

**System design Overview**

**Version 1.3**

**CONFIDENTIAL**

By accepting this document from Driftworks, or from your advisor or other agent, you accept that the information contained herein is the confidential property of Driftworks Limited. It has been released to you and your advisors as an introduction to **compliance team** for the purpose of assessing an investment opportunity in Compliance Team and you agree not to copy, share or make public any of the content herein, or to use part or whole of this document for any other purposes.

**content**

1. General description
2. Security & APIs
3. User logon
4. To do list & compliance diary
5. Core system - Principal point solutions and pieces of functionality
   1. Compliance document resource
   2. Compliance Monitoring
   3. Building compliance audits
   4. Delegating and scheduling compliance controls
   5. Managing compliance templates
   6. Enterprise Risk Register
   7. Compliance training
   8. Reporting
   9. Business continuity/crisis/disaster action plan (to be added later)
   10. other operational functionality (divert, tracking actions, audit trail of edits, data deletion and etc)
6. Infrastructure
7. Visual appeal and ease of use

note on terms

- Content; refers to compliance information, documents and processes provided on the system to manage compliance

- Data; refers to information inputted into the system to evidence compliance

- Controls/questions; these terms are used in an interchangeable way.

##### Introduction

# Compliance Team is a unique software as a service (SaaS) based compliance business that provides compliance content, advice, support, monitoring and training. This document describes the functionality of the software required to provide this service to clients.

The software is a platform that tracks and monitors policy and process documentation, and evidences the activities undertaken to deliver against same. It enables the compliance officer to automate the monitoring processes, have real-time visibility, and deliver reports

The simplicity and visual reporting capabilities of this product are key to it's user acceptance and success.

##### 1. general description

This system enables organisations to demonstrate that they have completed due process regarding their regulatory obligations, and provides their boards with detailed oversight. It ultimately provides an evidence trail of activities and outcomes to ensure that the business is administered in line with the direction of the board and regulation. Much of this service will be driven by templates that are auto-updated for clients as appropriates.

It needs to deliver 8 core functions

1. host directives and documentation on regulation, corresponding legislation and guidelines from the respective regulators, and manage updates. Store policy and process documents and manage the review process
2. an audit trail of actions and events for the delivery of compliance obligations
3. risk management process and risk register
4. an API to enable integration with other systems and the management of data recieved
5. provide a video based training module
6. deliver a to-do list and compliance calendar
7. provide summary and detailed reporting
8. a robust security and data protection capability (ability to report and delete by data subject, psudonymisation ).

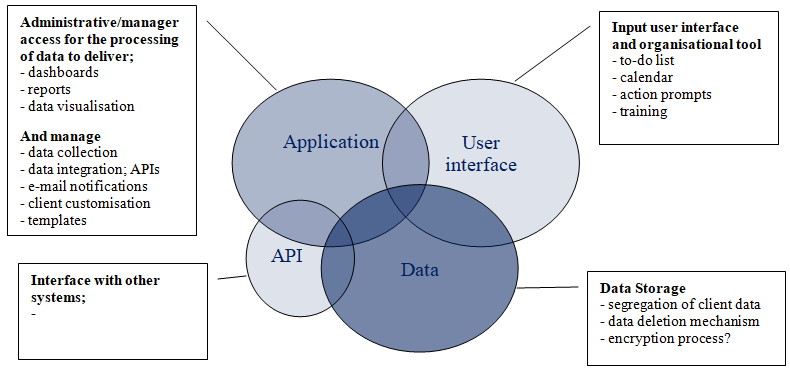
note; 2 and 5 are different uses of the same workflow application

There are four key factors which will make this software attractive to corporates;

* it is simple, intuitive and attractive to use - the user experience
* content is easily updated either through templates, or directly by the client or individually
* visual reports that are appealing and easily understood

This is primarily an oversight system that monitors on a monthly or other basis. It is to a degree a meta level application. It will integrate with other functional processes (e.g. 'Know your Client' or AML applications) that manage specific functions. We may build some of these ourselves in time.

It needs to be scalable, modular in design, facilitate interaction between the data in each module, and integrate with other specialist software.

****

##### 2. security & APIs

**Compliant with ISO & SSAE 16 standards including**

* Data/files encrypted on transition and in storage
* Multiple levels of user access; to edit, to view, to review and etc.,
* Segregation of individual client data from other client data
* Segregation of application and data databases
* Mechanism to manage the deletion of expired data
* Access to the to-do list will be more broadly used and links to this module will be forwarded to third parties. It would be good to take additional precautions with this module to mitigate against malicious access? i.e. segregate the collection and viewing of data from the data and application. Is this practical?

**User types;**

CT personnel

* System master - access to all aspects of the system,
* System Administration - restricted to certain administration aspects of the system, can access client accounts with access controlled and logged

Clients;

* System administration

**All users customisable**

**to grant access to**

- Audits

- Teams/groups

- View others

- Filtered views

* Manager user
* View only manager
* User - to do list and personal data

Consultant

* As client access plus;
* Ability to view a number of clients
* Ability to manage selected templates

Options for each category of user;

* Ability to create/edit/publish templates

**Logon**

Ideally a click through from this link would be mapped to a serial number (or another identifier) on the computer, and access be restricted to approved machines devices (just like WhatsApp)?

