Management of Risk Process Pathway

2019

Senior Responsible Owner	P Flaherty, CEO	July 2019
Author	P Pursley, Strategic Risk Manager	June 2019
Quality Assurance	Strategic Risk Management Group Governance Board	August 2019 September 2019
Final copy signed-off	Senior Leadership Team	1st October 2019
Adopted into the business	Cabinet	December 2019

Management of Risk – Process Pathway

Main Principles

The Management of Risk processes shall be structured to include:

- **Risk identification and assessment;** of risks to determine and prioritise how the risks should be managed;
- **Risk treatment;** the selection, design and implementation of options that support achievement of intended outcomes and manage risks to an acceptable level;
- **Risk monitoring**; the design and operation of integrated, insightful and informative
- **Risk reporting;** timely, accurate and useful to enhance the quality of decision-making and to support management and oversight bodies in meeting their responsibilities.

The Management of Risk process wheel

Risk management is the identification, evaluation, and prioritization of risk (defined in ISO3100:2018) as *the effect of uncertainty on objectives* followed by coordinated and economical application of resources to minimize, monitor, and control the Likelihood or impact of unfortunate events or to maximize the realization of opportunities.

Risk Identification and Assessment

This process does not cover Hazard Management, for example, working alone away from your office can be a hazard. The risk of personal danger may be high. Electric cabling is a hazard. If it has snagged on a sharp object, the exposed wiring places it in a 'high-risk' category. Hazard management is covered under the SCC Health & Safety policy. All enquiries should be directed to the Central Health & Safety Team at County Hall. You do not record hazards in JCAD.

Risk Identification:

Risk identification should produce an interconnected view of risks, they can be organised by categories or they can be genuine 'one-offs'. The aim is to identify and understand the council's risk profile, especially those that may potentially impact on one or more of our objectives. Risks can come from any of the following activities;

- Strategic Planning
- Service and Commissioning Plans
- Financial planning
- Contract management
- Procurement
- Performance monitoring
- Key and non-key decisions
- Partnership working
- Project and Change Management
- External factors beyond our control

Risks should be identified even where their sources are not under the organisation's direct control. Even seemingly insignificant risks on their own have the potential, as they interact with other events and conditions, to cause great damage or create significant opportunity.

Talk with your team: The best time to look at the uncertainties (risks) around successful delivery of your services annual objectives is to hold a risk identification session when you are writing your *Commissioning* or *Service* Plans. For projects and programmes, this is when you are at the start of your work, when you are developing your project or programme plans. The councils Risk Manager can help facilitate this.

There are many techniques you can use when identifying risks, examples include; Horizon Scanning; looking into the future of your service, Strength, Weakness, Opportunity and Threats (SWOT) analysis or scenario planning.

Write the risk description, keep it concise.

Start by writing the risk portion–the uncertain event or condition. When defining risks, think about what may or may not happen. Risks are uncertain events or conditions, not things that have already happened. (Threats that have occurred are called issues; opportunities that have occurred are benefits).

All risks need to be written following the format below

- **The uncertain event or condition** (description) **.....**
- **caused by .....**
- **resulting in** (consequence/impact) **.....**

Ask the following questions;

- Is this risk within our gift to control, is this something we can do anything about?
- Is the risk connected to a corporate or service objective?
- Does the risk description focus on uncertain events or conditions?
- Is the risk clearly defined and specific?
- Does the risk description drive clear response plans, i.e. do the new actions/controls really help to mitigate the risk, can you measure the results of the control?
- Does it matter? if not, is this really a risk?

This simple table could help with the identification process.

<table>
<tr><td>Caused by ...</td><td rowspan="2">The uncertainty/condition

?</td><td>Resulting in (Consequence/Impact)..</td></tr>
<tr><td>New Controls
[what new actions are you going to put in place to mitigate it this risk]</td><td>Existing Controls
[What plans do you have in place already to minimize the impact?]</td></tr>
</table>

Assessment:

Risk evaluation should involve comparing the results of the risk analysis with the nature and extent of risks that the organisation is willing to take to determine where and what additional action is required. Options may involve one or more of the following:

- **Terminate:** avoiding the risk, if feasible, by deciding not to start or continue with the activity that gives rise to the risk;

- **Tolerate:** retaining the risk by informed decision;
- **Treat:** changing the likelihood, where possible or changing the consequences, including planning contingency activities;
- **Transfer:** sharing the risk (e.g. through commercial contracts or partnership working).

