NEW ZEALAND
CUSTOMS SERVICE
TE MANA ĀRAI O AOTEAROA

MAF

REQUEST FOR INFORMATION

THE NEW ZEALAND CUSTOMS SERVICE
AND
MINISTRY OF AGRICULTURE AND FORESTRY

JOINT BORDER MANAGEMENT SYSTEM

APPENDIX 4

INTELLIGENCE & RISK
KEY BUSINESS REQUIREMENTS

RELEASE VERSION
RELEASE DATE 21 MAY 2010

COMMERCIAL IN-CONFIDENCE

This page intentionally left blank

TABLE OF CONTENTS

This page intentionally left blank

1. INTRODUCTION

1.1. PURPOSE

The purpose of this document is to describe the JBMS intelligence and risk management framework with particular emphasis on the associated JBMS functionality required to support it. It is intended to set the vision of the framework for the business and to provide context for the various components and processes which will make up the overall framework.

1.2. INTENDED AUDIENCE

This document is intended for the following stakeholders:

- Business Stakeholders – ensure alignment with programme objectives, and broader strategic goals;
- Risk and Intelligence Subject Matter Experts – validate definitions, requirements and scenarios;
- JBMS Business Analysts – understand definitions and concepts for inclusion in requirements specifications;
- JBMS Architects – understand definitions and concepts for impact analysis on system specification and design;
- Vendors – provide context in support of detailed business requirements.

1.3. DOCUMENT STRUCTURE

This document describes the intelligence and JBMS risk management framework and introduces the main aspects from a business and process point of view. The framework is presented in term of the intelligence cycle, with particular regard to the risk management standard NZS/AS 4360 (and its revision AS/NZS ISO 31000:2009). The appendix provides a concept model that describes the relationships between the component parts.

1.4. INTELLIGENCE AND RISK MANAGEMENT FRAMEWORK – JBMS SCOPE

Whilst this document describes the framework as a whole, its main focus is on describing the framework with regard to how it is supported by JBMS.

Key elements of JBMS scope for intelligence and risk management are as follows:

- Support an integrated intelligence and risk management framework of People, Goods, Craft and Commodities across multiple agencies and multiple shared services as well as supporting Customs / MAF -specific risk management needs;
- Enable pre-set profiles and risk rating rules that will contribute towards automated risk identification and assessment;
- Enable automatic searching and matching of current and historical entities to increase efficiency and reduce manual effort of Customs / MAF officers;
- Support Customs / MAF risk management, specifically:
  - Gathering and assessment of information from a variety of sources;
  - Identification and evaluation of Risk Type;

- Rating of risks in accordance with rules;
- Management of risk profiles;
- Support pattern recognition and matching;

- Support the assessment and management of Intelligence products;
- Provide tools to assist the analytical process;
- Use pattern analysis to assist with identification of risk profiles;
- Facilitate audit and assurance activities.

1.5. TERMINOLOGY - ENTITY VERSUS COMMODITY

JBMS is a single system, providing shared services to both Customs and MAF i.e. both agencies use the same processes and often the same data. From a risk and intelligence perspective, the system focus is on entities (people, places, organisations, consignments, premises etc.) and their attributes [redacted] 6(c) 6(c) [redacted]. A commodity (type of good) can be an entity, the attributes of which are the type of container, packaging, mode of transport, country of origin etc.

From a solution perspective, the functions required of the JBMS Risk and Intelligence components to support an entity-based model are exactly the same as those for a commodity-based model.

2. INTELLIGENCE AND RISK MANAGEMENT FRAMEWORK OVERVIEW[1]

The intelligence and risk management framework will underpin business processes and the analysis of all information within the system. It will assess all risk-relevant data received using a risk rating mechanism, profiles and alerts, and constantly reassess these risks as new information is received and as time passes. This range of risk assessment tools will be managed within the system, providing improved support for Customs / MAF decision-making.

6(c)

Whilst Intelligence has historically had a focus on enforcement, through the application of JBMS we will also be able to detect non-deliberate compliance breaches.

The intelligence and risk management framework utilises a range of treatment options; it reflects the Intelligence Cycle; and it follows the Risk Management Standard AS/NZS 4360:2004 (and its revision AS/NZS ISO 31000:2009).

2.1. TREATMENT OPTIONS

The Customs / MAF intelligence and risk management framework includes a range of treatment options. These fall under the following categories:

- **Encouragement of Voluntary Compliance** - Provide advice and feedback to clients to encourage voluntary compliance with rules / regulations / legislation.
- **Deterrence** - Raising the profile of Customs / MAF interdiction activities so that the risk of being caught is perceived to be higher.
- **Prevention** - Use of systems, processes and legislation to reduce opportunities for illegal behaviour.
- **Detection** - Collection and analysis of information, which creates intelligence, to identify higher-risk transactions.
- **Capture** - Development of techniques to improve the effectiveness of interventions.
- **Treatment** - Treating risks using an appropriate level of intervention from available options.

The *system* elements of the intelligence and risk management framework will exist within this context and are largely associated with detection of risk, but also cover elements of prevention and prosecution. Prosecution is just one of a number of potential responses to detected risk. The human elements of detecting and preventing risk are mentioned at the end of this document.

[1] Whilst workflow, action plans and evidence management are referred to in this document, they are functions which will be provided outside of the intelligence and risk management framework.

2.2. THE INTELLIGENCE CYCLE

The Intelligence Cycle is the process of creating intelligence from raw information. The cycle comprises the following six steps:

- **Collect -** Gather information and raw data according to requirements (Collection Plan).
- **Evaluate -** Assess the credibility, reliability, pertinence, and accuracy of information items
- **Collate -** Sort, file and link information to establish relationships
- **Analyse -** Assemble information in a logical manner; assess elements of information to form patterns and meaning; identify significant facts. The product (conclusions and recommendations) is intelligence.
- **Disseminate -** Distribute the intelligence product to clients/users. The resulting intelligence product can take many forms depending on the needs of the decision-makers and reporting requirements.
- **Re-evaluate -** The intelligence cycle is a closed loop; feedback is received from the transactions or decision-maker and revised requirements issued where necessary.

Each of these steps is reflected within the intelligence and risk management framework.

2.3. THE RISK MANAGEMENT STANDARD

The Customs / MAF intelligence and risk management framework, based on the Risk Management Standard AS/NZS 4360:2004 (and its revision AS/NZS ISO 31000:2009), progresses through the stages of:

1. Gathering information;
2. Identifying risk types;
3. Analysing risk;
4. Evaluating and treating risks;
5. Communicating risk;
6. Monitoring and reviewing risks and responses to risk.

The functionality of the framework is explained below, under these headings. It is largely focussed on the JBMS (system) components (i.e. not the human element) of managing risk.

2.4. GATHERING INFORMATION

2.4.1. Establish information source reliability and information validity

All information received will be assessed in terms of source reliability, data validity and government security classification and handling instructions, before being linked to the entity or entities to which it belongs.