**APIs**

* inbound; Input of data or documents from third party systems to fields on the System i.e. auto completion of controls in the system
* outbound; Extraction of data or documents from fields on the system
* ready for connection to 10 top ERP/accounting systems, SAP, Oracle, ... and specialist industry specific ERP applications

**Stand alone**

some clients way wish to host their application on independent servers, or in their own environments. We need to bare this in mind. Issues with, support for system, system updates, and delivery of push content (i.e updates or templates)

**Access control**

There are two forms of access links to the system;

Temporary links; expire after a pre defined time e.g.40 days. - these are to the to to-do list module only

Permanent links; present to the logon facility of bypass it id permissioned to do so.

Client system functionality

* All links should have a person's name and other identifiers against them
* can produce reports against each name detailing the links that have been provided, status (active/expired) when last used.
* Administrators can remove/renew access

##### 3. user logon

A desktop icon from which a user can click through to the logon

Click to access this logon field

24 actions outstanding in 3 separate compliance modules

- turns red under certain conditions

user name ;

password ;

[client logo and text]

Enter

This section is to be greyed out, and the orange circle not made visible. All becomes visible upon a successful logon.



to-do list

system logon

... or directly to system if permissioned

**Other logon options -** all programmable per user per system. User name is typically the user's e-mail address.

* Click directly into the to-do list from a unique link delivered by e-mail,
  + This unique link will expire after a number of days (duration defined per system)
* Click form a button for a closed loop process e.g. Breach report, client on-boarding form or etc. this will typically be for an 'event' based audit

**Future functionality**

To do lists can be completed offline and synchronised when is broadband is available.

##### 4. to-do list & compliance diary

A users to-do list comprises of a list of all of the actions outstanding at that point in time for that particular user. It will comprise of actions from, 1/ the calendar, 2/ monitoring process, 3/ Authorisations awaiting approval, 4/ document reviews or /5 the actions process. This module also provides access to the compliance calendar and the main system (if they have that privilege)

* An individual's to-do list, history, actions and calendar will always appear in this module.
* To do list is prompted by e-mail and the orange circle
* This should be built to fill the whole browser page

Actions

compliance calendar

History

main system

to-do list

Settings

close



**John Doe**

**To-Do list**

[client logo]



Supplier Management - November 2017

AML - December 2017





Data Protection - December 2017

Section 1 - Review & Breach

1.2 Has the data subject agreed in writing for their information to be shared with sister organisations?

yes no



**Enter**

1.3 Are all review processes up to date?

yes no partially 25% partially 50% partially 75%



**Enter**

1.3.1 When will they be completed?

Enter date

**Enter**

1.3.1 Please comment?

**Enter**

**Enter All**

1.4 Have any breaches occurred during the last month?

yes no



**Enter**

1.5 Have there been communications (not including generic update information) from the regulator?

yes no



**Enter**



1.6 has the board reviewed and commented on the monthly GDPR report in accordance with policy

yes no



* Users land with the most recently issued to-do list of controls to the front and the rest loaded chronologically behind
* the current question has a blue bar beside it for ease of navigation.
* a completed question disappears from the to-do list when is scrolled off the page.
* the user may partially complete a question. Once submitted this will be stored, however the question will not disappear off the to-do list until the whole question is completed
* the page is to populate with sub questions pre-loaded (but hidden) so they will appear without delay if required.
* we need a visual indication of progression, bar and % probably
* N.B. this module will evolve the be the individuals daily compliance manager. It will organise and track daily/weekly activities and we need to be cognisant of the fact that there will be significant additional functionality added to it in time.

**History**

This will display all of the audits that the individual user has contributed to, and the dates/titles. To be viewed like this;

main to-do system top section

Data Protection - John.Doe@abcgroup.com

Jan 2017

Feb 2017

Dec 2016

all questions and responses here, including links to all uploaded documents

February's data here

Decembers data here

* The user can scroll up and down to view their responses, and right and left to view the same control over a number of months.
* the information shown will relate to the privileges of the user, i.e it may display others in the team if the user is privileged to see that information. User can filter by user or status.
* options to view the prime question only, or an expanded view with all sub questions
* If they click on a question they can see that question in it's entirety in a separate pop box.
* the user can edit the response if they are partitioned to do so. They will need a re-set button for this function. reset settings; on/off and on timer e.g. for 20 mins after the question was initially completed. An audit trail is maintained for all changes.

**Settings for the to-do list;**

This enables the individual user to select customisation options to their personal to-do lists

* Auto enter upon completion of all questions (with the exception of the open text field). Default to on.

