

## Payroll unit risk register

Only the first five risks are shown. Bolded columns are the ones you would show in a compact summary (Summary description of the risk, Unplanned outcome on an objective, and Likelihood).

		Risk description by components			Likelihood components			
Ref	Summary description of the risk	Reasons for uncertainty	Event or wrong assumption	Pathway to the unplanned outcome	Unplanned outcome on an objective	Assumed controls	Explanation of likelihood	Likelihood
		ISO: Risk sources, sources of risk. Includes uncertain assumptions.	ISO: Event	ISO: Consequence		ISO: Controls		ISO: Likelihood
<i>Risk ID</i>	<i>Rolls the components into one or two short sentences. Best completed after the detailed description. (The summary is not 'the risk'. It is a distinguishing title or label.)</i>	<i>Ensure it is clear why you are uncertain that reality will match this risk description and the unplanned outcome. ISO 31000 refers to the reason for uncertainty as the 'risk source'. The risk source is not the same thing as the cause for an event. Event causes are shown in the next column. Sources of uncertainty affect not only events and assumptions, but also the pathway from event or discovery to outcome.</i>	<i>Clear description of the key event that may or may not happen, or of the assumption that may or may not be correct. Where a combination of events and conditions are involved, show a list connected with AND or OR as applicable.  An event description may include causes for the event. It need not detail all the ways in which the event might come about, and there is no need to trace each potential event back to 'root' causes.</i>	<i>Explain how the event or wrong assumption may lead to the unplanned outcome. Include notes on:</i> <ul style="list-style-type: none"> <li><i>the certainty with which the outcome will follow from an occurrence of the event or from the wrong assumption</i></li> <li><i>secondary events and uncertainties affecting the consequences of the main event</i></li> <li><i>response actions that will affect the year-end outcome and its likelihood, after the event or wrong assumption have occurred.</i></li> </ul>	<i>Copy or refer to the text in the outcome picture collection. A short version may be enough. [Examples use short versions from the summarised outcomes table.] The consequence is the effect on objectives. The outcome picture shows that effect precisely.</i>	<i>List the registered controls assumed when estimating likelihood.</i>	<i>Summarise factors such as the frequency of events and wrong assumptions of this kind, effect of controls, history of related scenarios, confidence or uncertainty about what can and can't happen. If the likelihood could be much higher or lower than the estimate, show and explain the plausible range.</i>	<i>Assessed likelihood that this pathway will lead to the indicated outcome for the year, as a % value. This likelihood rolls up all the 'known' event frequencies and all the acknowledged uncertainties within the pathway to the outcome.</i>
01		Pay agreements are somewhat complex, and they are affected by regulations and law cases outside the organization. There is a significant body of workers on shifts, with non-trivial effects on their weekly pay. There has been no practical way to ensure that all interpretations by the payroll team have been legally correct, and the situation will continue to evolve over the coming year.	In response to direct pressure from upper management, the payroll team interprets systematically interpreted specific parts of pay agreements in a way that employees feel is unfair, for example in the start and end times for shift-work loadings. AND The legal interpretation actually adopted is actually dubious (or worse), but the payroll team assume that upper management are right, OR that the payroll unit has no authority to raise objections. AND Formal complaints from employees are systematically rejected.	Under these conditions, there is a clear possibility that the union, and/or other employee representatives, will commence a legal action.	<b>Payroll team failures led to legal action against the organisation, OR loss of workforce threatening viability. (Timely and accurate payments, Worst imaginable)</b>	(From Controls Register) Employees have a well-defined process to query or complain about pay errors (email to payroll.complaints@) Employee complaints are logged and reported monthly within the payroll team.	The logging and review of employee complaints makes it extremely unlikely that there is an unrecognised legal breach that will appear as a legal action without a long period of warning. Those complaints have never been of a nature that would suggest that this scenario is plausible. However, the scenario might become plausible as agreements change or if the attitude of upper management hardens, for instance after a merger.	<b>.01% (1 in 10000 for the coming year)</b>
02	<b>Gap(s) in the audit trail created by the payroll policy of accepting emails from employees and managers.</b>	Payroll team members are expected to file officially all evidence supporting payroll transactions, but it is not known to what extent they have been doing so, or will do so in future. One category of particular doubt is emails sent to the email addresses of payroll team members.	The payroll team accepts employee requests and manager authorisations via email to payroll team members. AND Some team members do not reliably file an auditable copy of each such email in the official system. AND One or more of those team members leave the organization while the transactions are still subject to audit. (If the team member is still around at the time of the audit, the team member can find key emails when required, from their personal mailbox.)	A substantial number of emails forming part of the audit trail are 'somewhere' in the personal mailboxes of the payroll team members who are no longer in the organization at the time of an audit. However, it is not practicable or justifiable to unseal and search the personal email collections of former team members for the audit. Effectively, there is no supporting evidence for the corresponding payroll transactions. Management will assume that most transactions were legitimate and processed accurately, but the truth of this belief will not be readily demonstrated. From there, it is very likely that the audit trail gap would be detected and reported by an independent audit.  (If emails are not properly filed but are recovered during the audit by team members, the filing failure is likely to attract a minor critical comment from the audit.)	<b>Substantial gaps in the audit trail, almost certain to be reported by a future audit. (Audit, Partial Success)</b>	(From Controls Register) There is a well-defined method for payroll team members to file emails supporting payroll transactions, for subsequent retrieval in an audit. Payroll quality control is supposed to include a sample check for correct filing, anticipating an audit.	All payroll team members are aware of the requirement to file supporting evidence for payroll transactions. They are also aware of quality control checks and periodic independent audits, which motivate proper filing. Exceptions are likely, at least occasionally. Similar instances have been found in past audits, though that was before payroll started accepting emails. The new policy makes this outcome relatively likely, despite quality control (see the Control).	<b>40%</b>