Where possible, this assessment will be automatically made by JBMS, based on knowledge of the information's source system. System-generated assessment can be changed for the information source as a whole, or for individual pieces of information as appropriate but only by an authorised person.

Officers will manually assess the reliability/validity of information they enter (e.g. information received from an informant), based on the judgement of that

officer. Some types of information they enter though, for example information recording a seizure, will not require manual reliability/validity assessment because this is information directly available to the officer; it is not coming from a third party.

2.4.2. Entity Mining

Within JBMS, the process of deriving high-quality, relevant information from a variety of disparate sources will, where appropriate, be automated (or semi-automated) using Entity Mining. In the context of JBMS, entity mining encompasses elements of concept mining, named entity mining, search and query. For instance an analyst will be able to conduct a broad entity mine encompassing a number of facets, one of which will retrieve and present all data stored within JBMS that is about or potentially related to the specified named entity.

6(c)

[redacted]

2.4.3. Entity Matching

Customs / MAF must ensure that all data received is attributed to the right entity (e.g. person, consignment, craft, etc) as soon as it is received, to ensure that a complete view of the available information for the entity is available for risk assessment. This includes avoidance (minimisation) of duplicate entities and identification of potential duplicates.

All data entered into the system will either be:

- Linked to an existing, matched entity; or
- Flagged for addition to one or more potential matches; or
- A new unique entity record will be created for the data to be linked to.

System linkages between potential matches will allow for relationships to be updated when they are confirmed or disproved.

The matching function will be semi-automated and governed by rules which define the acceptable level beyond which matches can be confirmed for merging by the system itself.

2.4.4. Entity Merging

Entity merging will occur whenever it is determined that two or more entity records represent a single unique entity. It will be predominantly system prompted and, where a pre-set level of certainty is met, will be automated. A high degree of functionality in the merging process will allow fields to be managed in order to retain and display the most relevant and current data. The merge history will allow users to review changes and undo these if necessary.

2.5. Identifying Risk Types and Establishing Baseline Risk

This section aims to clarify key terminology as it is used in this and related documents, in particular the terms threat, risk, organisational risk, operational risk, and finally risk types which are a key component of the framework. It also discusses baseline risk.

2.5.1. Identifying Risk Types

Threat and Risk

Threats and risks are managed by both Customs and MAF. Threats are typically described as arising from intention and capability, where either or both of these factors may be present to a greater or lesser extent. For example the potential for a particular entity to traffick drugs is a threat that is present in the environment, comprising the entity's intent and capability to do so.. Risk is a combination of the likelihood of a threat occurring and the consequences or impact of that threat. Customs and MAF also deal with risks which do not have an "intention" component, so the term "risk" also includes likelihood and consequence of unintentional events.

The nature of biosecurity risk usually requires MAF to deal with risks associated with legitimate goods i.e. the entity importing them is not accused of any wrong doing. For example a consignment of fruit could be an innocent host for a harmful pest or organism. This could also apply in the Customs environment. JBMS will enable the assessment of both risks and threats.

Organisational risk and Operational risk

There are two key categories of risk - organisational and operational. The intelligence and risk management framework is focussed on identification and management of operational risks only. However, the prioritisation of operational risks may be impacted by organisational risks. Each of these is defined below so that the distinction here is clear.

- **Organisational Risks** - these are risks that have an impact on an organisation's ability to fulfil its duties to the Crown, for example, the risk of loss of key staff. They are considered annually by the respective Customs / MAF executive, and are published, for example, as the "New Zealand Customs Service – 201X/201Y Organisational Risk Profile" or the MAF equivalent.
- **Operational Risks** - these are the risks which Customs / MAF are charged with managing on behalf of the Crown, [redacted] 6(c) [redacted] They are reconsidered periodically (at least annually), and updated as needed, based on intelligence and on feedback from within the intelligence and risk management framework itself. [redacted] 6(c)

Risk Types

Operational risks are ordered into Risk Types. These include but are not limited to the risks of [redacted] entering the country. It is these risk types that the intelligence and risk management framework focuses on. 6(c)

However, Customs and MAF recognise that there can be threats and risks to officers' safety in the course of carrying out their work. This requires a separately rated risk type so that the significance is not lost in any aggregated risk rating. This is included as an operational risk type as it arises from the assessment of entities and events in the operational domain. [redacted] 6(c)

2.5.2. Establishing the risk baseline

It will be important to assess the baseline level of risk associated with each work-stream (people, goods, craft) for a number of reasons:

- To enable Customs / MAF to demonstrate the effectiveness of its activities, and track changes to baseline risk over time;
- To assist with identification of a move to new techniques by the perpetrators of illegal activity or of new entities that 'fly under the radar' of standard intelligence network;
- To assist with planning and resourcing of all interventions, including those carried out for sampling, to encourage front-line staff to undertake sampling and intuition-based activities;
- To better inform resource allocation on the basis of intelligence-based risk assessment, in addition to historical interception levels;
- To assist with measurement of the effectiveness of deterrence and intervention activities and provide incentives for these.

A *measure* for the baseline level of risk of each key risk area needs to be established. For example, a count of interceptions of methamphetamine and its pre-cursors at the border as a percentage of the total number of methamphetamine related interceptions nationally will form the baseline using the figures for the full year prior to the implementation of the new risk management framework. The assumption is that there is a direct relationship between the number of methamphetamine related arrests and the number of consignments across the border that host methamphetamine or its precursors. For other risks e.g. the importation of untreated wood products, the baseline level of risk might be a combination of seizures and the efficacy of interventions (where an intervention might be the fumigation prior to export of certain types of goods from a particular country of origin).

2.6. Analysing Risk

The intelligence and risk management framework will use the following tools to analyse risk:

- Risk rating;
- Profiles;
- Pattern Analysis;
- Interest Register Notifications;
- Audit and assurance.

2.6.1. Risk Rating

Risk rating is a measure of the likelihood that a transaction or entity is involved in activities of interest to Customs or MAF, for a given risk type.

The goal of the risk rating mechanism is to assist with the identification / prioritisation of those entities / transactions which pose the greatest risk so that resources can be directed toward treating those risks. The risk rating application is a tool only and should be used to augment the work of both Intelligence and front-line officers.

Customs and MAF are charged with addressing quite different types of risks, which will have different risk factors. Where similar risk factors exist, their relative importance may differ between agencies. Therefore Customs and MAF

will each have their own risk rating (or set of risk ratings) on any entity or transaction.

Customs and MAF priorities, and their associated risk types, may change with government priorities. The system will be flexible so as to integrate and react to changes in prioritisation of Customs and biosecurity risk.

Selected data elements will be considered indicative of risk, and in some cases the value of an element will be rated differently. For example, as the severity of the offence for which a person has been convicted increases, the associated predictive value increases proportionally

The result of the preceding three points is that there will be a matrix of risk ratings, not just a single risk rating. Each entity will have an *overall total level of risk* from an agency perspective. This will be an aggregate of *scores based on more specific, weighted criteria* – for example the risk of being a drug trafficker / involved in organised crime, etc.