**Compliance Calendar**

A visual compliance diary for user to view events that are relevant to their work

* includes data provided by CT, consultants, client company or the user
* includes reminders and validation of licenses/certificate renewals, and actions due.
* all data to be sorted by compliance type. an event may be connected to multiple compliance types. Can also sort by people, functions or teams
* calendars are created separately to the user, typically for a department, and users see the entries relevant to their position. Users in groups can be set to see each others' personal entries.
* the user needs to be able to mark the event as done/partial/not-done, and to add a comment. They also need to be able to 'star' certain events
* Events can be sorted by done/partially/not-done/star.
* displayed by day, week, month, quarter, next 7 [variable] days and etc.
* the diary is to be opened in a separate window.
* option to include actions/events in the to-do-list

Is there a simple way of synchronising with outlook, google, sap, oracle and other commonly used diary systems?

**Actions**

This is a module where an individual can create an action and allocate it to an individual or team. Actions are delivered through the to-do list and prompts for the to-do list are delivered by e-mail. E-mail prompts have a link that lands the user on the Actions part of the to-do list.

Actions include;

* Recording the creator of the action,
* Allocate responsibility for this action, and if a group, who takes primary responsibility.
* Enter the action (plain text)
* A due date, and a capacity for creator to extend the due date or to permission the recipient to extend the date
* Each action can have footnotes
* Each action can have a level of importance
* Actions can be connected to a compliance control (question), compliance type, or diary event, or all. This is optional and is set by the action creator. This facilitates filtering.
* Reporting on actions, and can be filtered by user, group, function, footnote entry
* Actions can be filtered in the to-do list by the user to bunch actions. E.G. all AML actions together.
* viewing action - in a format that can be filtered and deliver reports.

Screen to generate an action typically looks like this;

drop box of users on the system

Originator; Joe.bloggs@abc.com

**Actions**



V

Owner; johnjones@abc.com

text

thumbnail

upload file

Go

Attach to audit

25/10/2018

due by

Send reminder

V

e-mail

notify by by

V

Red

priority

Edit

Post

Attach the action to one or more of

- department/group

- Audit (label eg AML - December 2016)

- a control

e-mail text

one or more of;

- e-mail immediately

- to do list

- calendar

Red - high

Amber - medium

Green - low

send

**to-do list settings**

settings can be set by group or by user

Notifications - General

* send when triggered
* send at 9.00am [variable] when new material arrives
* do not notify
* remind of un answered for more then 10 [variable] days
* show on desktop icon and on tab in browser
* turn button red on

- authorisation awaiting approval

- action waiting

* Authorisation awaiting approval - notify

- immediately

- hourly

- daily

- none

##### 5. core compliance system

A user will have access to different aspects of the system in line with their settings e.g. a credit controller may have access to the calendar, relevant docs, their own actions, and the regulation and credit-check aspects of resource.

##### 5.1 - dashboard





Client logo

**Calendar**

**Risk Reg**

**Resource**

**Dashboard**

**Audits**

Help

Settings

**Actions**

**Other**

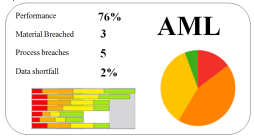
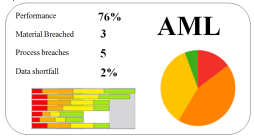
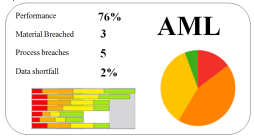
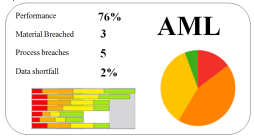
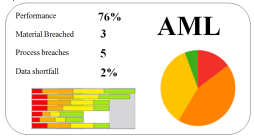
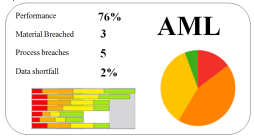
my to-do

**User; John.Doe@abc.com**

End of last month

to

Most recent



Material Breaches & important upcoming events

Risk Profile

* the dashboard is the default home page.
* The dashboard is primarily a view of other reports generated by the system, all displayed on a single sheet
* The system needs to be able to deliver a number of dashboard formats, and store them as templates as the system grows. These can be built over time as the market lets us know what is needed per industry, but the flexibility to do this must be built in the first instance. We aim to have a suite of standard templates
* All dashboards can be customised to a max of 20 (or more depending on practical restraints) items.

##### 5.2 - calendar

The calendar will appear in a separate window as described in the 'to-do' section above. the content of the diary will correlate to the users permissions.

##### 5.3 - compliance documents

There are three categories of documents in the system;

* The document store; Client compliance documents e.g. policies and procedures and other documents of the organisation. Some template docs and template videos also held here.
* Resources; Regulatory documents e.g. directives, legislation, guidelines & etc
* Data; documents uploaded by the user as part of the compliance validation process.

**The document store;**

* filed by compliance type & subset, or other hierarchy designed for the client
* review docs with an audit trail of the process, The review process to be delivered through the to-do list or calendar.
* attach docs to compliance controls and the compliance calendar
* store of historical versions of documents,
* store all forms of media docs, excel, pdf, video and etc.

Client logo

**Calendar**

**Risk Reg**

**Resource**

**Dashboard**

**Audits**

Help

Settings

**Actions**

**Other**

my to-do

**User; John.Doe@abc.com**

documents accessed from a section of the help facility, a section of the Resource section, or a link from a control or action, as appropriate.

an option under 'Other' to view/manage policy and process documents

We are relatively open on the design of this module. There are many open source designs available today and it would be good to build upon one of them.

