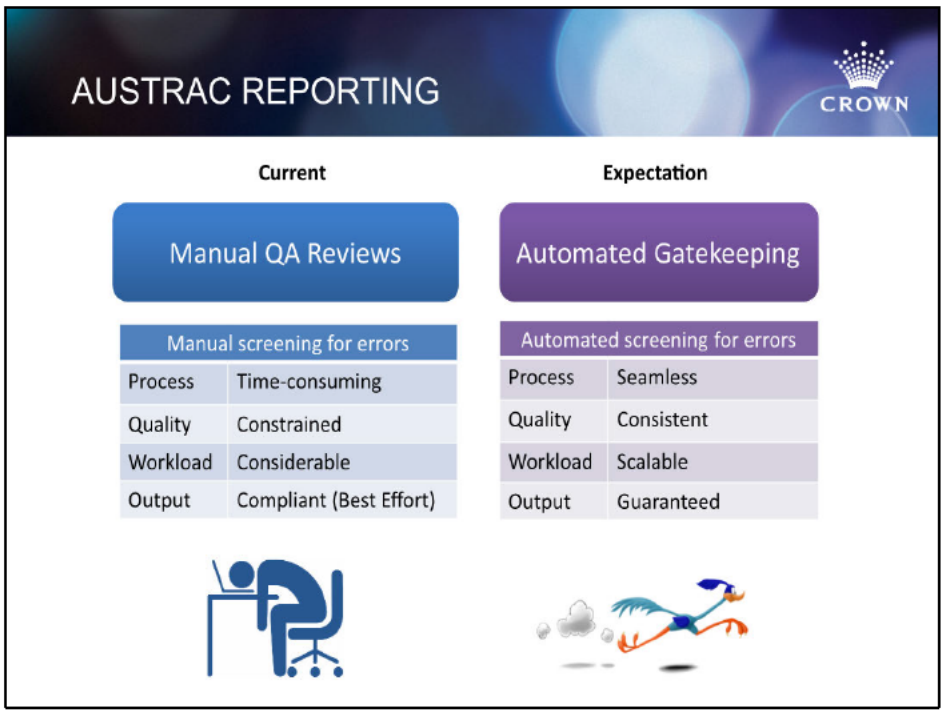
# AML Sentinel Program

## Executive Brief

August 2018

# BACKGROUND

- Regulatory recommendations and environment
- Overview of Crown Melbourne's compliant AML/CTF Program – in particular, reporting and how we monitor transactions of customers, services and patrons
- Opportunities through automation:
  - use of software for quality assurance in reporting ('the gate')
  - real time transaction monitoring, informed by the existing compliant program
  - auditable documentation of investigative work and actions