All entities / transactions will be risk-rated each time new information is received about them. Risk rating will take into account all relevant information held about the entity / transaction at the time of the rating. A risk rating represents the "potential value" of the risk an entity / transaction poses, rather than the actual risk associated with the entity / transaction when it is encountered, although the latter would contribute to an updated risk rating.

A risk rating algorithm / method will be applied by the application to all of the information now held on this entity to arrive at a score. This score is one element within the risk assessment toolset. It can be used to rank entities (by entity type; by risk type, etc) to assist with directing Customs / MAF resources to areas of greatest need.

The system-generated risk ratings will not be manually adjustable. In this way they remain evidence-based, consistent and defensible.

Risk ratings will be reassessed at particular time intervals and when the risk rating criteria changes.

Risk rating will assess the risk of an entity / transaction pre-, post- or at the border, because these risks may be different.

Where the risk rating for an entity / transaction exceeds a predetermined threshold an alert will be created automatically, identifying that entity / transaction to be of concern.

2.6.2. The "Red Flag" Concept

In order to cater for the situation where an entity's rating does not seem to accurately reflect its perceived risk [redacted] a ***"Red Flag" concept*** will be available. A Red Flag can be placed on such an entity, signalling an issue with the risk rating and that further information needs to be gathered to confirm its rating where the instigator, [redacted] believes there is a higher or lower risk associated with that entity. A Red Flag can also be placed on an event.

6(c) 6(c) 6(c)

The instigator will set the flag in place and be required to record a free-text justification and select one or more risk types indicated by the information, then indicate or assess the level of risk.

To address the information gap the instigator or the assigned analyst may recommend activities to be performed that may need to be subsequently approved by a manager [redacted]

6(c)

The Red Flag risk element does not impact the risk rating scores, rather it qualifies a rating, highlighting that other factors may be relevant.

If and when sufficient information has been gathered the requirement will be re-evaluated and the flag may be removed.

The Red Flag concept may include a time limit. A range of time limit options would be available.

The risk rating scores and the Red Flag will require flexibility in the way in which they are presented and to whom they are presented. It must be clear at all times to those receiving such information what they are to do with it (i.e. what it means to them in the context of their interaction). Note that the "Red Flag" is expected to be an exceptional event.

2.6.3. Profiles

Profiles are aimed at identifying all entities / transactions that meet criteria set within the profile (whereas alerts are aimed at identifying one - and only one - specific entity or transaction).

Profiles can be based on identified patterns, that is, a range of criteria that collectively indicate a type of risk. [redacted] 6(c)

Risk types are generally agency specific and therefore most profiles will also be agency specific. However, a recent analysis of passenger interventions across Customs and MAF demonstrated that there was little difference in the risk profile for certain types of offenders. One profile therefore may require an accompanying action plan that involves multiple agencies.

All profiles co-exist in the JBMS domain and all relevant transactions and entity changes are tested against them.

Profiles have a quantitative element that allows the system to select transactions based on a combination of a range of risk variables.

Profiles can be based on any set of data elements the system collects, and may include criteria such as observations which must be made by an officer [redacted] 6(c)

MAF, and potentially Customs in the future, has a requirement for Low Risk profiling. That is, positively identifying those entities which have been assessed as unlikely to pose a risk. These profiles would assess entities / transactions against a set of criteria and, if these criteria were met, they would be automatically cleared to cross the border. An example could be that everyone on a particular flight will be subject to a MAF inspection except those that meet a low risk profile.

2.6.4. Pattern Analysis

Pattern Analysis (a type of Data Mining) is the process of finding previously unknown patterns and trends across the information stored within the JBMS and using that information to suggest profiles, identify risk entities and [redacted] 6(c) 6(c) [redacted] It also includes pattern matching - the ability to review data or transactions and match them to an already identified pattern. It is based on statistical analysis of all data that is available, whether that is client, transaction, finance or user activity related.

Once identified, patterns can be used to build profiles and inform risk rating, the results of which are analysed over time to assess effectiveness and ensure continuous improvement.

[redacted]

6(c)

2.6.6. Audit and Assurance

JBMS will support regular, periodic audits of risk treatments through a range of methods such as statistical sampling and population search (e.g. a preset percentage of all containers through a particular port within a month or a randomly generated action plan for inspection against a particular type of low risk transaction to assure Customs or MAF that it is still low risk). JBMS will also support evaluation of the use and effectiveness of different risk management tools.

Statistical sampling will be an important tool for identifying new risks – i.e. those risk areas for which there is, as yet, no intelligence.

2.7. Evaluating and Treating Risks

The intelligence and risk management system will use business rules to set thresholds, to determine whether an identified risk will be evaluated by the system itself, or by an officer. The risk management system will interact with the workflow system to invoke actions.

The actions to be taken will be established, recorded and managed using the action plan component of the JBMS.

The actions taken will be one of the following:

- Where a transaction or entity is deemed to be an *exact match* to a profile:
  - The profile may dynamically generate an alert and its actions (e.g. where an entity or transaction is to be intercepted before being cleared to cross the border); or
  - The profile may directly invoke identified planned actions (e.g. such as sending a notification to a craft that it must not cross the border).
- Where a *partial match* on a profile is made, and depending on cumulative risk rating, a task will be created for an analyst / evaluator to assess whether or not there is an actual match. If it is considered there is a match, the process will proceed as for an exact match; if not, the analyst will decide what response is appropriate
- When an alert hits, the action plan (including planned tasks, unplanned tasks and subsequent outcomes) is invoked for a response as per the alert. This may simply be to search a person, or to search or spray a container, for instance. Resulting outcomes are recorded, depending on what is found at that time.
- Where an Interest Notification is triggered, the interested party will be notified and can assess the information and respond appropriately.

2.7.1. Generate new information

As a result of any of the above actions, new information may be created either by the system or by manual entry (e.g. from observation).

6(c) [redacted]

2.8. COMMUNICATING RISK

There are a number of methods of communicating risk:

- Via alerts (and their associated action plans). The presence of an alert on an entity or transaction is a signal that there is an identified risk associated with that entity or transaction and that action is required, either now or in the future;
- Via notifications to frontline staff and/or Customs / MAF clients;
- Via intelligence reporting, assessments and other outputs.

2.8.1. Alerts

Alerts are placed on specific entities / transactions to detect them at their next interaction. They can be manually placed on an entity / transaction by an officer or created by the system as an output of profiling as the result of a profile match, and by risk rating as the result of a risk rating exceeding a pre-set threshold (where the latter two may be routed to an analyst / evaluator for approval first).

The system will process entities / transactions for matches against Alerts. If the transaction matches one or more alerts, the system may send notifications to the party or parties that registered the alert (according to rules set), and will invoke that alert's action plan. Alerts may be restricted in terms of their visibility.

6(c) [redacted]

2.8.2. Notify Frontline

JBMS will provide concise, timely information to front-line staff (and to external parties as required).

