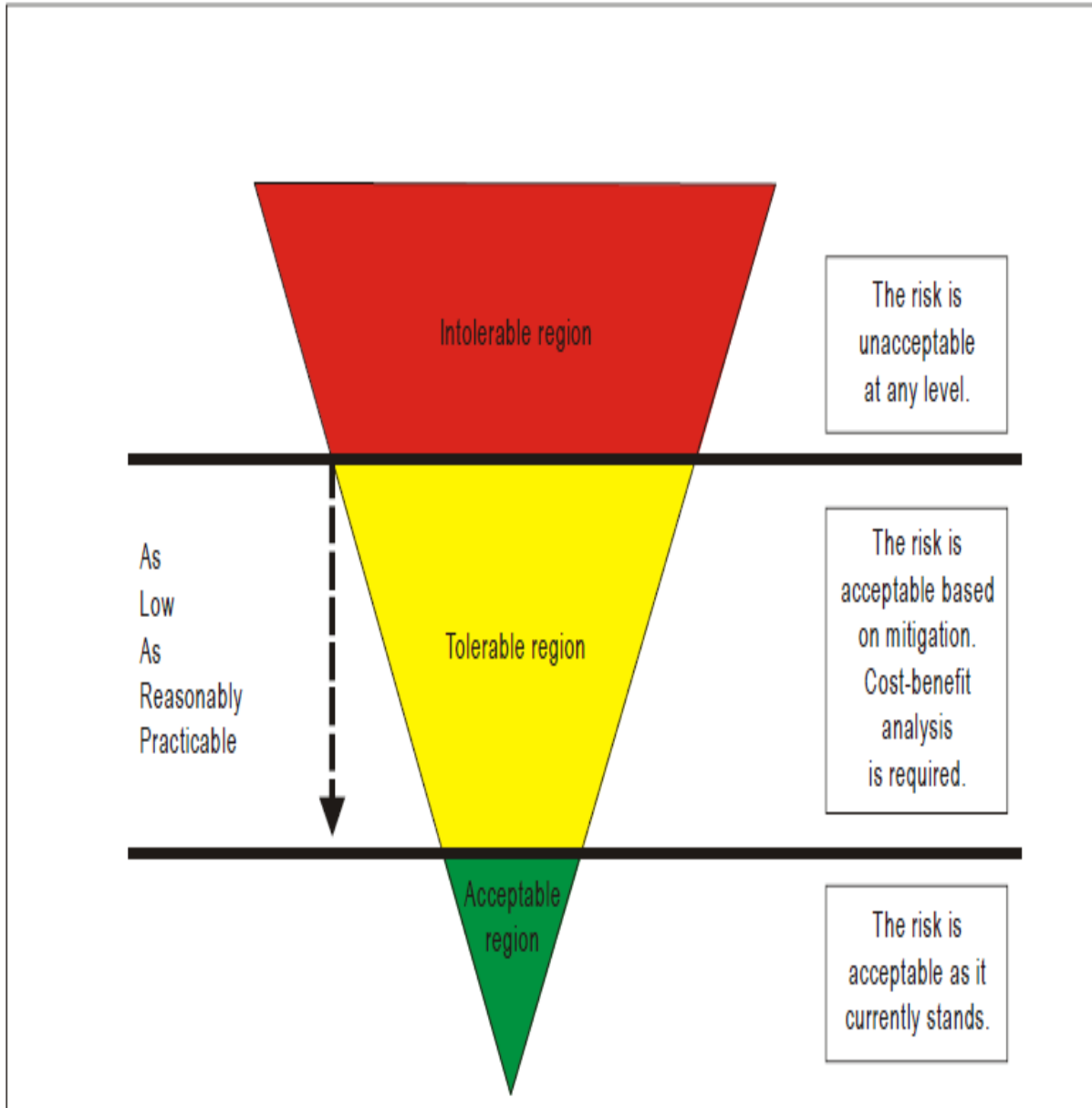
Suggested criteria	Assessment risk index	Suggested criteria
	<p><b>5A, 5B, 5C, 4A, 4B, 3A</b></p>	<p>Unacceptable under the existing circumstances</p>
	<p><b>5D, 5E, 4C, 4D, 4E, 3B, 3C, 3D, 2A, 2B, 2C</b></p>	<p>Acceptable based on risk mitigation. It may require management decision.</p>
	<p><b>3E, 2D, 2E, 1A, 1B, 1C, 1D, 1E</b></p>	<p>Acceptable</p>