##### 5.4 - compliance monitoring

This comprises of three distinct elements

1. Managing compliance documents (described above)
2. Information collected from officers or responsible persons
3. Information fed to the system through an API

**b) compliance collected by CT**

Information comes from actions and calendar items (covered above), and from compliance controls. This section describes the generation of audits and of compliance controls (questions).

The system manages audits which comprises of a series of questions (a mini workflow;- the result of the prime question dictating what the sub questions should be). The outcomes are scored.

**User; John.Doe@abc.com**

my to-do

Settings

Help

Client logo

**Other**

**Actions**

**Audits**

**Dashboard**

**Resource**

**Risk Reg**

**Calendar**

List of audits in the selected section displayed here

Example below;

List of audits in the selected section displayed here

listing to include;

**manage**

**New**

directory

sections and subsections

- minimise/

expand to side



Manage directory

new audit

audit name

Edit

Actions

copy

compliance score

AML - Jersey



Another 66%

Another 30%

AML - Jersey 79%

click on the bar to view this audit in the grid view, or click one of the other buttons for other actions

Actions relating to this audit

* The user can see audits that they have been permissioned to view
* audits, sections and questions and sub questions can be dragged and dropped in new locations
* audits sections and questions and sub questions can be copied (control click and drag)

Creating a new audit

* press the 'new' button, and land in the 'edit' section of a new audit
* the user will be asked the audit name and for individuals with viewing privileges (can be edited later)
* and for the title to the first section
* tick for a master template if this is to be a master template and if so, tick for the type; time or event based.
* if this is to be a copy of a template, select from a menu of templates available to this system.
* is a risk profile to be completed in this audit monthly/quarterly and etc
* the user is ready to start creating controls (questions).

Creating/editing questions

The workflow - A prime question can have a number of sub questions, each of which is triggered on the outcome of the prime question. The outcome can in turn generate a further sub questions. The overall score of the question will be represented as green (compliant), Amber (partially compliant) or red (non compliant). All questions are scored.

Each question will be configured at the time of creation to;

* One of eight types; 'yes/no', 'yes/no/partial25%/50%/75%', 'single choice', 'multiple choice', 'enter date', 'enter number' 'upload file' and 'text'.
* Each type can have the option to be set to have a 'Not Applicable' response.
* Each type can be set as a video question; i.e. present a video, and following the completion of the video ask the prime question. This facilitates training. There needs to be a facility to set an option for a timeline for the completion of questions e.g. 10 mins to complete.

**Prime Question**

**(one of 8 types)**

**Sub question**

**(one of 8 types)**

**Sub question + 1**

**(one of 2 types)**

**resulting in one of the following outcomes**

compliant

partially compliant 75%

partially compliant 50%

partially compliant 25%

non-compliant

not applicable

or, unanswered

Triggers on the outcome of the prime question

triggers on the outcome of a sub question with either

- A request for a comment

- a link to create an action

* Questions can be allocated a 'star' status. This title can be set by the client. this allows us to differentiate between material and non material outcomes

one of 9 options;

yes/no (default)

yes/no/partial

single choice

multiple choice

enter date

enter number

Video

text

upload file

For **prime questions only**

This question triggers on the outcome of another question or the performance of an audit

For **sub questions only**

This question triggers on the selected outcome(s) of the prime questions

The setup page will look like this;

content of an information button attached ot the question. It can contain a file(s), and if so, the file can be represented as a thumbnail

Outcome =

=

Follow-on outcome

on

on

**Create/Edit question**



Compliant

Compliant

V

Non-Compliant

V

no

V

Compliant

V

yes

V

Question type

yes/no

Triggers on

Compliant

non compliant

partially compliant

not-applicable

Question text

Information

thumbnail

upload file

Dependency

dependent on occurrence

Footnote

Star

Star on NC only

Video format

Allow non-applicable

Always compliant

Weighting

V

Comment text

Actions

0

1

2

3

4

5

6

7

8

9

10

V

Add Subquestion

Delete Question

mechanism to attach docs and specify if they are to appear as thumbnails

one of 6 options;

complaint

partially compliant 25%

partially compliant 50%

partially compliant 75%

non-compliant

not applicable

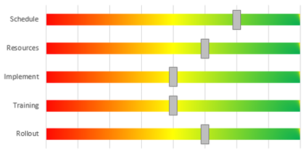
Generates a comment field subject to the outcome of this question

Simply presents an option to the user to generate an action. it is preloaded with the users name and attached to this control. the user has the option to decline to create an action

A footnote can be added to each question. The system can perform searches by the content of this field

* Completed questions have one of six outcomes;