JBMS will enable the sending of information to frontline staff to make them aware of characteristics they need to be looking for which the system cannot identify. For example, goods are contained in packaging which is considered to

6(c) be a [redacted] In such cases, as these items are identified they will be recorded against a pre-set profile and the subjective assessment recorded by

[2] SmartGate is a kiosk system for automated passenger clearance. It uses facial recognition technology to identify the passenger, and accepts the passenger's responses to border clearance questions for Customs, immigration and biosecurity purposes,

the officer. The profile may prompt them to assess and record specific features which an analyst may then interpret in order to be able to create a more specific profile.

2.8.3. Notify Clients

The system will notify clients of a potential risk that they can mitigate themselves. For example, when lodging a declaration online, the system can check the details of the entry against a profile and notify the client of potential breaches of legislation or treatment requirements. They can then take corrective action before lodging their declaration.

2.8.4. Intelligence Output – Managing Information into Intelligence

The system will provide support for the creation and dissemination of Intelligence products. While there are some reports (mainly statistically based) that can be system-derived and disseminated, the majority will be completed manually. The workflow system will manage the approval and dissemination of these.

2.8.5. Investigation – Managing Information into Evidence

All information received will be managed as if it were to be required as evidence. The system will provide support for managing information into evidence to facilitate compliance with the Evidence Act 2006.

Some classes of information may be withheld from discovery under the Official Information Act. JBMS will enable appropriate management of this information.

6(c)

[redacted]

2.9. Monitoring and Reviewing Risks and Responses to Risks

2.9.1. Review Risk Rating

The risk rating on individual entities will be regenerated at pre-determined intervals (as well as every time there is a transaction or the receipt of information concerning that entity).

Review periods can be set for individual entities. The setting of the review interval will include a description and record the type of information required to be gathered to improve the quality of the risk rating on that entity.

The risk-rating algorithms themselves will be reviewed as necessary and at least annually. It is expected that periodic audits will be undertaken to determine whether or not the algorithms are correctly calibrated, by manually assessing the risk ratings for a sample of entities of various types.

Risk rating will also be reviewed as risk types and priorities change.

2.9.2. Review Alert

When alerts are created a review period (based on elapsed time or the number of activations) will be defined by the analyst. At that time the alerts will appear as a workflow item for the Analyst to remind them to assess whether or not the alert should remain in place in its current format, be changed, or be removed.

2.9.3. Update Interest Notification

Analysts will be able to update the "Interest Notification" on any entity, and change this Notification as events evolve.

2.9.4. Review Interest Notification

Interest Notifications may be reviewed but this will not be mandatory.

The system will provide the facility to identify active Interest Notifications by criteria such as age of notification, time since it was last triggered.

2.9.5. Create / Update Profile

Profiles can be generated manually or automatically (from pattern analysis). In either instance the profile will be assessed by the system for effectiveness and for impact on resources. The impact assessment will consider, for example, whether or not the profile is identifying entities as expected and the extent to which it will impede the flow of goods, passengers or craft across the border in relation to the significance of the risk is it attempting to target.

A profile cannot be activated until it has been approved by an authorised person. Workflow management will support this creation/approval process.

Profiles can be manually updated as required – and may (according to rules) require further impact assessment and re-approval.

2.9.6. Review Profile

As for Alerts, Profiles must be reviewed at regular intervals to determine their continued effectiveness and to assess their ongoing impact. They may, for example, be reviewed after a certain time period has passed, or after x matches, or after x successful interceptions based on that profile. A typical performance report against a profile might include:

- The number of transactions that the profile fully matched;
- The number of transactions that the profile partially matched where subsequent analysis resulted in an alert or action plan;
- The number of transactions that the profile partially matched that did not breach the predetermined risk rating threshold for notification to an analyst;
- The number of action plans generated;
- The number of action plans that were implemented;
- The number of times that the risk identified was found;
- The number of times that something else was found.

2.9.7. Analyse Data Automatically

As data is entered into the system the system may look for patterns over collections of data.

2.9.8. Analyse data manually

Data mining techniques and statistical analysis tools will also be manually employed to identify patterns. As patterns are identified, the system will facilitate the capture of those characteristics in a profile.

2.9.9. Identify Pattern

As new patterns are identified they will be considered (manually) in terms of the current set of Operational Risks and added as appropriate. That is, they may just suggest a new pattern identifying a current risk type, or they may suggest the presence of a new risk type.

2.9.10. Review Sampling / Audit Targets

Sampling and audit targets will be reconsidered (manually) as needed but at least on a periodic basis based on the observed outcomes of the risk management effort and any other information which may be relevant (e.g. offshore Intelligence information).

2.9.11. Conduct Population Audits

The system will facilitate the identification of populations (e.g. goods consignments, importers of a certain type), and related information for audit purposes. For example, the audit of transactions of all importers of X in time period Y, with a view to identifying what may have been missed in terms of risks. The results of such audits may lead to the identification of new profiles or additional risk indicators.

2.9.12. Monitor identified risk against baseline level

The concept of Risk Value will be used to quantify identified risk. Risk Value applies only to risks which are actually found (e.g. a quantity of drugs). When a detection is made the value of the detection will be determined by the system (using pre-set dollar values or other measure assigned to types of detections). The value will be based on data recorded for the detection, such as the type of material detected, the origin, and the degree of processing and intended end use. The risk value of detections is used in determining the baseline level of risk in a work stream, and would also contribute to the risk rating of an entity.

As risks are identified and assessed the results will be compared to baseline levels to determine whether or not there has been any significant improvement in risk detection and / or reduction in levels of risk. This information will be used to inform resourcing levels, to ensure that resources are targeted towards risks appropriately.

The value of the effort focused on a particular risk will be assessed against the value of the risk itself to ensure that excessive effort is not being applied to low risk areas.

6(c) [redacted]

6(c) [redacted]

2.10. THE HUMAN ELEMENTS OF DETECTING / PREVENTING RISK

The implementation of an enhanced information management system, in and of itself, may not be enough to realise significant operational benefits. It is important to consider what organisational changes might be required to ensure that maximum benefit is achieved from JBMS. The following should be included:

- Managing people to provide better outcomes, by
  - Regular meetings for two-way interchange of information between front-line staff and intelligence analysts; and between agencies. Such meetings currently exist between front-line staff and Analysts. They should at least be maintained, and enhancements considered as appropriate.