Table 4 (b)





# Advisory Circular

TCAA-AC-GEN015A

February 2020

**Table 5: An Alternate Safety Risk Tolerability Matrix**

<b>Risk index range</b>	<b>Description</b>	<b>Recommended action</b>
5A, 5B, 5C, 4A, 4B, 3A	<b>High risk</b>	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.
5D, 5E, 4C, 4D, 4E, 3B, 3C, 3D, 2A, 2B, 2C, 1A	<b>Moderate risk</b>	Schedule performance of a safety assessment to bring down the risk index to the low range if viable
3E, 2D, 2E, 1B, 1C, 1D, 1E	<b>Low risk</b>	Acceptable as is. No further risk mitigation required

## 4.0 SAFETY RISK MANAGEMENT

### 4.1 General Principles

Safety risk management encompasses the assessment and mitigation of safety risks. The objective of safety risk management is to assess the risks associated with identified hazards and develop and implement effective and appropriate mitigations. Safety risk management is therefore a key component of the safety management process at both the State and product/service provider level.

Safety risks are conceptually assessed as acceptable, tolerable or intolerable. Risks assessed as initially falling in the intolerable region are unacceptable under any circumstances. The probability and/or severity of the consequences of the hazards are of such a magnitude, and the damaging potential of the hazard poses such a threat to safety, that immediate mitigation action is required.

Safety risks assessed in the tolerable region are acceptable provided that appropriate mitigation strategies are implemented by the organization. A safety risk initially assessed as intolerable may be mitigated and subsequently moved into the tolerable region provided that such risks remain controlled by appropriate mitigation strategies. In both cases, a supplementary cost-benefit analysis may be performed if deemed appropriate.

Safety risks assessed as initially falling in the acceptable region are acceptable as they currently stand and require no action to bring or keep the probability and/or severity of the consequences of hazards under organizational control.

### 4.2 Human Factors and Risk Management

Given that mature SSPs and SMSs target both human and organizational factors, a specific analysis process is a component of any mature, effective risk management system. In the course of any hazard identification and risk mitigation exercise involving human elements,

it is necessary to assure that existing or recommended defences have taken human factors (HF) into consideration. Where necessary, a supplementary HF analysis may be conducted to support that particular risk mitigation exercise/team. An HF analysis provides an understanding of the impact of human error on the situation and ultimately contributes to the development of more comprehensive and effective mitigation/corrective actions. A human error model is the basis of the analysis process, and it defines the relationship between performance and errors and categorizes errors to permit the root hazards to be more readily identified and better understood. This understanding ensures the adequate completion of a root-cause analysis. Individual actions and decisions viewed out of context can appear to be virtually random events, escaping their due attention. Human behaviour is not necessarily random. It usually conforms to some pattern and can be analysed and properly understood. Ultimately, this important HF perspective results in a more comprehensive and in-depth mitigation process. An HF analysis ensures that during the organization's risk mitigation process, when identifying root, contributory or escalation factors, human factors and their associated circumstantial, supervisory and organizational impacts are duly taken into consideration.

#### **4.3 Cost-Benefit Analysis**

Cost-benefit or cost-effectiveness analysis is normally an independent process from safety risk mitigation or assessment. It is commonly associated with a higher level management protocol, such as a regulatory impact assessment or business expansion project. However, there may be situations where a risk assessment may be at a sufficiently high level or have a significant financial impact. In such situations, a supplementary CBA or cost-effectiveness process to support the risk assessment may be warranted. This is to ensure that the cost-effectiveness analysis or justification of recommended mitigation actions or preventive controls has taken into consideration the associated financial implications.

### **5.0 SAFETY RISK MITIGATION**

#### **5.1 General Principles**

After safety risks have been assessed through the preceding step, elimination and/or mitigation to As Low As Reasonably Practicable (ALARP) must take place. This is known as safety risk mitigation. Safety risk controls/mitigations must be designed and implemented. These are measures to address the hazard and bring under control, the safety risk probability and severity of the consequences. These may be additional or changed procedures, new supervisory controls, changes to training, additional or modified equipment, or any of a number of other elimination/mitigation alternatives.