		Risk description by components			Likelihood components			
Ref	Summary description of the risk	Reasons for uncertainty	Event or wrong assumption	Pathway to the unplanned outcome	Unplanned outcome on an objective	Assumed controls	Explanation of likelihood	Likelihood
03		<p>Senior payroll team members can create fraudulent transactions, but are normally deterred by quality control checks and reconciliations that would detect them.</p> <p>The extent to which frauds would be detected in the extended absence of the payroll unit manager is unclear. The normal presumption is that fraud detection checks would continue as normal.</p> <p>The possibility of the audit trail being lost (accidentally or otherwise) has never been given much thought by anyone. The potential for that to actually happen is assumed to be nil, but may actually be quite high.</p>	<p>The payroll unit manager is temporarily assigned elsewhere for an extended part of the year. The Assistant Manager is left in charge.</p> <p>The Assistant Manager is overwhelmed by the added workload, and there are other staffing gaps that put the whole team under unusual pressure.</p> <p>As a result, the Assistant Manager puts one of the senior team members in charge of quality checks and reconciliations. On the ground, all non-urgent parts of payroll processing, such as quality checks, are deferred indefinitely.</p> <p>The same senior payroll team member creates a number of fraudulent transactions and recruits two other team members into trying the same thing. The senior team member engineers the loss of the audit trail for the period of the fraud, making it look like an accident. The loss of all audit trail records during that period means that the fraudulent transactions will not be distinguishable from the legitimate ones in the same period. The 'accident' story is spread widely, with embellishments to make it sound like the IT department was responsible.</p> <p>Management assumes that the audit trail is safe from accidental loss or deliberate meddling (until the 'accidental loss' story is put around).</p>	<p>The fraud itself is dealt with in a separate risk with a different outcome picture. [Risk 04 below]</p> <p>The events would result in the picture described, a period of un-auditability and a well-founded suspicion of fraud much more extensive than any known cases. The fact that such a thing is possible will reflect very badly on the managers responsible.</p>	<p><b>Payroll is unauditabile, and there is a suspicion of fraud or gross mis-management. (Audit, Failure)</b></p>			
04		Same as 03 above	Same as 03 above	<p>Some payroll team members will have committed a fraud. However, the fraud is detected and will be investigated, with disciplinary responses as appropriate. Conditions that allowed the fraud will almost certainly change, for example, removing all payroll team members' access to delete evidence trails.</p> <p>The gaps in the audit trail mean that investigation will be difficult, but there will be enough evidence and pain to deter or prevent future fraud attempts along similar lines. The final outcomes will match up well with the outcome picture in the collection.</p>	<p><b>Some frauds achieved short-term success, but were subject to investigation, and action was taken. Employee reporting is not uncommon. (Fraud, Partial Success)</b></p>			
05		The possibility of the audit trail being lost (accidentally or otherwise) has never been given much thought by anyone. The potential for that to happen is assumed to be nil, but may be quite high.	<p>The payroll system itself has defined security and audit controls. However, the database containing the evidence supporting payroll transactions is quite separate.</p> <p>A non-expert member of the payroll team or of the IT support team messes with database tables or configuration details of the system in which the audit trail is kept.</p> <p>That person does something hasty (or irresponsible) that results in deletion of supporting evidence for payroll transactions, covering a substantial category of evidence records covering an extended period.</p> <p>Management had assumed that an accidental or unauthorised deletion is not possible, but that assumption had come more from wishful thinking than from known facts.</p>	<p>Deletion of records means that there are not auditable records at the time of an independent audit. The situation cannot be overlooked by auditors, even if there is no other evidence of fraud. There will be a negative audit finding, with broad visibility.</p>	<p><b>Payroll is unauditabile, and there is a suspicion of fraud or gross mis-management. (Audit, Failure) Refer to the original outcome pictures, not just the summary</b></p>	<p>(From Controls Register) Database tables and their configuration files are normally kept secured from unauthorised or accidental changes. There is a defined procedure for authorised changes, requiring special approvals and post-change validation. (effectiveness unknown)</p>	<p>The likelihood of this scenario during the year is based on subjective ignorance, rather than on a known frequency for similar events. The likelihood shown is a fair guess. There would be little argument against a likelihood is as high as 50%, or below 1%.</p>	10%