6(c) [redacted]

  - Maintaining experienced and talented staff at the front-line to ensure information gathered is of a high standard. JBMS will not replace good front-line staff. The intelligence the system contains is only as good as the people gathering and/or using the information upon which it is based, so the two agencies must maintain experienced and talented staff at the front-line. The quality of information captured plus the ability and experience required to spot and act upon unusual behaviours are key elements in the Customs / MAF approach.
  - Allocating resources and budget to the different work-streams based on assessed risk. As risk levels change over time in the various operational areas, there will be a requirement for flexibility of the allocation staff to manage those risks.
- Working with clients to provide better outcomes, by
  - *Providing general indicators to industry to encourage compliance.* The more information and assistance that can be given to industry regarding compliance requirements the more likely interactions with clients will be compliant from the beginning.
  - *Entering into partnerships with both on- and off-shore supply chain parties to optimise the supply chain process.* There are opportunities within the supply-chain to prevent issues, rather than attempting to cure them after the fact, by moving certain activities as close as possible to the beginning of the chain thereby leaving risk offshore. Such opportunities will be sought and pursued where practicable.

Organisational change, including cultural change, can be more difficult to implement than an IT system, and it is important that these organisational

factors are adequately considered and managed through the design and implementation phases.

3. APPENDIX: RISK ASSESSMENT AND INTELLIGENCE TERMS AND CONCEPTS

These appendices formalise the definition of terms that are used throughout the Risk and Intelligence set of requirements. A clear definition of terms such as Risk Type, Risk Rating, Entity, and Content Source is vital as they constitute a common semantic framework that ensures a consistent understanding of the JBMS risk assessment concepts.

3.1. STRUCTURE

The appendices are divided into two subject areas – Risk Assessment and Entity Mining, Matching and Merging.

Risk Assessment

In Risk Assessment two methods are used to assess the risks associated with entities (including commodities) and transactions. Also discussed is the notion of Alerts, which disseminate information regarding specific identified risks.

A conceptual model presents the primary elements and relationships of the JBMS risk assessment process. The model divides the assessment approach into three areas – data provision, risk profiling, and risk rating. Each concept is defined in detail and the function of each is explained with examples[3].

The conceptual model is followed by a scenario that shows how the two different risk assessment methods work in tandem to allow staff to efficiently assess the risk associated with entities and transactions, and to prioritise their workload accordingly.

Entity Mining, Matching, Merging

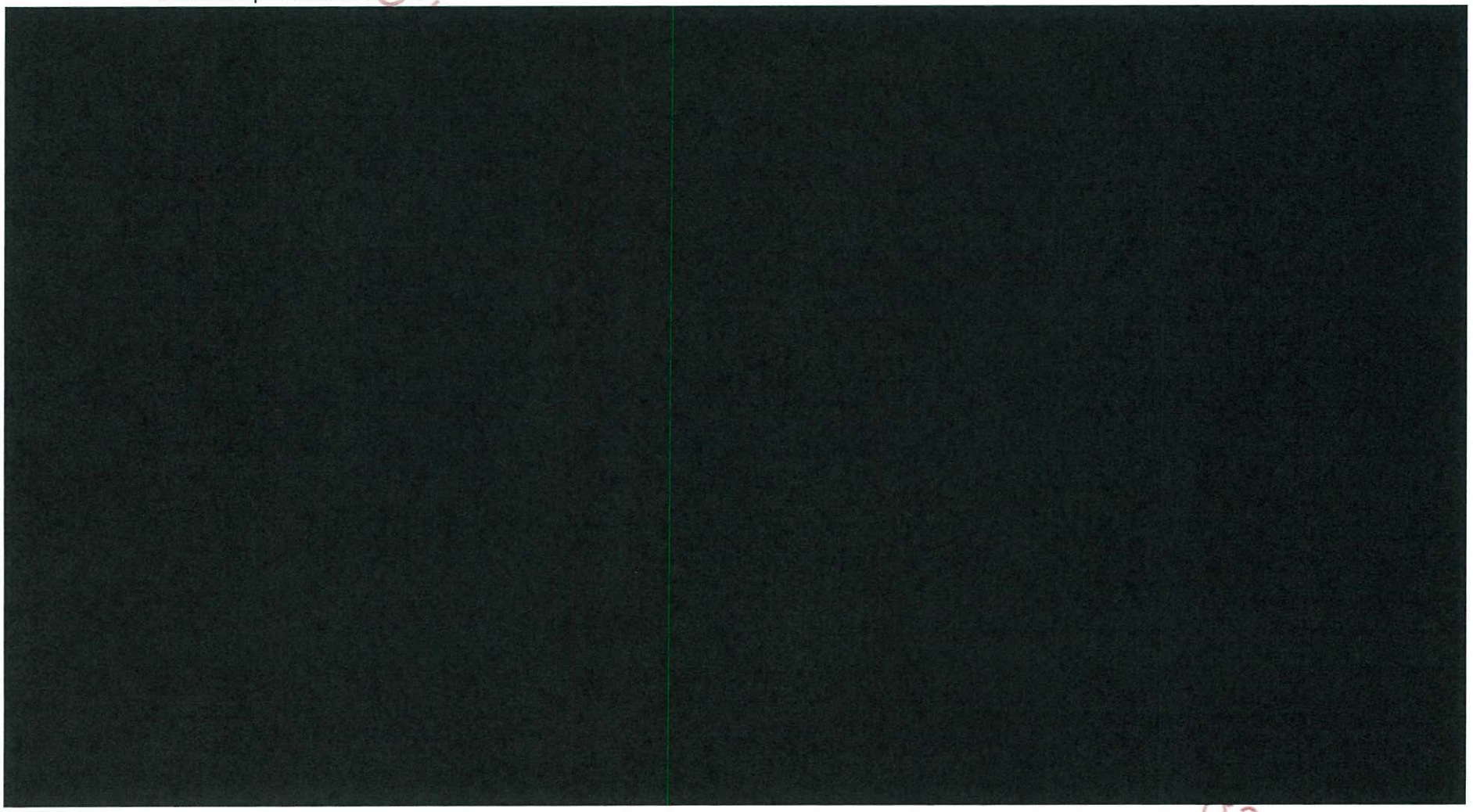
There are three methods used to discover and manage entities and transactions - Mining, Matching and Merging.

As for risk assessment, a conceptual model presents the primary elements and relationships of the JBMS entity discovery and management process, and this is supported by a scenario.

[3] These terms may map to one or more concepts that exist within the wider literature on intelligence analysis, risk profiling, and threat assessment.

4. RISK ASSESSMENT CONCEPTUAL MODEL

The diagram below illustrates the primary elements of the Risk and Intelligence risk assessment process and the relationship between them.



6(c)

The diagram is grouped into three categories, namely:

- JBMS data is collated in preparation for risk analysis;
- Risk Rating, which assesses and rates the risks associated with entities and transactions on an individual basis;
- Profiling, which also assesses and allows ranking of risks associated with entities and transactions, but on a grouped basis, to address targeted risks.

From the diagram it can be seen that the means by which Risk Rating and Profiling occur are very similar. As a result, the acts of Profiling and Risk Rating are easily confused – however, it will be shown that the results from each are very different.

The following sections provide definitions for the concepts presented in the diagram.

4.1. DEFINITIONS

6(c)

4.1.2. Profile Match Indicator

A Profile Match Indicator is a measure of the likelihood that an event or entity is involved in activities of interest to Customs or MAF, as determined by the degree of match to the profile risk factors.