The outcome of risk evaluation should be recorded in JCAD, communicated and then validated at appropriate levels of the organisation. It should be regularly reviewed and revised based on the dynamic nature and level of the risks faced.

Identify the **risk owner** – this must be an individual not a service name or Group, Board, Committee. The owner is usually from the service area effected by the risk, if the named owner changes role then a new owner must be identified. This is not always the case where a Director is the risk owner.

There are three levels of risk score required, the **risk owner** will need to use the Councils RAG Assessment Matrix to identify;

Inherent Risk Score: This is the **uncontrolled worst-case scenario** based on the pure risk without identified controls/mitigation. This will be the highest RAG score. See fig 1.

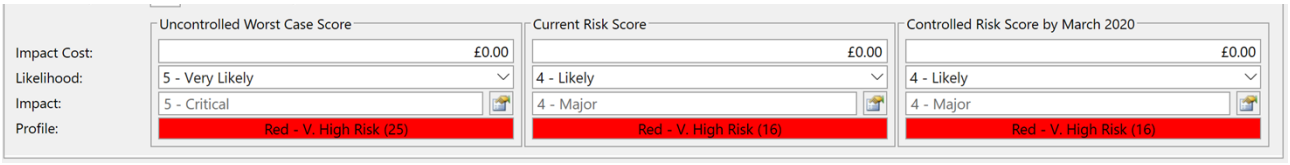


Fig 1.

Current Risk Score: Use the RAG scoring matrix again to now assess the level of risk This should be better than the inherent score if you were able to identify proactive (existing) controls, but, if this is a completely new initiative there may not be any proactive controls in place, in which case the current score would be the same as the inherent score. Fig 1.

The **risk owner** is required to:

- consider the current score and adjust, if necessary, at each review.

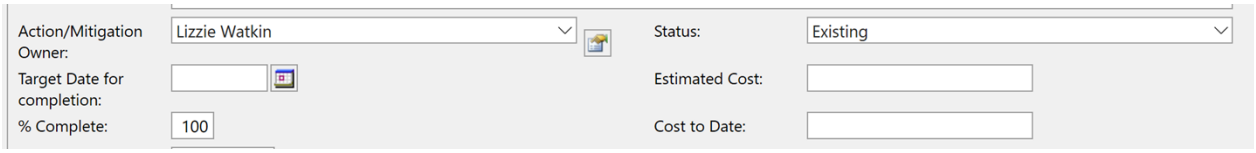


Fig 2.

Controlled Risk Score by March 2020 (example**):** Use the RAG scoring matrix, available at the end of this document or from the "My Summary screen" in JCAD, to plot the likelihood and Impact of the risk using the information you have gathered above. This score should

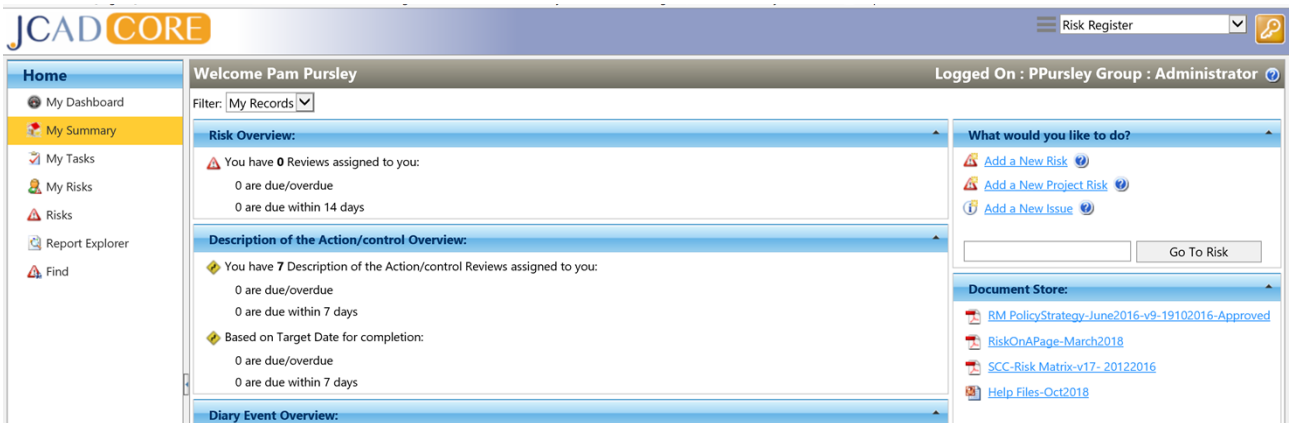
reflect the level of risk the service is able to accept/tolerate in the forthcoming financial year. Fig 1.

