BARNOWL

BarnOwl COBIT / NIST Overview

Table of Contents

1. Introduction

This document provides a high level overview of how BarnOwl can be populated with any process, risk, control, and control test structure. We use COBIT and NIST as examples in this document.

- BarnOwl is able to import any 'process>sub-process> risk> control>control test' structure from Excel provided it is in the BarnOwl specified format.
- The data (objectives, risks, controls, audit procedures & tests) is imported into the BarnOwl process library.
- The process library (with all its data) can then be published (applied) to the relevant business unit/s by an administrator. In addition, the data in the process library is searchable and can be copied by users when capturing data in their business unit.
- As per BarnOwl's standard risk functionality, the relevant risk & control owners (and administrators) within each business unit can:
    - rate the risks (qualitative impact and likelihood and / or quantitative values)
    - rate the controls (adequacy and effectiveness)
    - capture remedial action plans with due date and owner/s
    - capture and / or integrate (with 3rd party data analytics) key indicators including the specifying of thresholds and rules which trigger a re-assessment of the related object; the object being Objective/s (Key Performance Indicators (KPIs) linked to objective/s), Risk/s (Key Risk Indicators (KRIs) linked to risk/s) and Control/s (Key Control Indicators (KCIs) linked to control/s)
    - capture contributing factors (with associated controls if required) and consequences of the risk
    - send out risk and control self-assessments (voting) automatically to specified users
    - send out pre-configured surveys, checklists and questionnaires
    - capture incidents against a business unit and / or directly against a risk in the business unit. A client can define different types of incident registers with 'user-defined' fields per type of register. Typical incident registers include: loss events, forensics, findings, gifts register, burglaries / robberies, tip offs, allegations, conflict of interest etc. In addition, action plans can be captured against incidents driving the automated follow-up of incidents.
- The BarnOwl reporting module provides built-in reporting, advanced Power BI dashboard reporting and tabular type SSRS reporting. BarnOwl's Power BI dashboards and SSRS reports can be customised on a quotation basis.

2. Importing data using BarnOwl's excel import template

You can capture (directly into the system) and / or import data from Excel in BarnOwl's template.

FIG2a Example of COBIT in BarnOwl's Excel import template:

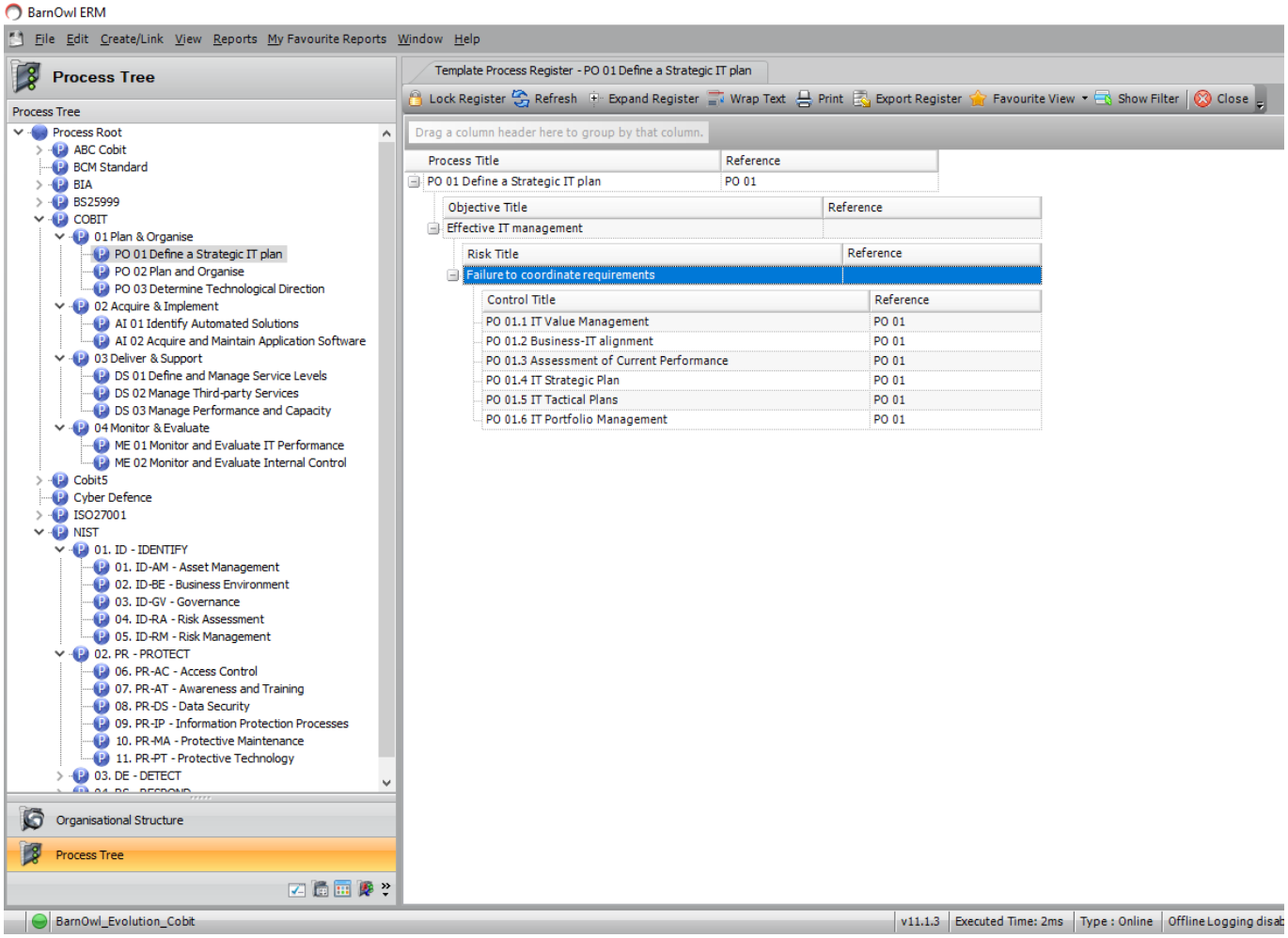
Process Name	Sub Process Name	Risk Title	Risk Category	Risk Subcategory	Risk Reference	Control Title	Control Reference	Control Procedure	Audit Test Title
01.EDM - Evaluate, Direct and Monitor	01.EDM01 - Ensured Governance Framework Setting and Maintenance	01. IT Risk - IT Governance	IT Risk	01 - IT Governance Framework Setting and Maintenance		01. EDM01.01 - Evaluate the governance system		01. EDM01.01 -Continually identify and engage with the enterprise's stakeholders, document an understanding of the requirements, and evaluate the current and future design of governance of enterprise I&T.	01. EDM01.01.Q2. Determine the significance of I&T and its role with respect to the business.
01.EDM - Evaluate, Direct and Monitor	01.EDM01 - Ensured Governance Framework Setting and Maintenance	01. IT Risk - IT Governance	IT Risk	01 - IT Governance Framework Setting and Maintenance		01. EDM01.01 - Evaluate the governance system		01. EDM01.01 -Continually identify and engage with the enterprise's stakeholders, document an understanding of the requirements, and evaluate the current and future design of governance of enterprise I&T.	01. EDM01.01.Q3. Consider external regulations, laws and contractual obligations and determine how they should be applied within the governance of enterprise I&T.
01.EDM - Evaluate, Direct and Monitor	01.EDM01 - Ensured Governance Framework Setting and Maintenance	01. IT Risk - IT Governance	IT Risk	01 - IT Governance Framework Setting and Maintenance		01. EDM01.01 - Evaluate the governance system		01. EDM01.01 -Continually identify and engage with the enterprise's stakeholders, document an understanding of the requirements, and evaluate the current and future design of governance of enterprise I&T.	01. EDM01.01.Q4. Determine the implications of the overall enterprise control environment with regard to I&T.
01.EDM - Evaluate, Direct and Monitor	01.EDM01 - Ensured Governance Framework Setting and Maintenance	01. IT Risk - IT Governance	IT Risk	01 - IT Governance Framework Setting and Maintenance		01. EDM01.01 - Evaluate the governance system		01. EDM01.01 -Continually identify and engage with the enterprise's stakeholders, document an understanding of the requirements, and evaluate the current and future design of governance of enterprise I&T.	01. EDM01.01.Q5. Align the ethical use and processing of information and its impact on society, the natural environment, and internal and external stakeholder interests with the enterprise's direction, goals and objectives.
01.EDM - Evaluate, Direct and Monitor	01.EDM01 - Ensured Governance Framework Setting and Maintenance	01. IT Risk - IT Governance	IT Risk	01 - IT Governance Framework Setting and Maintenance		01. EDM01.01 - Evaluate the governance system		01. EDM01.01 -Continually identify and engage with the enterprise's stakeholders, document an understanding of the requirements, and evaluate the current and future design of governance of enterprise I&T.	01. EDM01.01.Q6. Articulate principles that will guide the design of governance and decision making of I&T.
01.EDM - Evaluate, Direct and Monitor	01.EDM01 - Ensured Governance Framework Setting and Maintenance	01. IT Risk - IT Governance	IT Risk	01 - IT Governance Framework Setting and Maintenance		01. EDM01.01 - Evaluate the governance system		01. EDM01.01 -Continually identify and engage with the enterprise's stakeholders, document an understanding of the requirements, and evaluate the current and future design of	01. EDM01.01.Q1. 7. Determine the optimal decision-making model for I&T.