Given that a profile may not include all the information necessary to maximise the likelihood of a successful intercept, the concept of an entity or event Risk Rating is additionally used to qualify a risk in the absence of a match to one or more profiles.

4.1.3. Risk Rating

Where a work queue has more work activities than can be processed by available resource, risk rating can be used to prioritise those activities so that the available resource targets those activities with the highest risk first.

Risk Rating is a measure of the likelihood that an event or entity is involved in activities of interest to Customs or MAF for a given risk type. Unlike a profile match indicator, a risk-rating uses a greater degree of ancillary information that may be difficult to capture using a single profile specification[4]. In addition, some entities and transactions that are risk rated are unlikely to be the subject of a profile, e.g. a Maritime Zone.

[4] Given the definitions of Profile Match Indicator and Risk Rating the reader may postulate a third measure (the Risk Measure) which uses the information used to determine the Risk Rating and Profile Match Indicator to objectively provide another measure of the risk associated with the entity or event. However, this is outside the scope of this document.

4.1.4. Entity

An entity is something that has a distinct, separate existence, though it need not be a material existence. In particular, abstractions and legal fictions are usually regarded as entities. Examples include Consignment, Person, Border, Organisation and Organism.

4.1.5. Entity-Related Information

Any information related to an entity, including entities and events that an entity may be related to.

4.1.6. Transaction

A capture of the information relating to an interaction between one or more entities at a moment or across a span of time. Examples include a Passenger Movement, Goods Declaration, Craft Arrival/Departure, Excise Return.

4.1.7. Transaction-Related Information

Any information related to a transaction, including entities and other transactions that a transaction may be related to.

4.1.8. Risk Type

The Risk Type categorises the forms of risk that are associated with an entity or transaction, such as Illicit Drug Importation or Intellectual Property infringement.

4.1.9. Risk Factor

An attribute within the set of information associated with an entity or transaction that, on it sown or in combination with other risk factors, informs the likelihood that the entity or transaction is involved in activities of interest to Customs or MAF.

4.1.10. Risk Factor Group

A set of risk factors used to assess the risk for a given risk type and entity or transaction. A risk factor group is specific to an entity type and the risk type.

The purpose of a risk factor group is to identify the combination of risk factors required to calculate the risk rating for a particular entity type and risk type.

4.1.11. Profiling Algorithm

The algorithm used to rate and rank the risk associated with an entity or transaction as determined from the risk factors associated with a given profile. The profiling algorithm is typically determined from prior pattern classification and matching analysis.

4.1.12. Risk Rating Heuristic

The heuristic used to rate the risk associated with an entity or event and given risk type. A heuristic can be described as an algorithm (i.e. a logical procedure) that has been demonstrated to be effective, even though it cannot be proven to be true. It is able to produce an acceptable solution to a problem but may not be proven to produce an optimal solution. Heuristics are typically used when there is no known method to find an optimal solution under the given constraints (of time, space etc.), or at all.

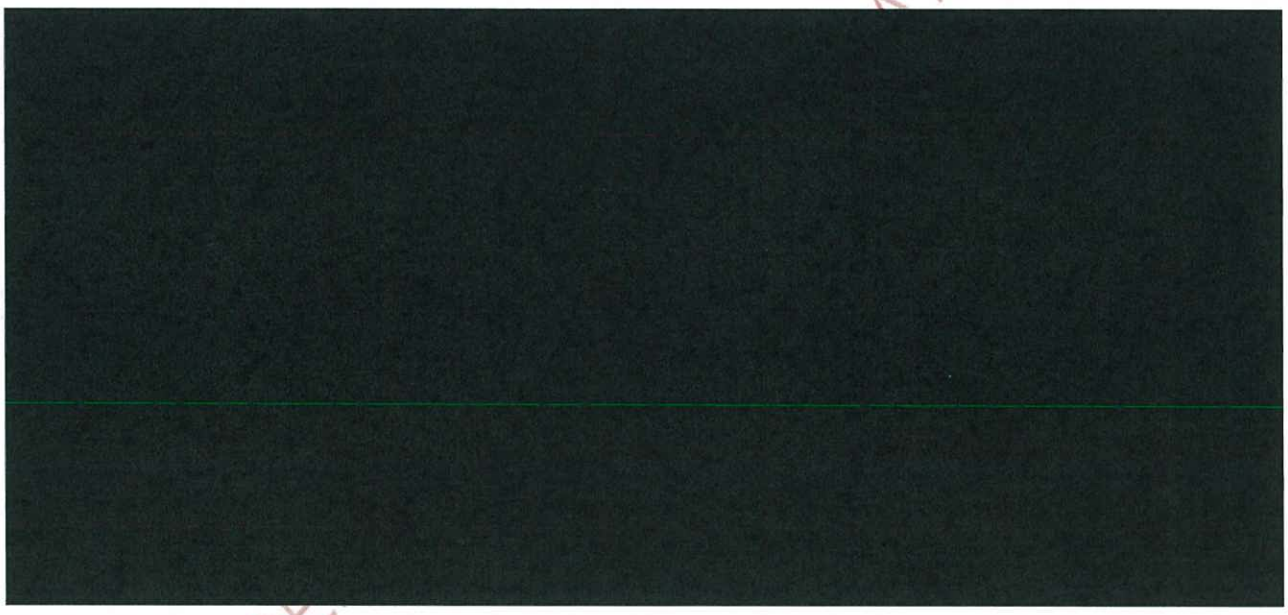
4.1.13. Alert

An alert is a flag held against a specific entity or transaction element, identifying that there is a risk associated to it, and specifying the action required to be taken when it is encountered. The alert is triggered by a specified event e.g. an alert on a person may be triggered when they arrive as a passenger at the border, in which case the alert may be set up to generate an Action Plan requiring a baggage search to be undertaken. Or an alert on a tariff code may be triggered when it is present on a Import Declaration submitted, in which case the alert may be set up to generate an Action Plan requiring an inspection.