***JCAD*:** Risks need to be entered in JCAD following the guidance below;

Current risk score:

- If your **current score** is '**Low**' (**green**) – the use of JCAD to record and monitor these risks is voluntary, but, this does not mean you can ignore them, you still need to monitor them as any risk has the potential to change over time. The Commissioning or Service Plan template is the idea place to record these risks so that they are still a living document, but the review is less formal.
- If the current score is '**medium**' (**yellow**) – you must record and monitor using JCAD. The requirement to review this level of risk is quarterly.
- If the current score is '**high**' (**orange**) – you must record and monitor using JCAD. The required review period is monthly.
- If the current score is '**very high**' (**red**) – you must record and monitor using JCAD. The required review period is monthly, but you can set the review for anything from 1 to 30 days if there is real concern the risk may occur imminently.

The Risk Assessment Grid and guidance are available from the 'Document Store' on the "My Summary" screen in JCAD or at the end of this document.



Risk Treatment

Selecting the most appropriate risk treatment option(s) involves balancing the potential benefits derived in relation to the achievement of the objectives against the costs, effort or disadvantages of implementation. Justification for the design of risk treatments and the operation of *internal control* is broader than solely economic considerations and should consider all the organisation's obligations, commitments and stakeholder views.

Proactive controls – what you already have e.g. policy, regulation, governance, insurance etc
Reactive controls - what you need to do: e.g. new / updated policy, business redesign, purchase insurance etc

When selecting reactive controls, you need to know the expected benefit to be gained, your goal is to reduce the risk to an acceptable level.

The 4 'T's' - Description of types of controls	
Terminate	Remove the cause of the threat, cease activity. These controls are designed to limit the possibility of an undesirable outcome being realized. The more important it is to stop an undesirable outcome, the more important it is to implement appropriate and proportionate preventive controls
Treat	Put in place mitigation to make it less likely to have a severe impact on the Council. Designed to limit the scope for loss and reduce undesirable outcomes that have been realized. They could also achieve some recovery against loss or damage
Transfer	Pass the whole risk to a third party. Designed to ensure an outcome is achieved. Transfer could be to another service area or an external contractor, you need to assure yourself that safe systems of work are followed by all concerned.
Tolerate	The Council accepts that the risk may occur. You may decide to 'tolerate' a risk because there is nothing more you can do to reduce the effect (impact) if the risk were to materialise. You may also tolerate a risk if the uncertain event has indeed happened in which case Issue management* needs to be put in place. You must get authorization from a Strategic Manager or above to tolerate a risk.

* Issue Management is not covered in the suite of Pathway documents. If a risk does indeed materialise then immediate management action needs to be taken to resolve any escalation in additional risk or undesirable impact on the Council.

Where appropriate, contingency, containment, crisis, incident and continuity management arrangements should be developed and communicated to support resilience and recovery if risks crystallise. Contact the Civil Contingencies Unit for advice and assistance with Business Continuity Planning.