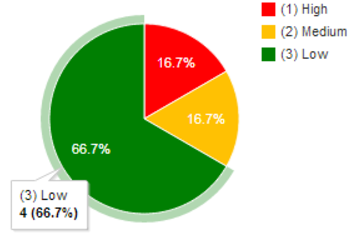
Compliant in Green

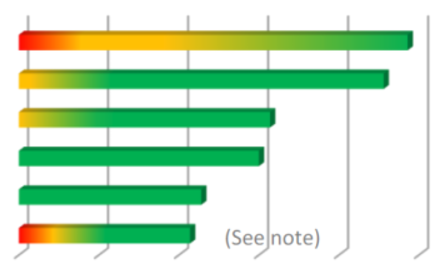
Partially compliant 25/50/75% in Amber

non compliant in Red

not applicable in Grey

Unanswered in Yellow





* The wording of these outcomes should be soft programmable e.g instead of compliant a word like 'approved' or 'low risk' may suite the sense of the application
* Each sub question, depending on it's outcome, has the option to enforce a comment, and/or an action
* Prime questions can be configured to appear subject to the outcome of a previous question.
* Each prime question has a default timing associated with it; no timing, once only; weekly, monthly and etc. This is also displayed in the right hand corner of the footnote
* Each prime question must have a unique tag (enables templating and updates; the question could be in a different place in different systems and etc)
* Ability to add exposed narrative, images or video to questions

Most audits will be monitored over time i.e monthly, quarterly, annually and etc. Others will be event based e.g. breached, client on boarding, training and etc.

Event based audits

Each client system needs to be able to generate a link that will enable a new 'column' and

* Allow an individual (or group) to generate an event. They can fill in the title, e-mail address of the recipient and a timeout duration. This duration will need to have a facility to be extended if need be. e.g for on-boarding of clients or job applications. This is e-mailed to the recipient through the system. or
* facilitate auto creation - a user can press a button and it will auto-generate an event and allow the user to fill in the title and recipients e-mail address. A link will be sent to this address to enter the to-do list. This needs to be subject to an administrator controlled timeout. e.g job applications on an intranet, or reporting a compliance breach
* facilitate incognito event generation to enable a 'whistleblower' function
* Events can also have info boxes and footnotes attached.
* Events can have pseudonames (to protect the identity of the subject) with protected information only available with higher security processes e.g. name, address, PPS no. phone number, ethnicity and DOB segregated.

Scoring questions

* Each outcome is scored, - and displayed on a coloured heatmap grid
  + red - non material non-compliance 0
  + amber - partially compliant .5 (or .25/.75 as applicable)
  + green - compliant 1
  + grey - not-applicable 0
  + yellow - unanswered 0
* Each question can be weighted 0 to 10, to differentiate importance. The outcome multiplied by the weighting provides the overall score for the individual question
* This enables a weighted score to apply to each section, period/event or audit

Deletion of questions

if there is no data, deliver a prompt to confirm the wish to delete

if there is data, deliver a prompt including the names of the contributors and

* have permission to delete
* generate a requirement for authorisation (this will appear in the to-do list of the authorised individual)

There may be a requirement to preserve the data. The authorised person needs to specify the number of months at time of authorisation.

Allocating / un-allocating questions to users

all controls need to be scheduled for users and/or draw information from an API.

The default timing is set in the question and may be changed for the individual

The controls are presented for completion in the to-do list

Controls may be un-allocated from an individual but the historical data always survives

**c) Information collected through other systems - API**

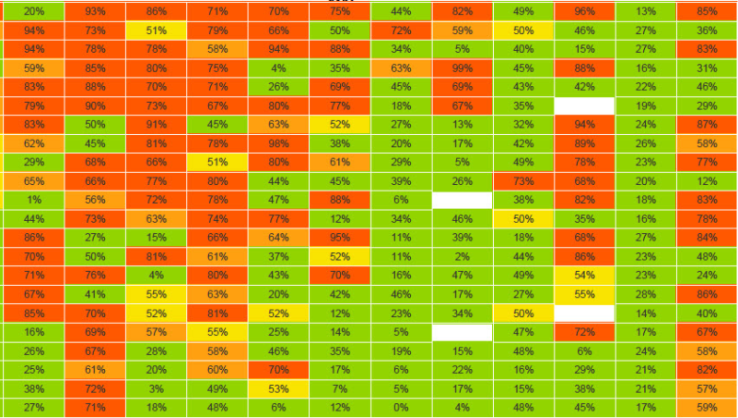
There needs to be a mechanism to integrate data collected elsewhere directly into CT. The expectation is to limit this functionality to;

* information that can be auto fed into a data field on the system,
* the information will be held independently of the other systems data and a bespoke report provided. This will be custom built each time.

**Displaying outcomes**

Grid - image and explanation

* filters of this information can be exported to excel



more detail to follow

graphic reports

Bar, pye, line and scatter graphs at a minimum. The capacity to display a selection of data (selected off the grid). It would be great to offer a wide selection of highly visual outputs.

note; this has a high impact on the sale-ability of the software.

* All graphics should nave an 'export to Excel' button in the corner

bespoke

The system needs to be designed to cater for the individual requirements of a client and have the ability to additional graphical representations of the data on a case by case basis.

##### 5.5 - creating and updating compliance templates

The core to the delivery of the CT service is the ability to deliver and update of compliance templates. There are three types of templates

1. Compliance audits
2. Calendar entries
3. Documents

**Compliance template Audits**

Each audit comprises of a number of questions that need to be responded to. Some are 'time based' e.g AML is tracked monthly, and others are 'event based', e.g. on-boarding of clients, or breach recording.