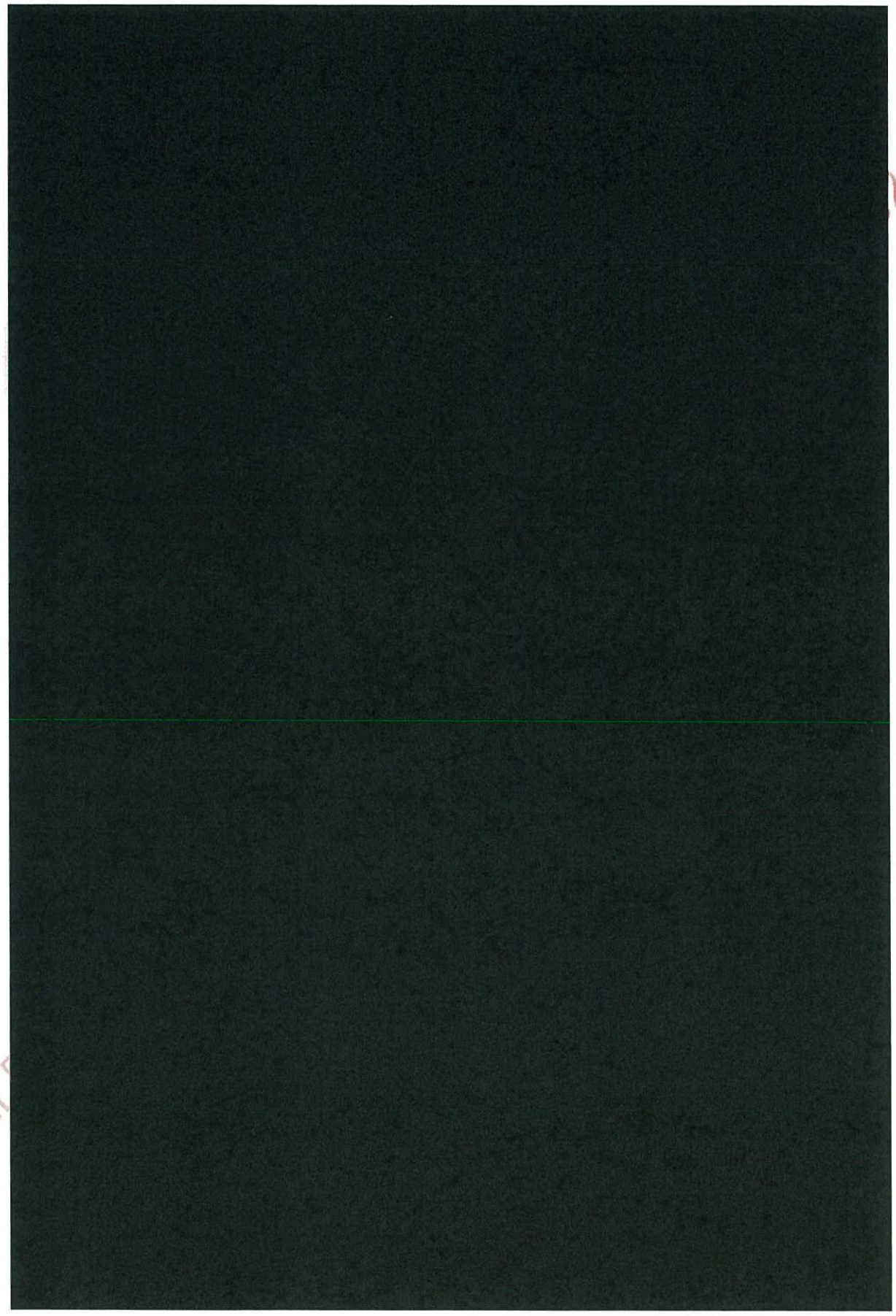
4.1.14. Action Plan

An Action Plan is a predetermined list of activities, usually associated with workflow. Action Plans may be carried out as a consequence of an alert or set of business rules that are associated with profiles and risk ratings, or to record standard business process activity.

6(c)

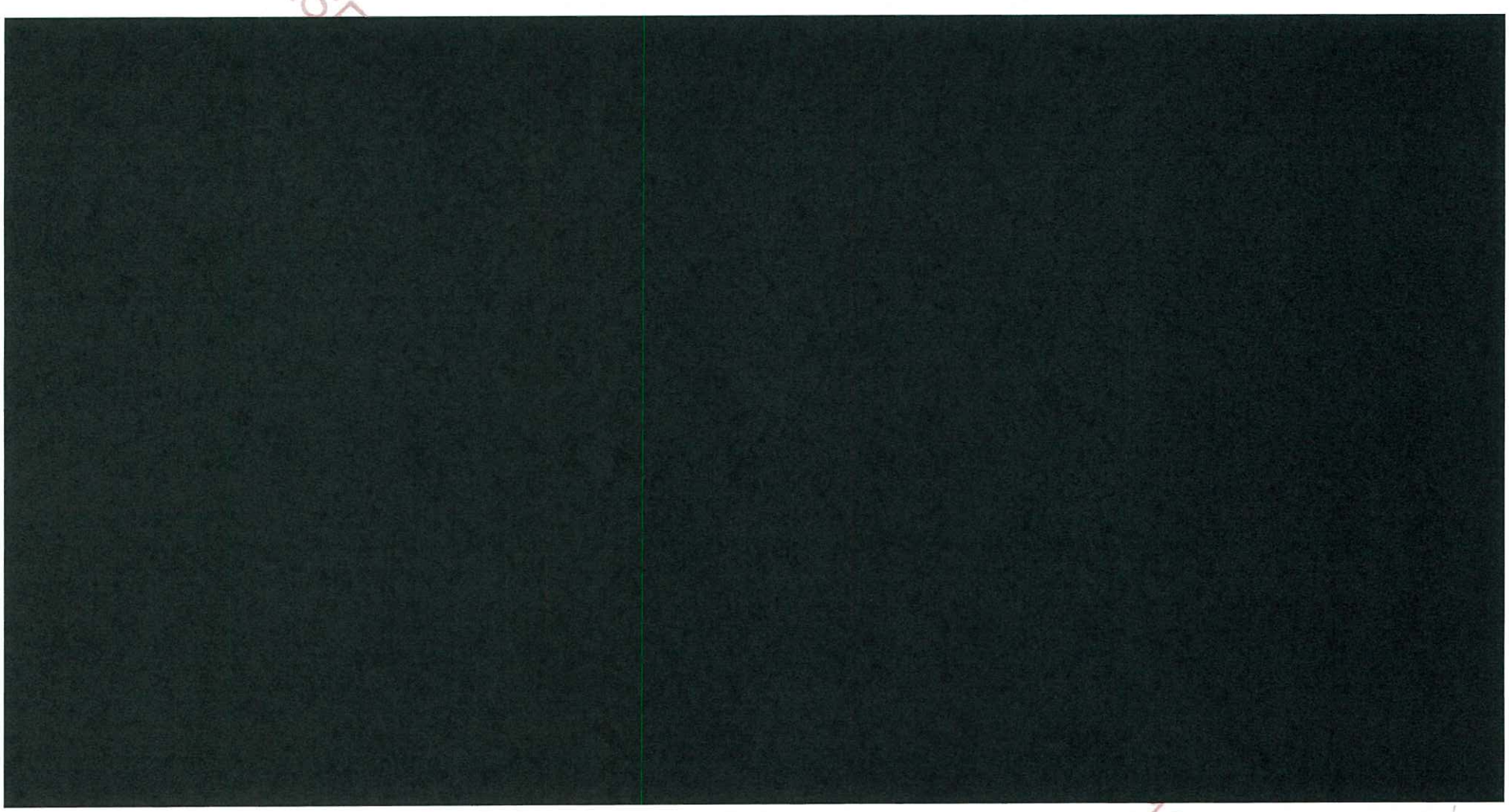


6(c)



5. ENTITY MINING, MATCHING AND MERGING CONCEPTUAL MODEL

6(c)



The diagram is grouped into three categories, namely:

- Data is searched and queried by the entity mining processes;
- Entity matching, which takes multiple entities (of a given type) from the consolidated results and processes them to determine the likelihood that they represent one and the same real-world entity;
- Entity merging, which is a process allowing a user to merge one or more entities together based on their judgment and analysis of the entity matching.