The **risk owner** is responsible for the identification of;

- **proactive** controls and for ensuring they are record in JCAD as "100%" complete and status of "existing". Fig 2

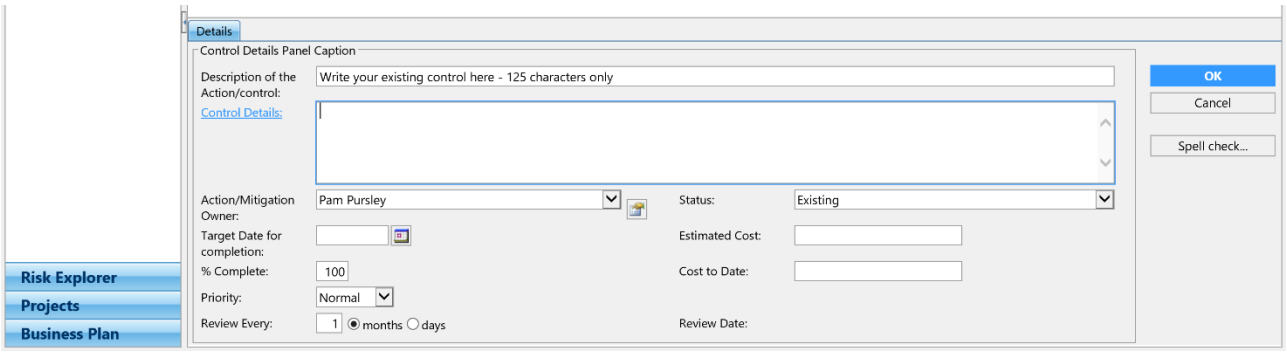


Fig 2.

- **reactive controls** – these are the additional pieces of work (actions) required to mitigate/control the identified risk (bottom right wing). Fig 2
- identification of the **control (action) owner**, this must be an individual not a post name or service area.

Completion of the 'Control Details Panel' will set the diary in JCAD that then generates the review emails to the action owner. Fig 3

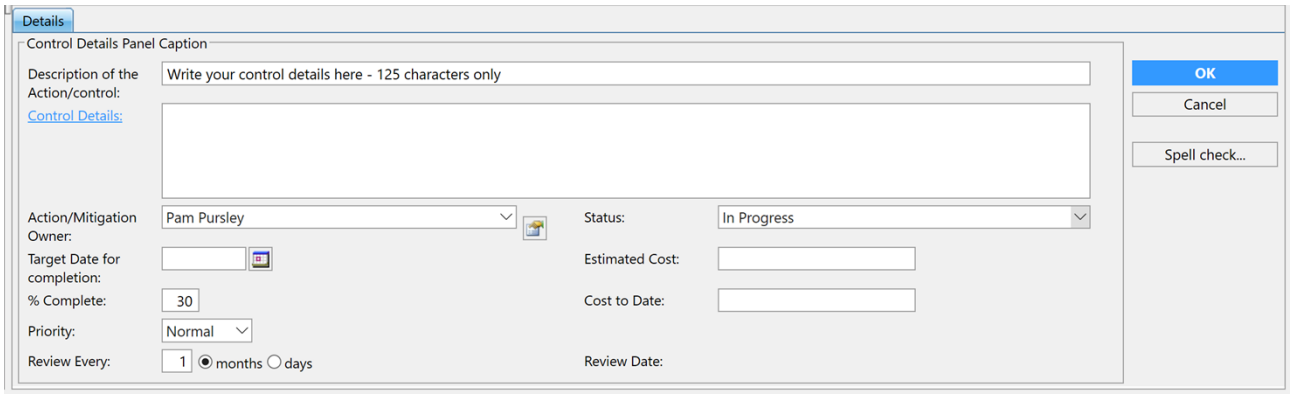


Fig 3.

Risk Monitoring

Monitoring should play a role before, during and after implementation of risk treatment. Ongoing and continuous monitoring should support understanding of whether and how the risk profile is changing and the extent to which internal controls are operating as intended to provide reasonable assurance over the management of risks to an acceptable level in the achievement of organisational objectives.