The master template differs from regular audits in the following ways;

* for simplicity, Each question (the prime, subs) in a template question are locked to the template i.e. may not be changed by the end client, however the client may add additional questions to that audit to customise for their purposes.
* each question will have a unique identifier. the enables a question to be in position 2.3 in one client's audit and 2.8 in another's.
* all compliance templates will be set up as 'time based' or 'event based' formats in the first instance. Time dependent questions will default to a monthly format, however may be changed by the client (weekly, quarterly, annually and etc)

The Master template is created by a category of user authorised to manage master audits

**Compliance template Updates**

Users with permission can make changes to the master template.

* has a button to publish changes. Only users authorised to publish can publish
* changes will be transmitted to the administrator of the client system, where they can see they changes and accept or decline individual changes. They can view the control in it's entirety prior to acceptance.
* an audit trail of all changes accepted/declined is maintained on the client system
* the client system administrator can view all unaccepted updates and opt to accept at a later point
* the impact of the change will only take effect on the client system from the time of acceptance, i.e. they will not act retrospectively

**Compliance calendar template**

CT will have a suite of calendar events.

* each event can be categorised, e.g. AML. KYC, Data Protection and etc
* selected categories are made available to client systems
* the individual user will have the entries for selected compliance types inserted in their compliance diary.

**Document Templates**

Regulatory and other template documents. All updates to this content will be approved by the allocated administrator and an audit trail of versioning will be maintained.

* where a document is attached to a question or event, the original document will remain with all historical items and all new items from the time of the update will contain the updated version.

##### 5.6 - Enterprise risk register

A standard risk register structure (sample in appendix II)

* Link certain fields to the outcome of audit/calendar activities
* Deliver consolidated reports from multiple registers
* deliver summary detail in dashboard

See youtube clip here https: //www.youtube.com/watch?v=1RIWTocFBvk , (SectetPM project risk register) this can be purchased for €20. It gives you the base macros for this process.

This will be perfect except,

* Facilitate once off risks situations e.g Server upgrades, or perpetual risk, e.g liquidity, fraud and etc.
* we need filters to produce the scatter and bar charts by multiple filters (category, sub-category, risk type, risk owner, top 10, risk changes since last report and etc. These are for a point in time, or displayed as performance over a period of time.
* Issue prompts through to-do list and calendar
* Record a comment against changes in risk scores.
* Link risks to compliance report outcomes and graphs
* enable auto completion of risk rating by using an 'mitigation effectiveness factor' that can be fed from elsewhere in the system. Option for Risk Officer to approve or decline and record comment on that decision
* Store all monthly/quarterly reviews in a user friendly way
* All views and reports to exportable to Excel.
* Capacity for user to make amendments (where technically easy) to this structure to customise for their own application

##### 5.7 - Resource

**Resource**

this module is to include

- Training

- Regulatory docs

- Credit check tool

- AML check tool

- Documentation templates

Regulatory docs include; up to date regulation, legislation and guidelines for individual jurisdictions. EU and US initially

##### 5.8 - other functionality

**divert (temporary diversions)**

an ability to divert responsibilities of a user to another over a period of time. The audit trail will need to show the initial; owner of an action and the new party. Typically these will be between two defined dates (to cater for holidays, maternity leave and etc)

**Audit trail**

An audit trail needs to be maintained of

* changes to regulatory documentation (policies and etc)
* changes to data

**Versioning**

* System - this is a hosted service and all users are to be on the same version
* Controls/question - a complete time stamped history is to be maintained of all changes. N.B. changes to the content only become applicable from the next point of delegation, i.e. all historical date is to be scored against the then current controls.

**System generated notification e-mails**

The system needs to be able to send e-mail

* messaging to deliver links to to-do lists, authorisation requests, reminders, reports and other items that need to be delivered to users.
* messages to be taken off a series of standard and client generated templates e.g. initial requests for information and reminders will be worded differently

**Filtering data**

This will typically be managed from the grid view.

* there should be a capability to select filtered views of data from each audit and to deliver reports. this data to be filtered by;
  + outcome - colour; i.e. compliant, non compliant and etc
  + date
  + person
  + category
  + footnote
* select by highlighting a section of the grid, or by defining these parameters manually
* filters display on the grid, or in any of the reporting formats in the system
* a capability to show 'most recent' reports e.g. set once as last 3 months and it will always show this result.
* ability to name, save and edit a filter
* ability to provide a 'permission to view' to an individual based on a filter

**Data deletion**

There is a requirement in regulation to be able to delete data from a system (right to be forgotten) we will need a process whereby data associated with

* a time period,
* a file type,
* Audit type
* a person
* an organisation

can be deleted. There will need to be real visibility of what is being deleted and the deletion approval process. If it is related to a person or client organisation, there will need to be an authorisation process.

This process also needs to include deletion from backups and other distributed locations.