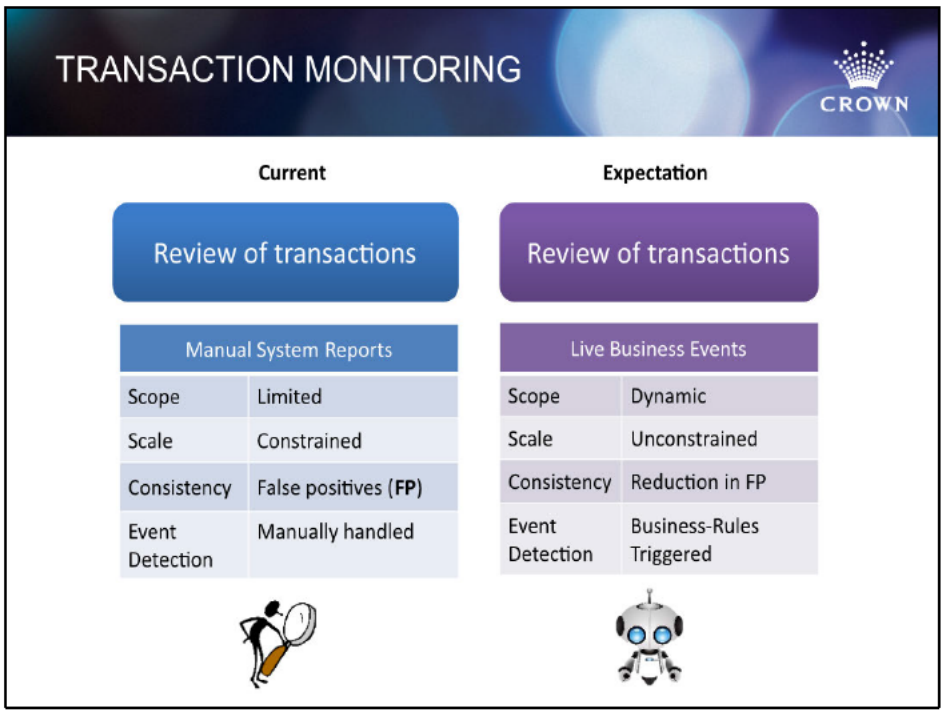



This slide addresses the manner in which Crown Melbourne conducts QA on information uploaded to AUSTRAC (threshold transactions, IFTIs, SMRs). This quality assurance is manual, with each transaction considered and reviewed to ensure the information is correct, at both the Cage and then again by the AML team, with identified errors either corrected or redirected back to the Cage for correction.

These errors may be an input error, or the result of historical population of data [TTR example with PO Box].

The use of an IT 'gate', which screens the contemplated data (the XML to be uploaded to AUSTRAC) against known errors in advance of upload (which each known "error" a business rule run against the data) gives further assurance to the business that all checks are run to ensure the quality of our reporting.

The gate **does not replace the review by staff** but rather is a tool to allow known errors to be identified in real time, for actioning by staff.




The current transaction monitoring program reviews identified customers and/or transactions included on daily or otherwise scheduled reports. These reports focus on various transactions including but not limited to: threshold transactions, gaming cheques, funds transfers (including an external party), funds transfers (between patrons), uncarded and carded buy-ins, alerted customers.

The identified customers / transactions listed on these reports are then considered by the AML team – with each identified customer or transaction type then reviewed by the AML team with reference to data we hold (for instance, customer behavior, rated play, win/loss, changes in average bet, etc).

Additional reports are considered by the AML team on a less regular basis (for example, gaming trends).

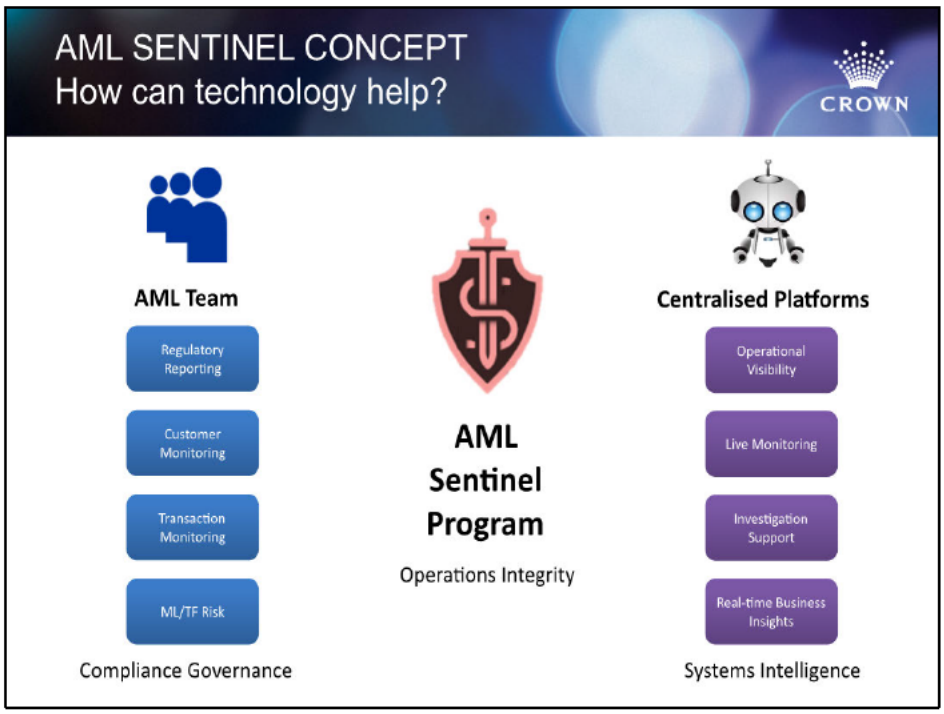
The existing compliant program may be enhanced through the use of technology to document the existing manual rules we run over the data when detecting potential suspicious behavior – that is, the review of the AML compliance team – into set business rules. This then creates 'events' for further investigation, which is then documented in a case management system (in lieu of hard copy ticks and crosses filed with the AML team). These events can be created in close to real time, to then be actioned immediately the following day by the AML team and/or highlighted to relevant business teams through alerts in close to real time (for example, table behavior and TG / Surveillance / Security).