FIG2b: Example of NIST in BarnOwl's import template

Process Name	Sub Process Name	Risk Title	Risk Category	Risk Subcategory	Risk Reference	Control Title	Control Reference	Audit Test Title
01. ID - IDENTIFY	01. ID-AM - Asset Management	01. Cyber Risk - Asset Management	Cyber Risk	01. Asset Management		01. ID-AM.1 Physical devices and systems within the organization are inventoried		01. ID.AM-1.Q1 - Are the physical devices and systems within the organisation identified and listed in an asset register in accordance to their importance? When, How
01. ID - IDENTIFY	01. ID-AM - Asset Management	01. Cyber Risk - Asset Management	Cyber Risk	01. Asset Management		02. ID-AM.2 Software platforms and applications within the organization are inventoried		01. ID.AM-2.Q1 - Are software platforms and applications within the organisation identified and listed in an asset register in accordance to their importance? When, How
01. ID - IDENTIFY	01. ID-AM - Asset Management	01. Cyber Risk - Asset Management	Cyber Risk	01. Asset Management		03. ID-AM.3 Organizational communication and data flows are mapped		01. ID.AM-3.Q1 - Is sensitive & or confidential data tracked over the organisational, with the aim of identifying critical assets that could potentially be vulnerable to exploitations.
01. ID - IDENTIFY	01. ID-AM - Asset Management	01. Cyber Risk - Asset Management	Cyber Risk	01. Asset Management		03. ID-AM.3 Organizational communication and data flows are mapped		02. ID.AM-3.Q2 - Are there formal transfer policies, procedures and controls in place to protect the transfer of information using all types of communication facilities
01. ID - IDENTIFY	01. ID-AM - Asset Management	01. Cyber Risk - Asset Management	Cyber Risk	01. Asset Management		04. ID-AM.4 External information systems are catalogued		01. ID.AM-4.Q1 - Does organisation / Department outsource any IT / OT or security functions to third-party service providers? If so, who are they, what do they do, and what type of access do they have?
01. ID - IDENTIFY	01. ID-AM - Asset Management	01. Cyber Risk - Asset Management	Cyber Risk	01. Asset Management		04. ID-AM.4 External information systems are catalogued		02. ID.AM-4.Q2 - Are security practises applied to off-site assets considering the different risks of working outside the organisation's premises.
01. ID - IDENTIFY	01. ID-AM - Asset Management	01. Cyber Risk - Asset Management	Cyber Risk	01. Asset Management		05. ID-AM.5 Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value		01. ID.AM-5.Q1 - Are there policies governing the classification of information assets (Confidential, Sensitive, Public). Is information classified in terms of legal (Regulatory, Contractual), value, criticality and sensitivity to unauthorised disclosure or modification.
01. ID - IDENTIFY	01. ID-AM - Asset Management	01. Cyber Risk - Asset Management	Cyber Risk	01. Asset Management		06. ID-AM.6 Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established		01. ID.AM-6.Q1 - Are all the information security responsibilities related to the classification of the information defined and allocated
01. ID - IDENTIFY	02. ID-BE - Business Environment	02. Cyber Risk - Business Environment	Cyber Risk	02. Business Environment		01. ID-BE.1 The organization's role in the supply chain is identified and communicated		01. ID.BE-1.Q1 - Does the organization protect itself against supply chain threats by employing defined list of measures to protect against supply chain threats as part of a comprehensive, defense-in-breadth information security strategy?
01. ID - IDENTIFY	02. ID-BE - Business Environment	02. Cyber Risk - Business Environment	Cyber Risk	02. Business Environment		01. ID-BE.1 The organization's role in the supply chain is identified and communicated		02. ID.BE-1.Q2 - Do agreements with suppliers include requirements to address the information security risks associated with information and communications technology services and product supply chain.
01. ID - IDENTIFY	02. ID-BE - Business Environment	02. Cyber Risk - Business Environment	Cyber Risk	02. Business Environment		01. ID-BE.1 The organization's role in the supply chain is identified and communicated		03. ID.BE-1.Q3 - Does the organisations regularly monitor, review and audit supplier service delivery.
01. ID - IDENTIFY	02. ID-BE - Business Environment	02. Cyber Risk - Business Environment	Cyber Risk	02. Business Environment		02. ID-BE.2 The organization's place in critical infrastructure and its industry sector is identified and communicated		01. ID.BE-2.Q1 - Is there a general awareness of the IT strategy and a clear assignment of accountability for delivery?

3. Data is imported into BarnOwl's process library

FIG3a: Imported COBIT processes showing Process>Sub-process>Objective>Risk>Control/s:



4. Applying / synchronising processes to your organisational structure

An administrator can decide which processes, risks and controls to apply (publish) to your organisation business unit/s. The applied risks and controls now become business unit specific in terms of ratings and ownership:

FIG4a: Select which processes, sub processes, risks and controls you wish to apply (publish) to your organisation

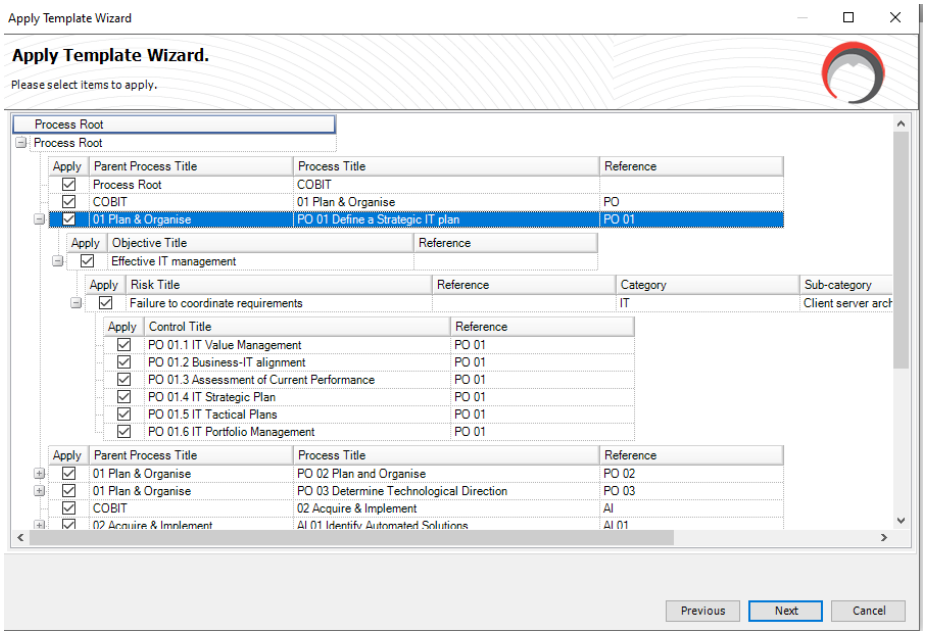
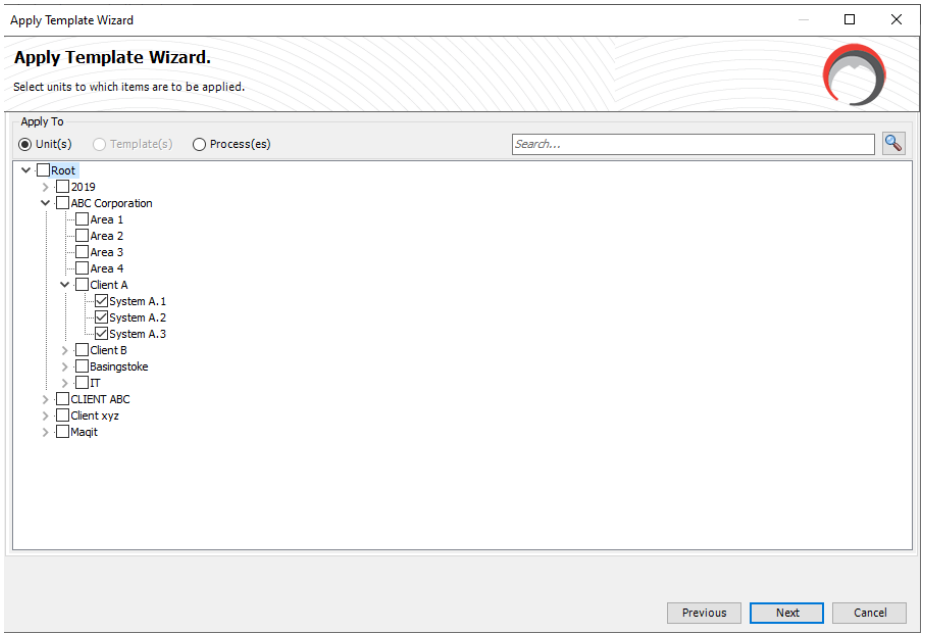