Data destruction and validation;

* There needs to be a permissioning process for the deletion of data
* An audit trail of deletions needs to be maintained
* Deleted data should be recoverable for a period of time by the client system administrator, and a further period of time by CT administration. Both of these timelines to be set by client in advance.
* Capacity to deliver a system generated certificate of destruction to include;
  1. The data description (audit, section, control/action number, individuals who inputted the data, date that the request for information as generated, date of initial input and last input).
  2. Who requested the deletion
  3. who approved the deletion
  4. Deletion status. one of
     1. Has been irrevocably destroyed
     2. Has been deleted from the client system and is recoverable through CT for the next 30 (or another number) days.
* Certificates of destruction to be customisable for individual client. They will contain the information above, but the client can customise the text, look and feel around it.
* A record of all destruction approvals and certificates to be maintained

**Other**

Other pieces of functionality

* reminders
* data archiving
* ability to provide a status to data 'restricted status' for personal data - cannot be viewed, used in a process or changed. GDPR clause 67
* attach documents to questions
* export cuts of information to Excel or CSV - and to pivot the view.
* Whistleblower functionality - only a nominated person will know the identity of this individual in the first instance
* Ability to Watermark & add CT generated text to reports - so as we can apply them to non-paying systems.

**Future functionality**

1. Meeting Management - attendees, reminders, minutes, documents, actions and etc
2. Text messaging - for access and notifications
3. Attach directly to a scanner for volume input of documents
4. Ability to record if a page has been screenshot'ed. - it will help to keep e-exams honest.
5. A desktop app for the to-do list to enable offline functionality

##### 6 - Infrastructure

**The big issues**

* data security
* data destruction
* Segregation of databases
* segregation of customer data
* stability
* Java on MySQL?

**Links/barriers between data**

links that need to be created between audits in a client's system

* Between the data and outcomes of one audit to another
* Controls and RR
* Controls/RR and reports

system

links between master and slave template documents audits, and the audit trail of same.

barriers

control to ensure that separate client systems never get vision of each others data

**Client billing**

Clients may be billed in various ways, per audit, per uses, per 'once off'' user, or other user metrics.

We need to be conscious that we may need to be able to collect this data for billing purposes

##### 7 - Visual appeal & ease of use

This is a client facing application. It needs to look good, be functionally robust, and be more desirable to use than our competitors.

* hover labelling - all icons and headings to have hover time delayed explanations
* click and drag - where possible, the ability to click and drag (or control click and drag to copy) folders, files, audits, questions and sub questions
* titles on buttons and controls editable along with the 'hover over' explanations. This enables multiple languages and client customisation

Appendix I - Infrastructure diagram

**Administrative/manager access for the processing of data to deliver;**

- dashboards

- reports

- data visualisation

**And manage**

- data collection

- data integration; APIs

- e-mail notifications

- client customisation

- templates

**Input user interface and organisational tool**

- to-do list

- calendar

- action prompts

- training

**Interface with other systems;**

-

**Data Storage**

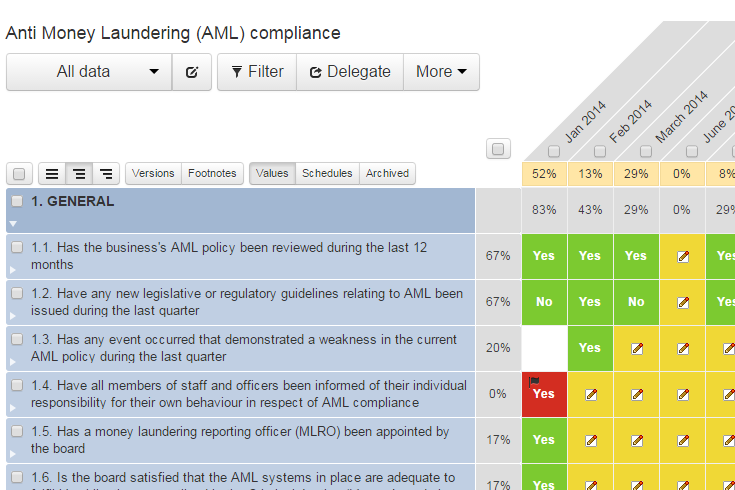
- segregation of client data

- data deletion mechanism

- encryption process?

Appendix II - images for conceptual purposes only, we need to adapt this to deliver our own unique visualisation experience