The purpose of documenting the rules identifying potential suspicious activity is that this

then will assist in removing potential false positive results, and will therefore allow additional 'triggers' to be included in the program on a daily basis (where they might otherwise be a trigger scheduled for a less regular review under the Program).

It also documents the existing IP, aligns to the identified ML/TF risks identified in our AML/CTF program, and allows for expeditious reporting to senior management.

**Importantly, a more focused set of reports from SYCO can be obtained outside of the AML Sentinel proposal. This has been seen with the targeted EGM/ETG reports**. However, such reports are constrained by the existing framework and as such, are not live, and do not allow for alert triggers to set business areas.

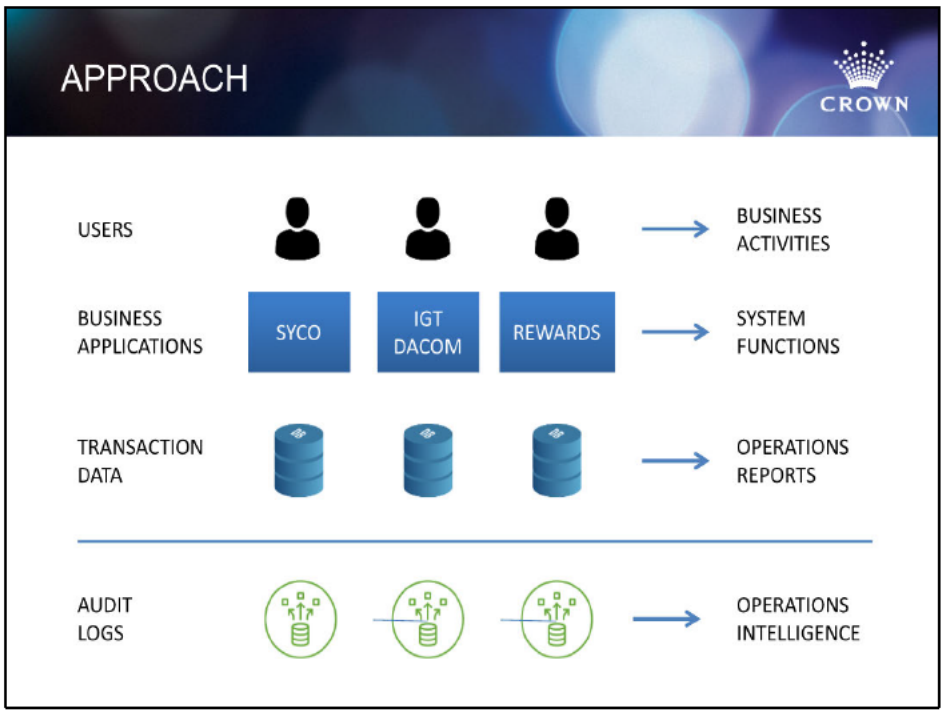



The AML team today manually follow a number of key practices to ensure Compliance, including through ensuring ongoing compliance with its AML/CTF Program. The manual program includes – from a monitoring perspective – the review of key reports generated from SYCO and DACOM.