The results of monitoring and review should be incorporated throughout the organisation's wider performance management, measurement and reporting activities.
Recording and reporting aims to:

- transparently communicate risk management activities and outcomes across the organisation;
- provide information for decision-making;

When a risk has been entered into JCAD, the systems internal diary will be activated with the monitoring period set depending on the **current risk score:**

- Very High / High, Red or orange – Monthly review
- Medium, yellow – quarterly review
- Low / very low, green – at least once a year. The use of JCAD for this level of risks is optional, but a record of the risk must still be kept and monitored.

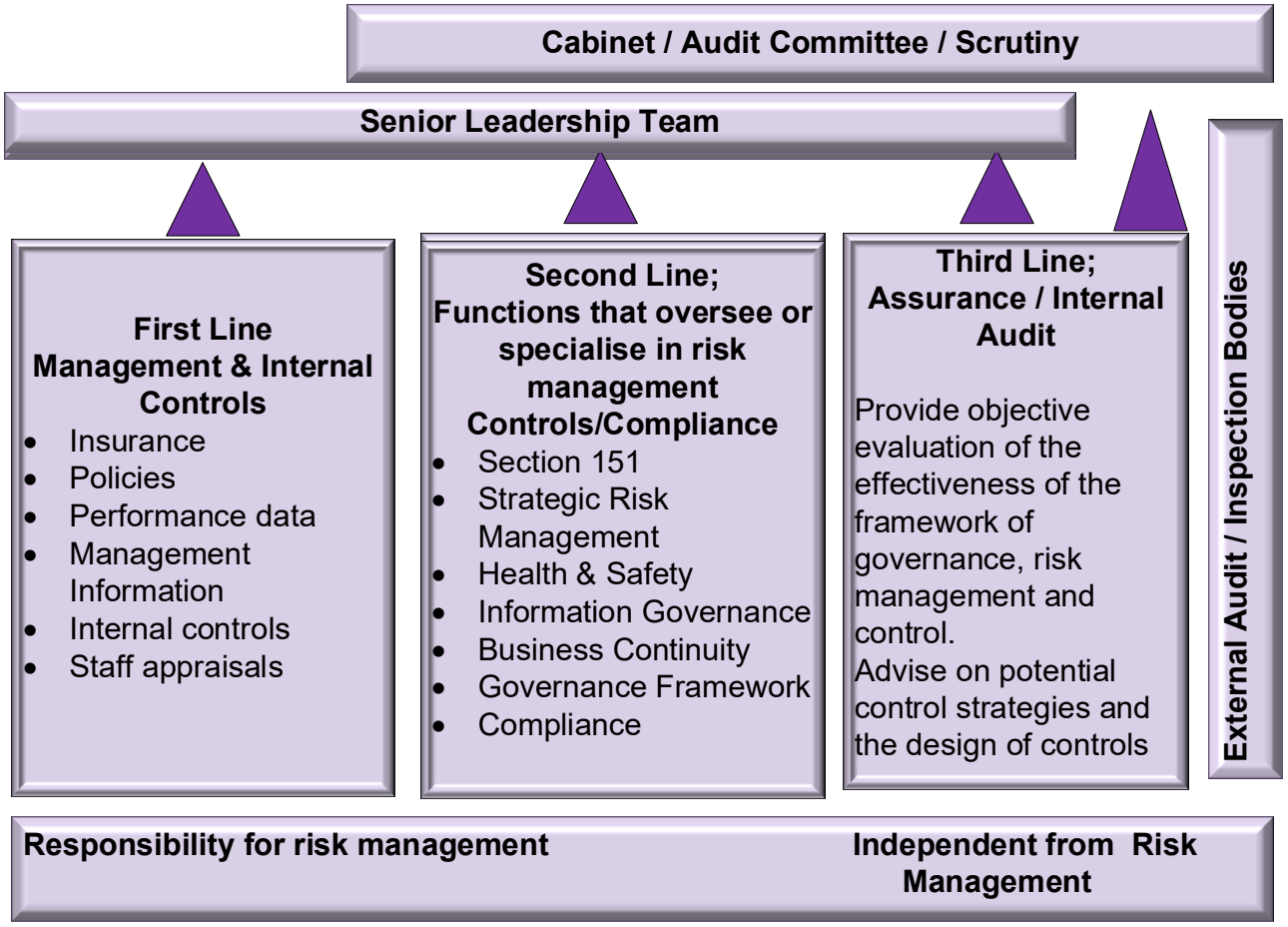
An email is sent to the Risk Owner and Action Owner when the review is due.