Almost invariably these alternatives will involve deployment or re-deployment of any of the three traditional aviation defences (technology, training and regulations), or combinations of them. After the safety risk controls have been designed, but before the system is placed "online," an assessment must be made of whether the controls introduce new hazards to the system.

#### **5.2 Mitigation Strategies**

There are three generic strategies for safety risk control/mitigation:

a) **Avoidance.**

The operation or activity is cancelled because safety risks exceed the benefits of continuing the operation or activity. Examples of avoidance strategies include;

- i) operations into an aerodrome surrounded by complex geography and without the necessary aids are cancelled;
- ii) operations in RVSM airspace by non-RVSM equipped aircraft are cancelled.

b) **Reduction.**

The frequency of the operation or activity is reduced, or action is taken to reduce the magnitude of the consequences of the accepted risks. Examples of reduction strategies include;

- i) operations into an aerodrome surrounded by complex geography and without the necessary aids are limited to daytime, visual conditions;
- ii) operations by non-RVSM equipped aircraft are conducted above or below RVSM airspace.

c) **Segregation of Exposure.**

Action is taken to isolate the effects of the consequences of the hazard or build in redundancy to protect against them. Examples of strategies based on segregation of exposure include:

- i) operations into an aerodrome surrounded by complex geography and without the necessary aids are limited to aircraft with specific performance navigation capabilities;
- ii) non-RVSM equipped aircraft are not allowed to operate into RVSM airspace.

Safety risk control/mitigation strategies are mostly based on the deployment of additional safety defences or the reinforcement of existing ones. Defences in the aviation system can be grouped under three general categories:

- a) technology;
- b) training; and
- c) regulations.

As part of safety risk control/mitigation, it is important to determine if new defences are necessary or if existing ones must be reinforced. This is done by determining whether;