On the other side of the spectrum, Centralised Platforms were launched 6 months ago. With these four key principles in mind as a support service to the business generally.

# PROGRAM CRITERIA

- Operationally non-disruptive
- Complements existing practices
- Leverage existing data, platforms & technology
- AML IP retention & reduction of key person risk
- Scalable and expandable platform
- Integrated case management




This is our existing ecosystem, since the beginning of time.

We have users who interact with a number of systems to perform Business functions. The transactions are stored in the databases, where we run reports from.

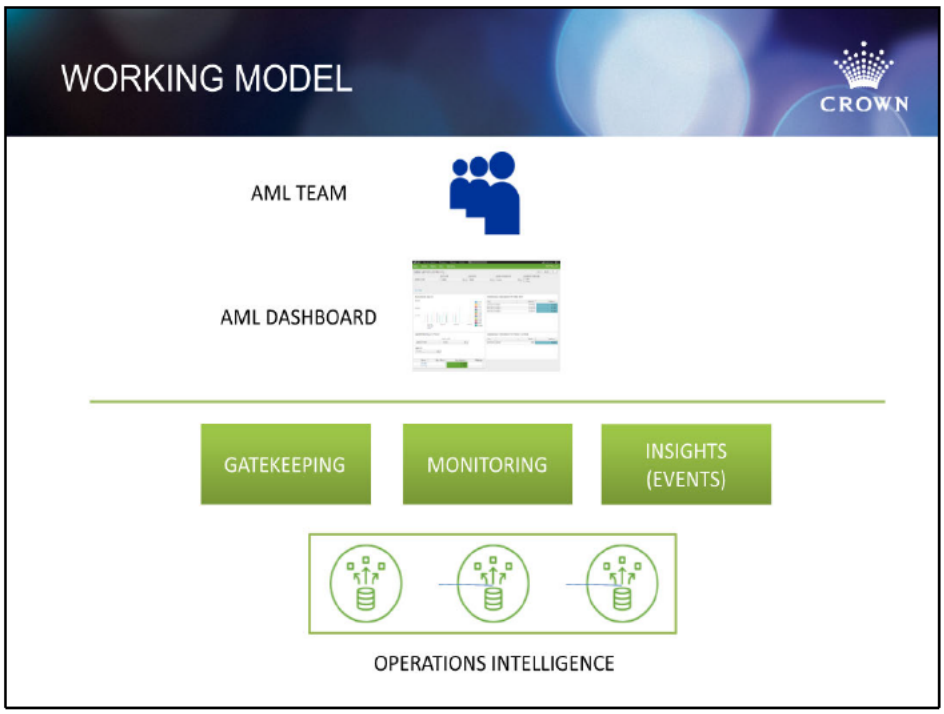
A new practice introduced in the ecosystem has an impact to Operations, whether it's intended or as a consequence.

So we need to dig deeper. And this is where Machine data comes in.

Machine data is a digital record that gets created when machines talk to each other. Most of our systems have been generating this data for years. But it's use has traditionally been limited to troubleshooting System outages. For example, machine data can tell us why did Syco went down yesterday, how can we prevent it moving forward.

In addition to that information, it also tracks Business activity. An example is a Syco audit log, that captures every buy in on a Table as it happens on the floor. Another example is the slots audit log, that's tracking every ticket in and out from a machine in real time. These are valuable Operational insights, that have never been utilised to it's full potential.

And that's the key to the Approach.