FIG4a: Select the relevant business unit/s the process will be applied to:



You can view which processes have been applied to which business units as well as synchronise any updated processes to the previously applied business units:

FIG4c: View which processes have been applied (published) to which business unit/s in your organisation

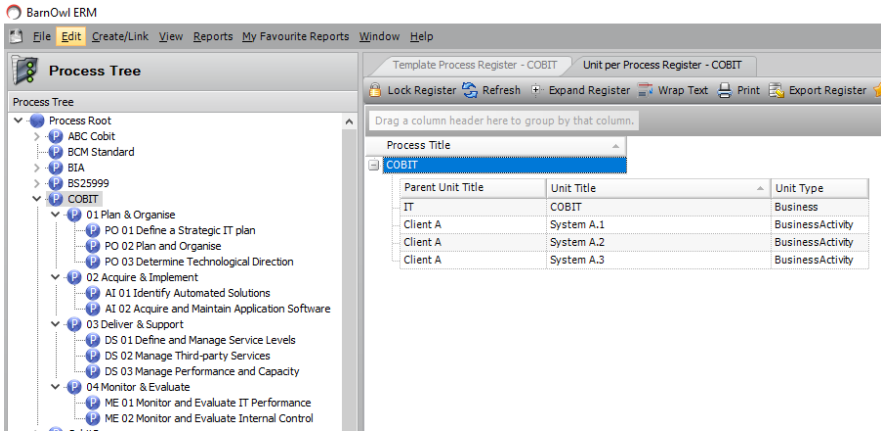
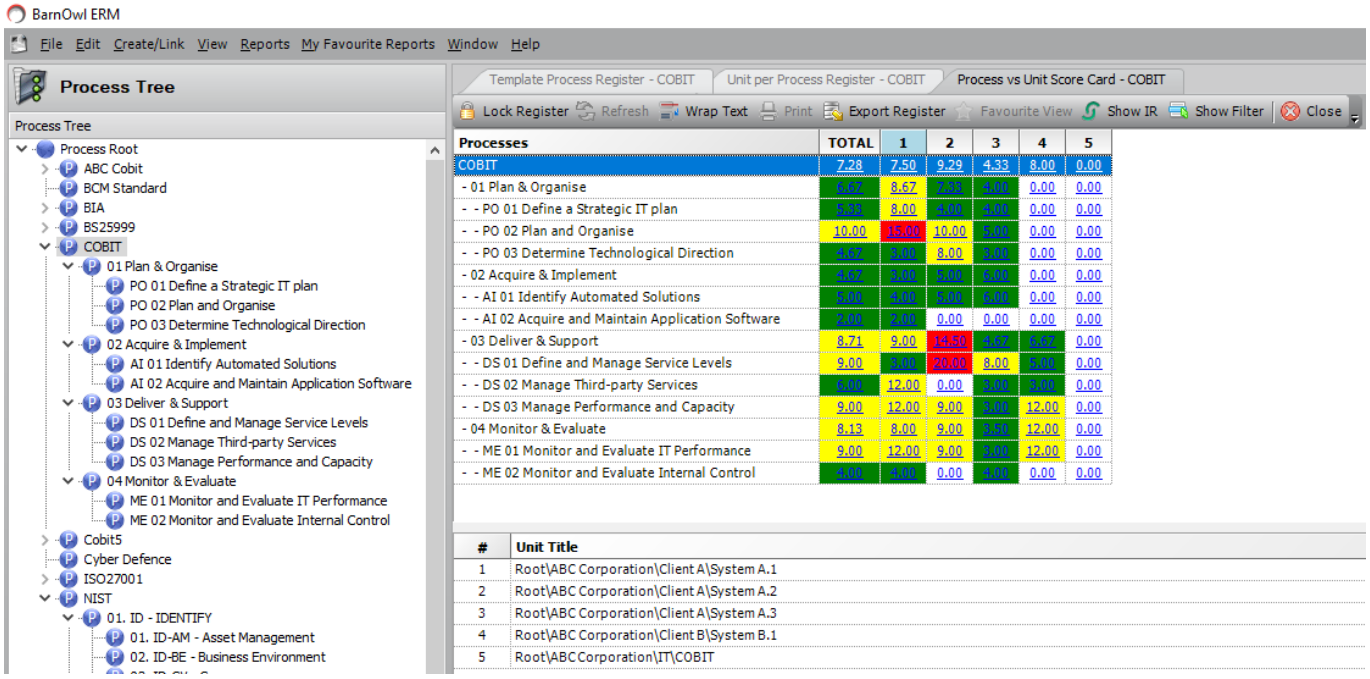