- The Action Owner is responsible for the review of the action assigned to them, they should provide a written statement on the current position, update the % complete and accept the next review date.

- The Risk Owner must assure themselves that the action owners are completing their reviews and update the current score by re-assessing the Likelihood and Impact scores. The risk owner is responsible for providing the review statement that reflects any changes/improvements.

The "three lines of defence" model, see below, sets out how these aspects should operate in an integrated way to manage risks, design and implement internal control and provide
assurance through ongoing, regular, periodic and ad-hoc monitoring and review. When an organisation has properly structured the "lines of defence", and they operate effectively, it should understand how each of the lines contributes to the overall level of assurance required and how these can best be integrated and mutually supportive.

There should be no gaps in coverage and no unnecessary duplication of effort. Importantly, the accounting officer and the board should receive unbiased information about the organisation's principal risks and how management is responding to those risks.



All members of staff within the Council has some responsibility for risk management and assurance can come from many sources. A concept for helping to identify and understand the different contributions the various sources can provide is the Three Lines of Defence model. By defining the sources of assurance in three broad categories, it helps to understand how each contributes to the overall level of assurance provided and how best they can be integrated and mutually supportive. For example, management assurances could be harnessed to provide coverage of routine operations, with internal audit activity target at riskier or more complex areas.

The **Management of Risk - Policy Pathway** explains the escalation process for the management, review and reporting of all levels of business risks across the Council. There are separate arrangements for Health & Safety risks and the daily safeguarding risks that arise in the Social care services.

Escalation of Risks						
	Service Manager	Strategic Manager	Service Director	Senior Leadership Team	Audit and or Scrutiny Committee	Cabinet
Service Level	✓	✓	✓			
Directorate Level			✓	✓	✓	✓
Strategic Level			✓	✓	✓	✓
Programme & Project Risks						
	Project & Change officers	Project & Change Managers	Project Board	Programme Manager	Programme Board	
	✓	✓	✓	✓	✓	

Risk Reporting

Strategic Risk Management Group	**Governance Board**	**SLT**	**Audit Committee**
Monthly reporting	Monthly by exception	Strategic Risks - Monthly. SWAP - Monthly	Strategic Risk -Twice yearly SWAP Partial Audits – At each Meeting

The Senior Leadership Team, supported by the Audit Committee, should specify the nature, source, format and frequency of the information that it requires. It should ensure that the assumptions and models underlying this information are clear so that they can be understood and, if necessary, challenged.
Factors to consider for reporting include, but are not limited to:

- differing stakeholders and their specific information needs and requirements
- cost, frequency and timeliness of reporting
- method of reporting; and
- relevance of information to organisational objectives and decision-making.

The information should support SLT to assess whether to review the adequacy and effectiveness of internal controls, and to decide whether any changes are required to re-assess strategy and objectives, revisit or change policies, reprioritise resources and improve controls.

Clear, informative and useful reports or dashboards should promote key information for each strategic risk to provide visibility over the risk, assess the effectiveness of key management actions and summarise the assurance information available.

SLT should have a standard agenda item at least monthly to discuss the current Strategic Risks profile. The Strategic risks should be subject to "deep dive" reviews by SLT at least annually or an appropriate frequency, set by SLT, depending on the nature of the risk(s) and the performance reported.

Strategic Risks are reported to Audit Committee twice a year, with the Partial Internal Audits being reported quarterly. The Committee Chair may request that an officer attend a subsequent committee meeting to explain the progress of an individual risk or risks for the service area.

Each month a Risk Awareness Report (RAR) is sent to each Director for the risks across their services. These reports should be used at management team meeting's so assurance can be gained that those risks / actions that need attention are highlighted and the appropriate action is taken.