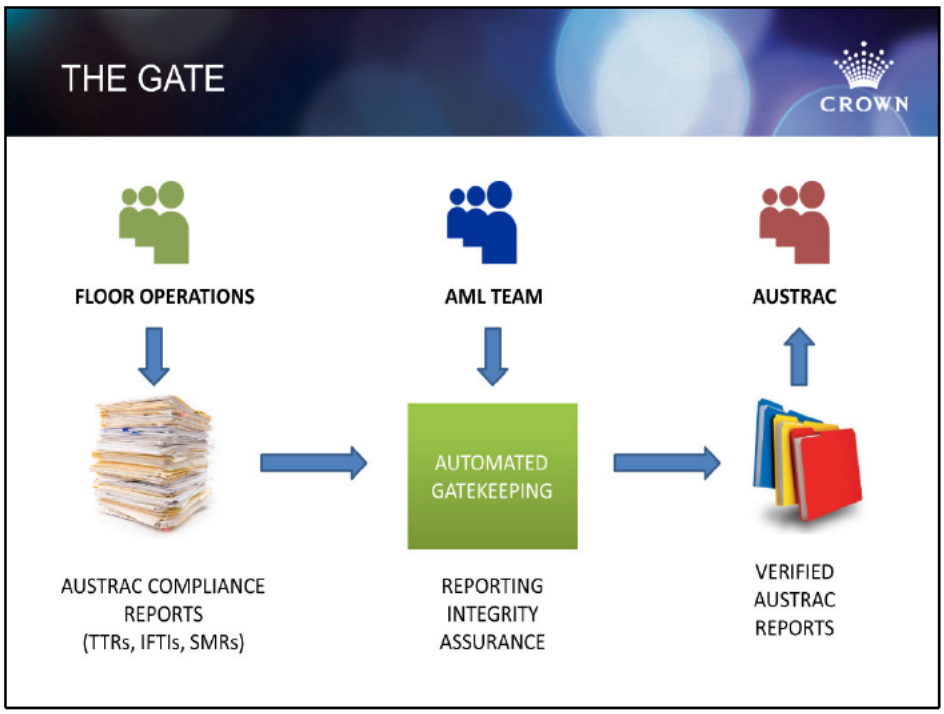

So how do we leverage this data to provide Operations Intelligence?

Plan is to deliver it in the form of three key AML functions:

1) Gatekeeping – Will help provide data quality checks on our Reporting commitments to AUSTRAC.
2) Monitoring – Is about observing certain "transactional" behaviours in real-time
3) Insights / Events – Are the Alerts that the Sentinel will bring to the team's attention

PRESENTER NOTE: Not necessary to go into details, if the three Functions have already been explained on Slides 3, 4 & 5.

And the AML team will consume it all via interactive dashboards, available on their desktop or mobile phones.




So how do we leverage this data to provide Operations Intelligence?

Plan is to deliver it in the form of three key AML functions:

1) Gatekeeping – Will help provide data quality checks on our Reporting commitments to AUSTRAC.
2) Monitoring – Is about observing certain "transactional" behaviours in real-time
3) Insights / Events – Are the Alerts that the Sentinel will bring to the team's attention

PRESENTER NOTE: Not necessary to go into details, if the three Functions have already been explained on Slides 3, 4 & 5.

And the AML team will consume it all via interactive dashboards, available on their desktop or mobile phones.


We will take a look at the TTR Validation dashboard to begin with.

This dashboard allows us a pick a file. These files contains transactions that are beyond the threshold we send across to AUSTRAC.

Before we do that, let's screen the file to ensure the data quality is up to the standard the Regulator expects from us.

Within seconds, the dashboard will scan the file and report any exceptions.

Select 1801, and walk through the PO Box and Middle Initial issues.

.....

.....

Now let's look at the Transaction Monitoring dashboard.

This dashboard allows us to monitor any Carded or uncarded buy in's on a Table b/w $5 & $10K. For someone who's trying to fly under the radar.

Walk through couple of tall buildings. Followed by "Carded Patron Buy in Activity".