**The Grid** - a view of the sections, questions, scoring, and the colour coded compliance outcomes

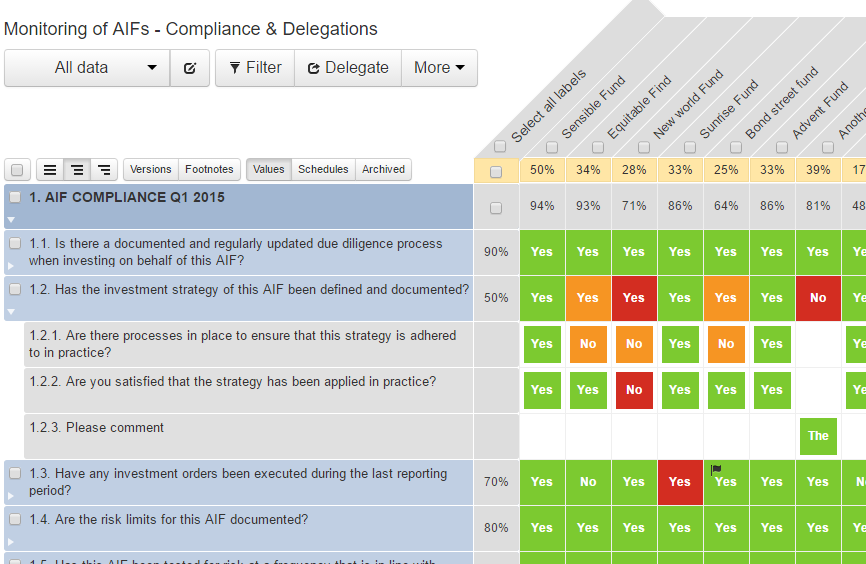


Time based audit

Event or item based audit

Composite scores for this item

Section scores

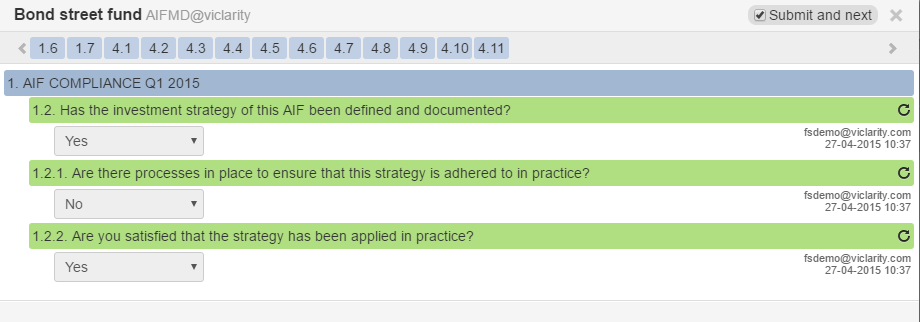


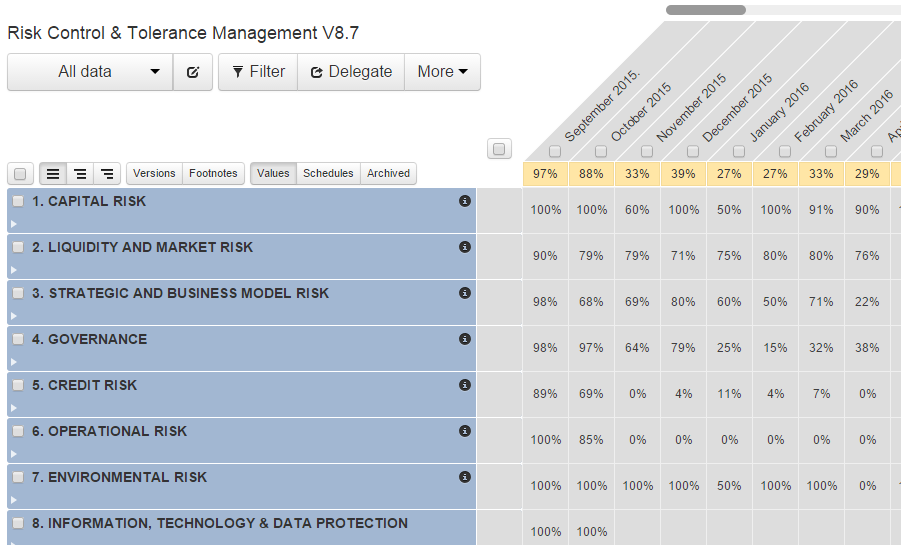
Question expanded to show sub questions and the their outcomes

Response to question displayed, and a 'hover over' will display the owner, time of completion, and the fill answered

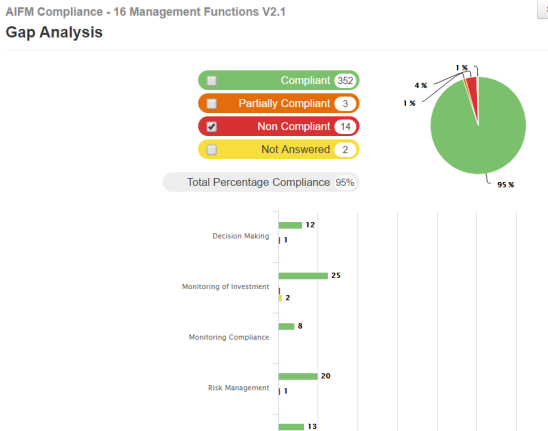
Flag identifies an action attached to this control

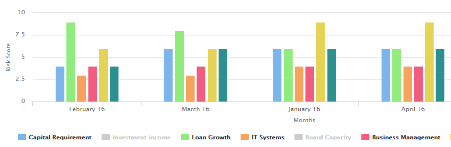
click to view full derail of this control





Grid collapsed to show sections and scores only





Appendix III - comment

user adoption and behaviour

- compliance - 'if it is not in Compliance Team it does not exist'

Team objectives and real transparency results in better engagement and outcomes