The Strategic Risk Management Group (SRMG) meets monthly and will look at various reports drawn from JCAD to assure themselves that the management of risk is taking place. SRMG also reports to Governance Board by exception and on a regular basis to SLT highlighting any concerns or suggestions of emerging risks.

JCAD has a few pre-defined report templates, the standard report template is called “Risk Register Business Unit Display” and is available from the Report Explorer tab.

Programme and project risk reports are available from the Report Explorer using the “Risk Register Project Display” option. See Fig 4 below.

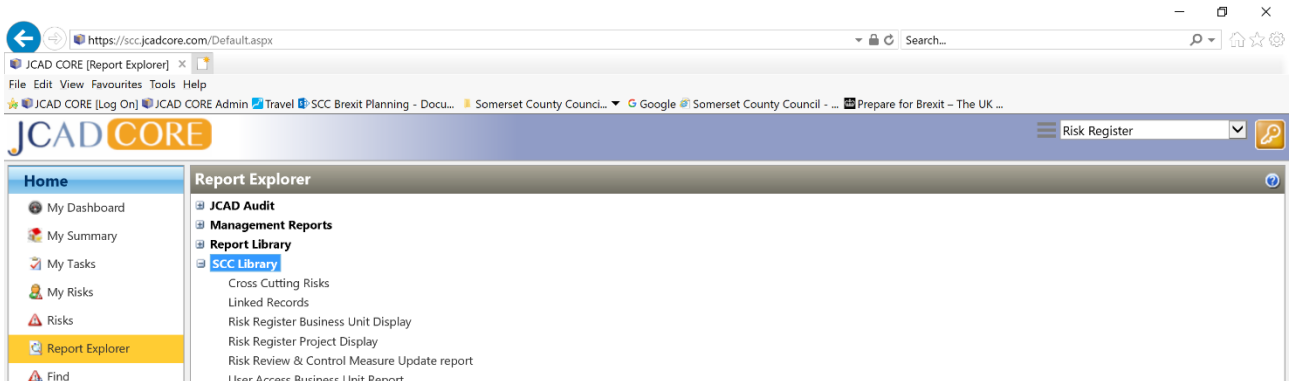


Fig 4.

The report launcher allows the user to select various options from the drop-down lists provided which, returns the standard risk report.