FIG4d: View your aggregated (average) risk rating by process (rows) by business unit (columns)



5. View / Rate your risks and controls in the BarnOwl web app

FIG5a: Example of a COBIT risk register

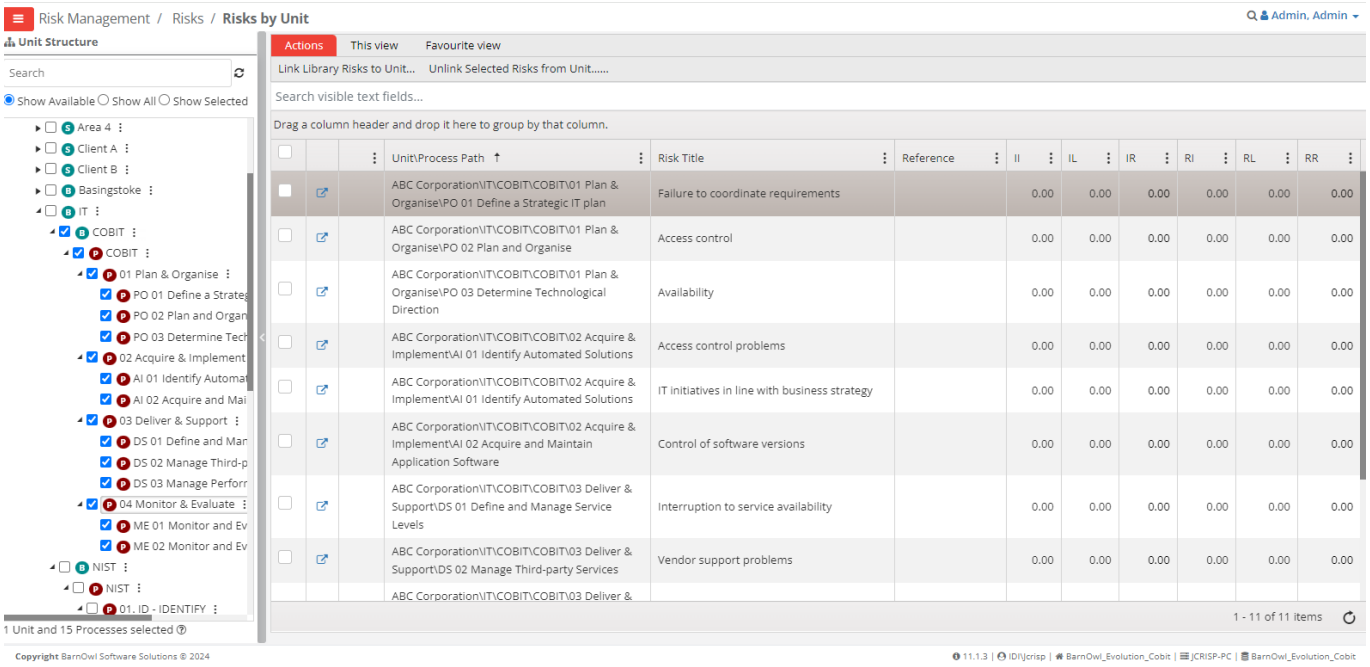


FIG5b: Example of a NIST risk register

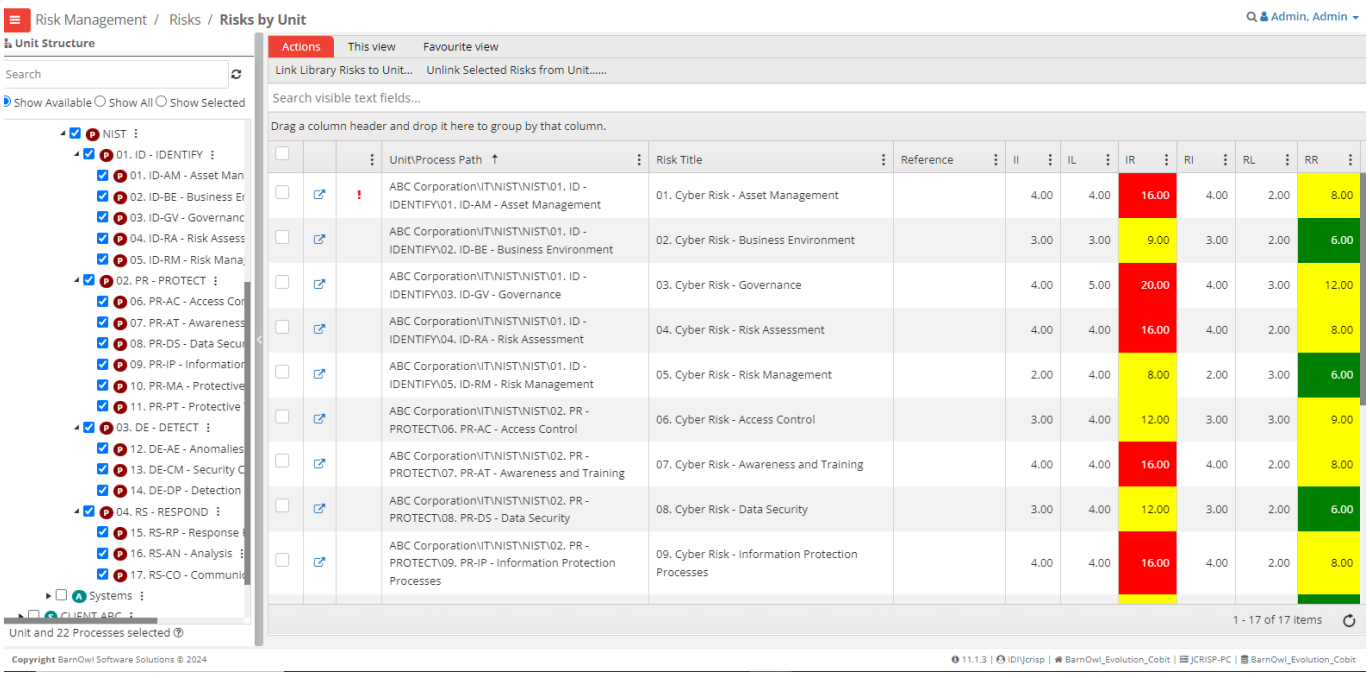
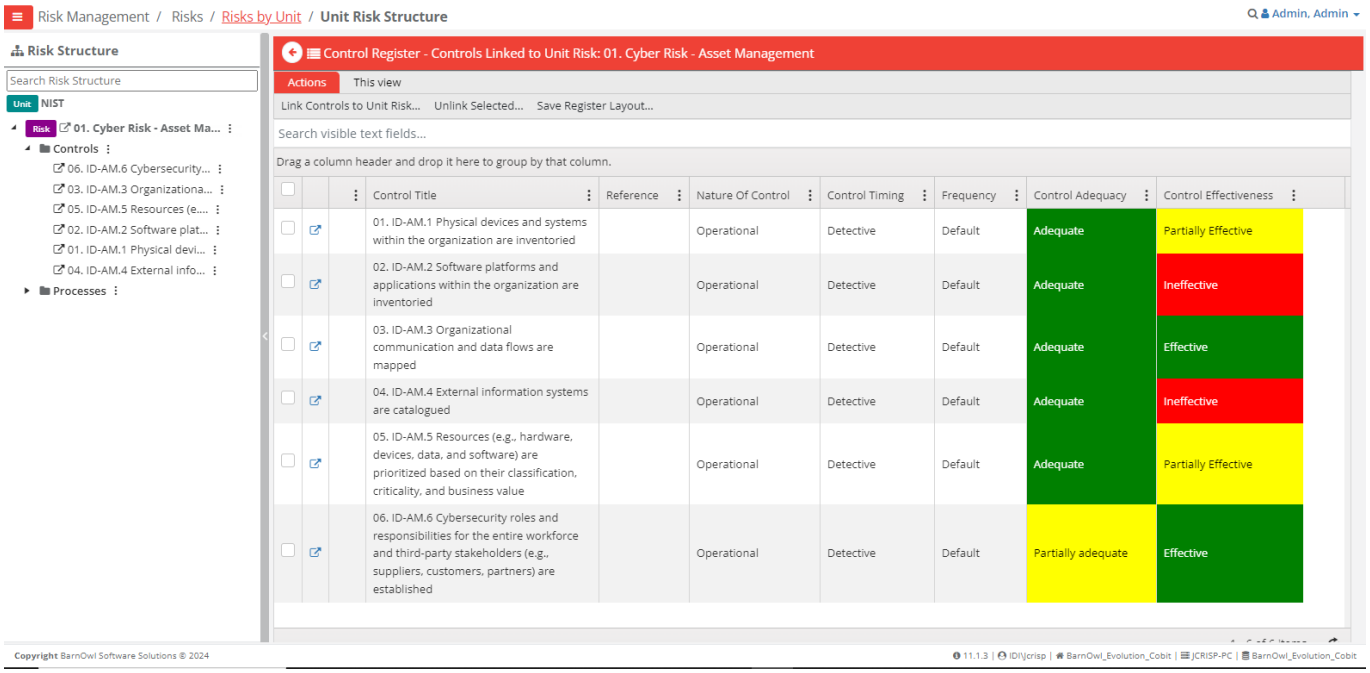