# Advisory Circular

TCAA-AC-GEN015A

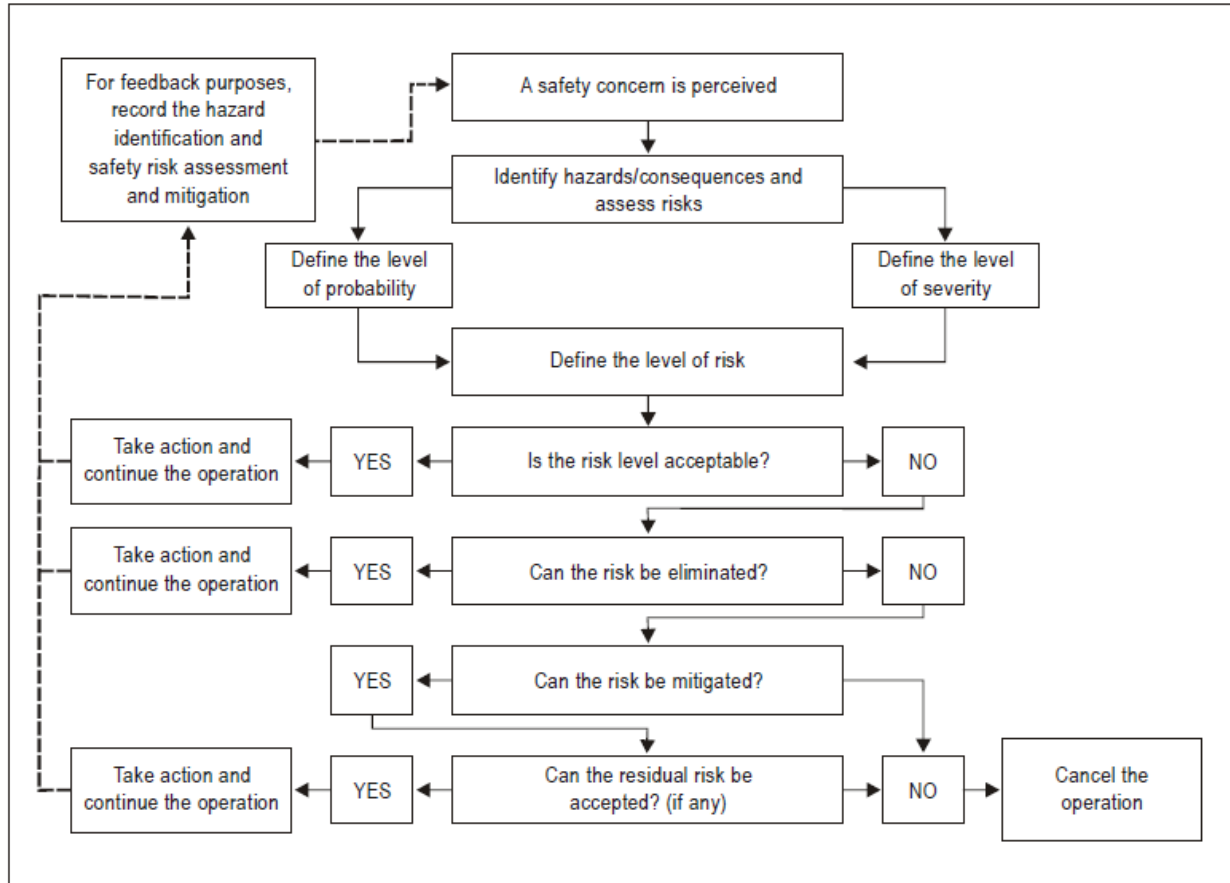
February 2020

- a) existing defences protect against the safety risks;
- b) defences function as intended;
- c) the defences are practical for use under working conditions;
- d) staff are aware of safety risks of the consequences of the hazard and the defences in place;
- e) additional safety risk mitigation and control measures are required.

A handwritten signature in black ink, appearing to be "P. P. [unclear]". The signature is written in a cursive style and is positioned above a horizontal line.

**Director Safety Regulation**

## APPENDIX 1: SAFETY RISK MANAGEMENT PROCESS



If the safety risks are assessed as unacceptable, the following questions become relevant:

- Can the safety risk(s) be eliminated?*** If the answer is yes, then action as appropriate is taken and feedback to the safety library established. If the answer is no, the next question is:
- Can the safety risk(s) be mitigated?*** If the answer is no, the operation must be cancelled. If the answer is yes, mitigation action as appropriate is taken and the next question is:
- Can the residual safety risk be accepted?*** If the answer is yes, then action is taken (if necessary) and feedback to the safety library established. If the answer is no, the operation must be cancelled.

These questions reflect the fact that mitigation strategies can never completely mitigate safety risks. It must be accepted that a residual safety risk will always exist, and the organization must ensure that residual safety risks are also under control.



# Advisory Circular

TCAA-AC-GEN015A

February 2020

## APPENDIX 2 TABLE A- HAZARD AND CONSEQUENCE

Operation/process:	Describe the process/operation/equipment/system being subjected to this HIRM exercise.
Hazard (H):	If there is more than one hazard to the operation/process, use a separate worksheet to address each hazard.
Unsafe event (UE):	If there is more than one UE to the hazard, use a separate worksheet to address each UE-UC combination.
Ultimate consequence (UC):	If there is more than one UC to the hazard, use a separate worksheet to address each UC.

## TABLE B - RISK INDEX AND TOLERABILITY OF CONSEQUENCE

	Current risk tolerability (taking into consideration any existing PC/RM/EC)			Resultant risk index and tolerability (taking into consideration any new PC/RM/EC)		
	Severity	Likelihood	Tolerability	Severity	Likelihood	Tolerability
Unsafe event						
Ultimate consequence						

## TABLE C- RISK MITIGATION

Hazard (H)	PC	EF	EC		RM	EF	EC	
H	PC1 (Existing)	EF (Existing)	EC1 (Existing)	UE	RM1	EF (to RM1)	EC (to EF)	UC
			EC2 (New)					
	PC2 (Existing)	EF1 (New)	EC (New)		RM2	EF (to RM2)	EC (to EF)	
			EC (New)					
PC3 (New)	EF (New)	EC (New)	RM3	EF (to RM3)	EC (to EF)			