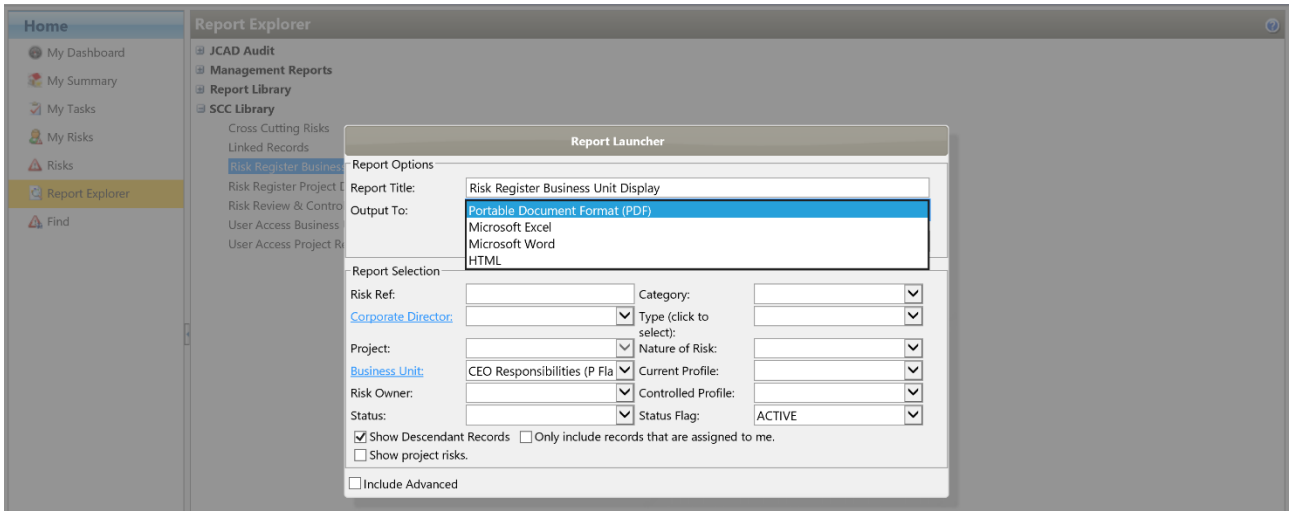
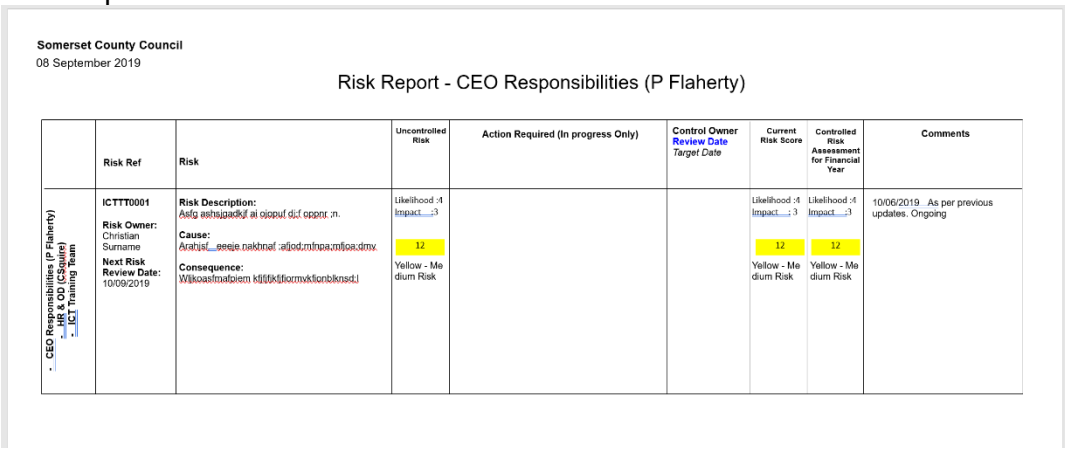


Fig5.

Users need to be aware that any risk report that is generated and saved has a retention period of 6 years from the date on the report.

Users need to note that as JCAD is a real-time system, any changes made to a record will instantly become the current iteration of that record, therefore risk reports are only valid on the **day** they are produced.

Risk Report



Somerset County Council
08 September 2019

Risk Report - CEO Responsibilities (P Flaherty)

	Risk Ref	Risk	Uncontrolled Risk	Action Required (In progress Only)	Control Owner Review Date *Target Date*	Current Risk Score	Controlled Risk Assessment for Financial Year	Comments
- CEO Responsibilities (P Flaherty) - HR & OD (CSquire) - ICT Training Team	ICTTT0001 **Risk Owner:** Christian Surname **Next Risk Review Date:** 10/09/2019	**Risk Description:** Asfg ashsjgadkjf ai ojopuf dj;f oppnr ;n. **Cause:** Arahjsf eeeje nakbnaf :aljod;mlnpa;mljoa;dmv **Consequence:** Wlkoasfmalpiem kljfjtkfjiormvkflonblknsd;l	Likelihood :1 Impact :3 12 Yellow - Medium Risk			Likelihood :4 Impact :3 12 Yellow - Medium Risk	Likelihood :4 Impact :3 12 Yellow - Medium Risk	10/06/2019 As per previous updates. Ongoing

Fig 6.

Training & workshop facilitation contact:

Pam Pursley, Strategic Risk Manager
T: 01823 359062
E: ppursley@somerset.gov.uk

The councils risk management process complies with the principles of the following National & International policies and strategies:

- ISO 31000:2009/2018 Risk Management – Principles and Guidelines
- 'A Structured Approach to Enterprise Risk Management', The Institute of Risk Management (IRM)
- Fundamentals of Risk Management, 5th Edition, IRM
- The Orange Book 2019, HM Treasury
- Management of Risk (M_O_R), OGC
- Guidance & Toolkit, ALARM, The **Public Risk** Management Association.