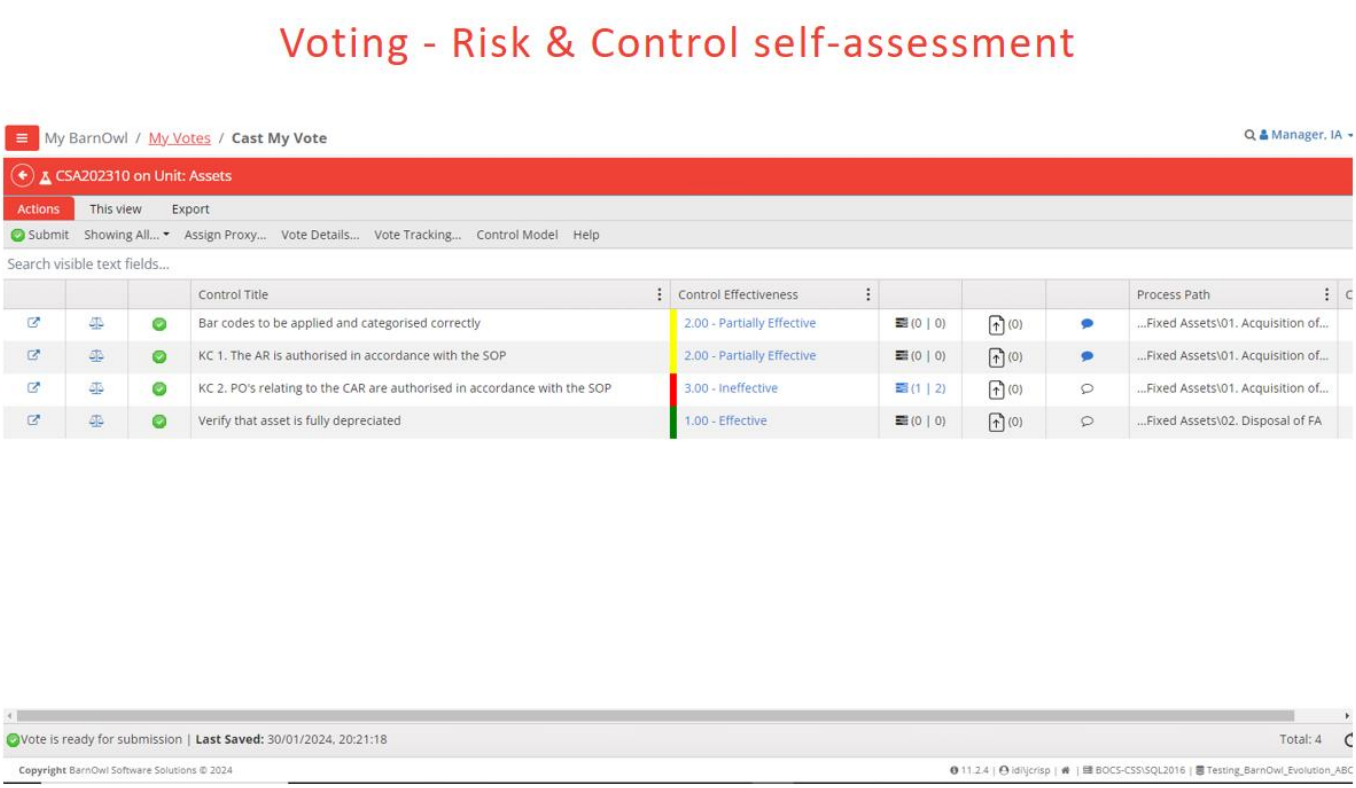
FIG5c: Risk on a page for '01. Cyber Risk - Asset Management' showing linked controls



6. Risk and Control self-assessments

It's very easy to send out automated RCSA's to the relevant respondents (e.g. risk / control owners) for them to rate their risks and controls (once off or recurring).

FIG6a: An example of a CSA (control self-assessment)



7. Reporting

BarnOwl provides many standard Power BI dashboards with extensive drill down and drill through capability. Simply click on the 'refresh' button in Power BI to get the latest up to date data from the system:

FIG7a: Risk dashboard

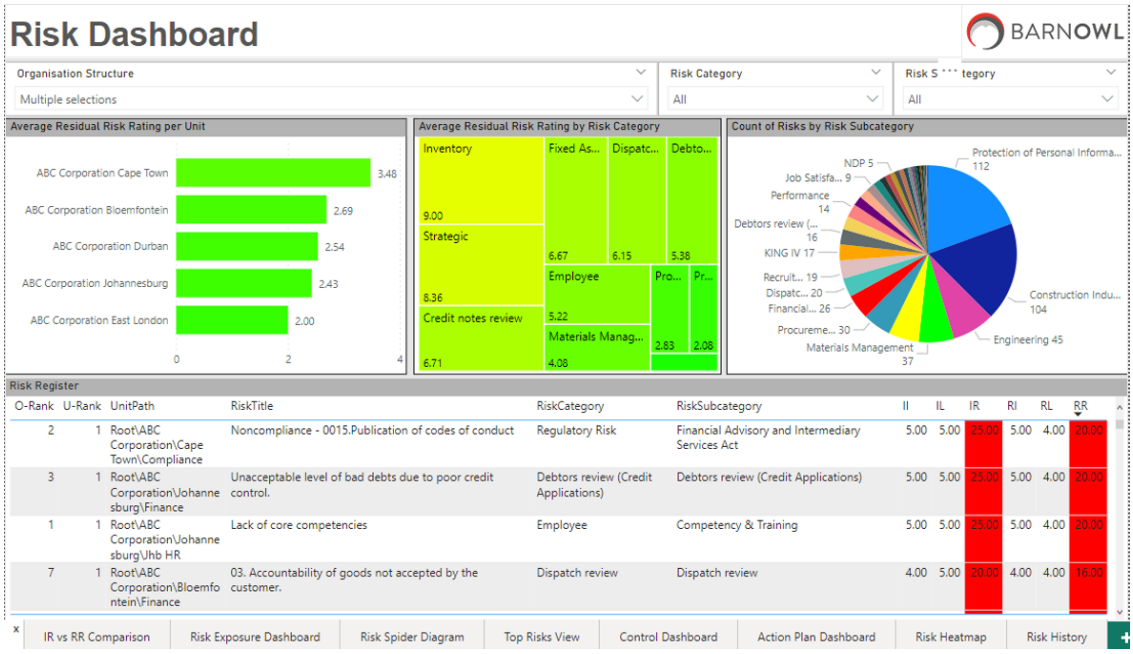


FIG7b: Risk heat map

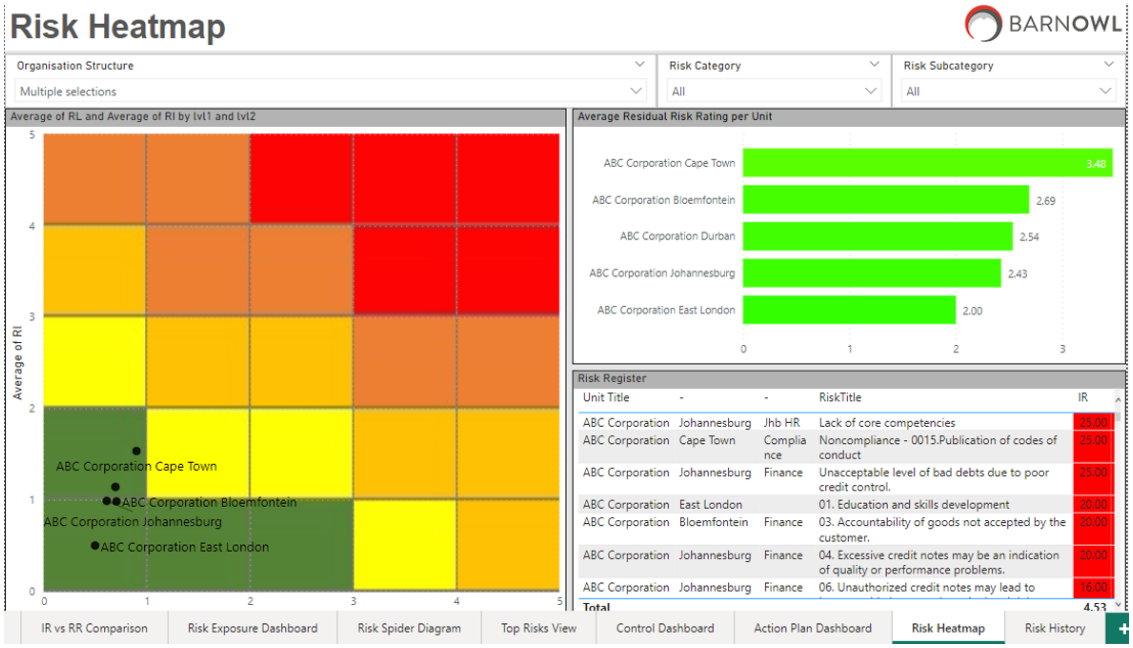


FIG7c: Risk trend dashboard

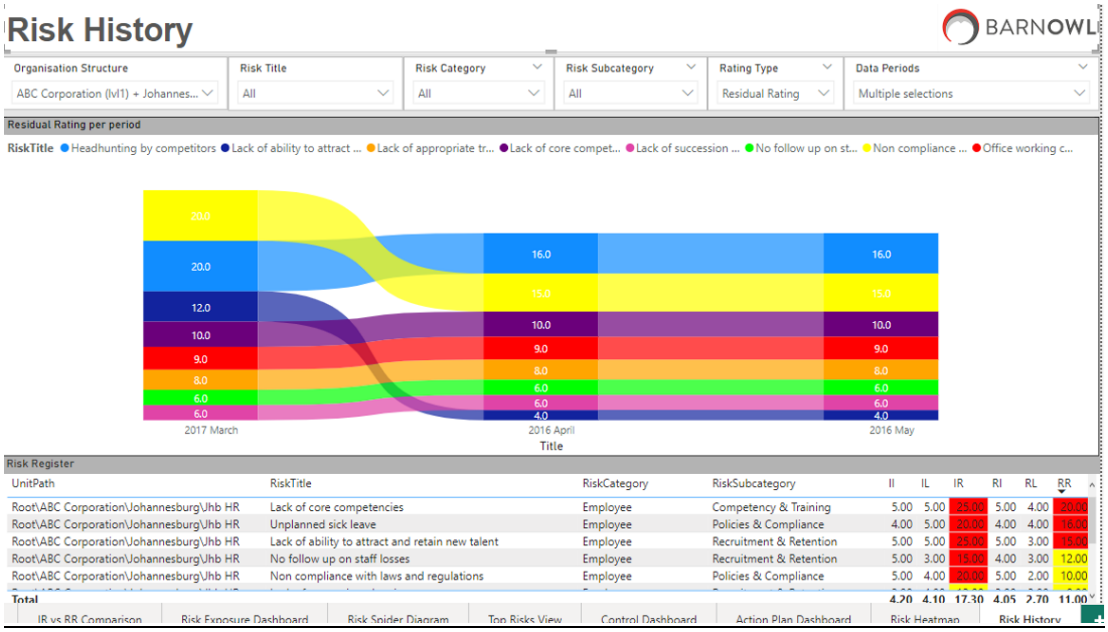


FIG7d: Control trend dashboard