The following sections provide definitions for the concepts presented in the diagram.

5.1. DEFINITIONS

6(c)

5.1.2. Entity Matching

A process that takes multiple entities (of a given type) from an incoming transaction or Entity Mining result, and processes them to determine the likelihood that they represent one and the same real-world entity.

5.1.3. Entity Merging

A process allowing a user to merge one or more entities together based on their judgment and analysis of the degree of entity matching.

5.1.4. Content Source

A repository of information and/or data that can exist either internally or externally to JBMS. The structure and format of the information and or data is not specified.

5.1.5. Index

A proprietary repository of information and/or data that has been previously sourced (harvested) from one or more internal content sources for the purposes of indexing to facilitate fast search and retrieval. This will include both entities and entity related information, transactions and transaction related information and any other content deemed useful to JBMS.

5.1.6. External Information

Externally located information that could be stored in any variety of forms and structures.

5.1.7. Search

A system or user initiated request that invokes the entity mining tool to search against a set of internal content sources that contain information that has been previously indexed for the purposes of fast search and retrieval. Or by proxy it

will pass the request to an external federated search interface and wait for search results to be passed back from an external content source/s. This will typically, but not always, be unstructured information.

5.1.8. Search Results

A set of results from the entity mining tool in response to a system or user initiated request that will come from either an internal content source via the indexes or external content source via a federated search interface.

5.1.9. Query

A system or user initiated action that invokes the entity mining tool to query against an internal or external content source through a query interface. Typically this will be a query against structured information.

5.1.10. Query Results

A set of results from the entity mining tool in response to a system or user initiated request that will come from either an internal content source directly from a content source or an external content source via a query interface.

5.1.11. External Query Interface

An external interface that represents a query interface provided by an external party, that allows a query to be conducted directly over one of their content sources against the live data.

5.1.12. Federated Search Interface

An external interface that represents a search facility provided by an external party that indirectly allows a search to be conducted over one or more of their own content sources through indexes.

5.1.13. Consolidated Results

Search results and query results brought together for the purposes of further processing by a down stream process such as entity matching or for presentation to the user.

5.1.14. Entity Match Set

A set of known entities of a given type passed to the entity matching tool.

5.1.15. Mined Entity (Type A)

A single instance of a known entity of a given type e.g. person, address etc that has been entity mined and passed to the entity mining tool along with other known entities of the same type in an entity match set for the purposes of system matching.

5.1.16. Entity Merge Set

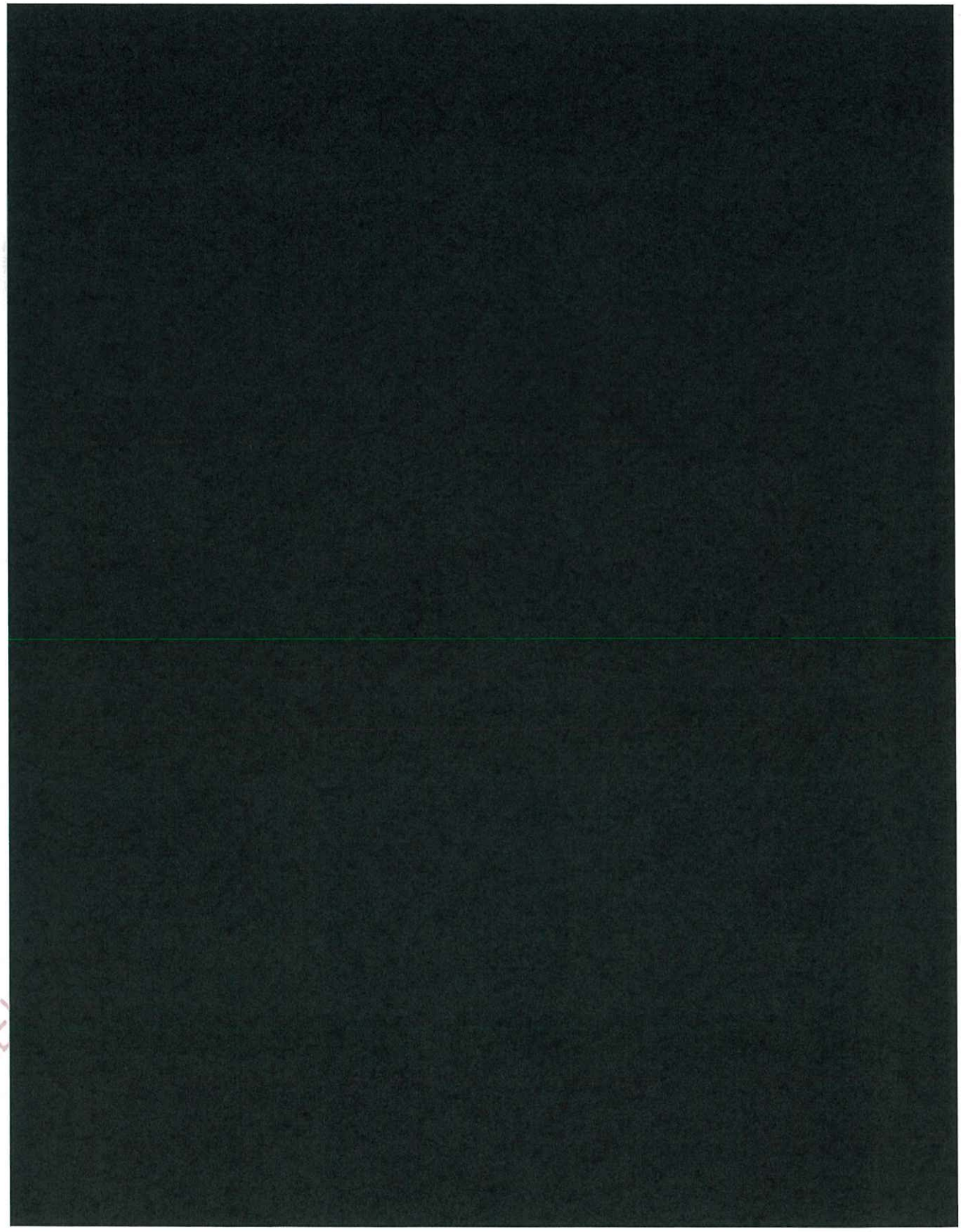
A set of user selected known entities of a given type selected for entity merging.

5.1.17. Entity (Type A)

A single instance of a known entity of a given type e.g. person, address etc that has been entity matched and passed to the entity merging tool along with other

known entities of the same type in an entity merge set for the purposes of user merging.

6(c)



6(c)