

**Information sheet 3**

Responding to risk – controls and actions

We regularly asses our risks, identify trends and respond to risks and opportunities for continuous improvement.

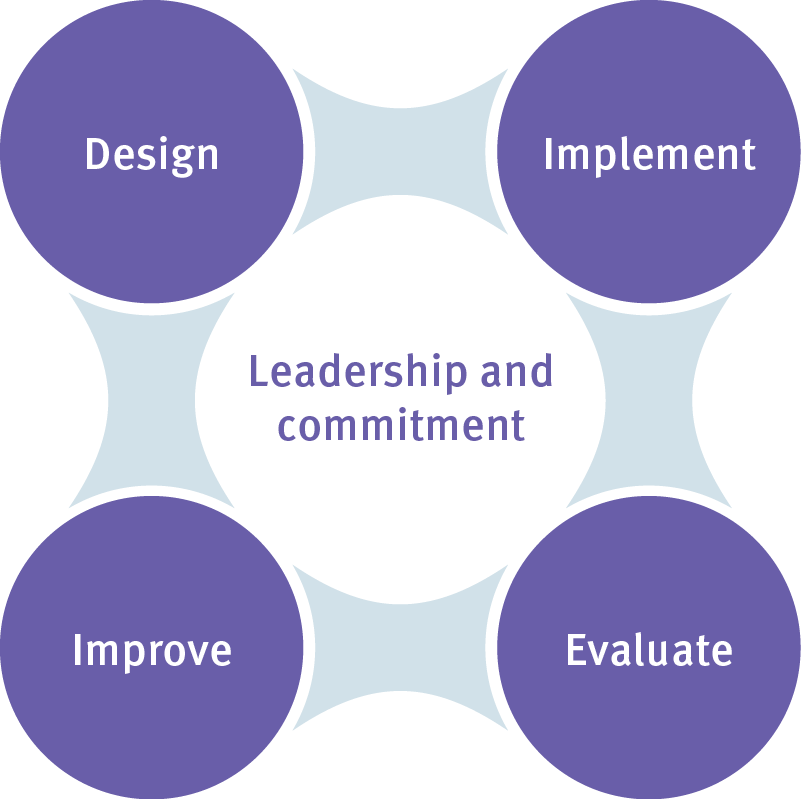
One way we respond to risk is to review existing controls and actions and/or implement new controls and actions, to maintain or modify the likelihood and/or the consequence of a risk.

When planning an appropriate and effective response, it is important to understand the difference between controls and actions.

* **Controls** are an existing strategy used to maintain or modify a risk and may include any process, policy or practice and are an ongoing function of the business
* **Actions** are a new planned, temporary strategy applied to maintain or achieve the target level of risk after controls are applied. Actions are undertaken in a pre-determined time-frame
* An **action can transition to a control** if the strategy becomes an ongoing function of the business

1. Control improvement

Improving controls is an essential part of risk management. Control improvement includes five elements:



**Leadership and commitment -** risk and control owners are committed to improving the effectiveness of controls applied to risks

**Design -** controls are designed based on an understanding of the department’s operating environment, they manage risks effectively and are cost effective

**Implement -** controls are documented, implemented and communicated to staff and, where appropriate, training is provided

**Evaluate -** control performance is periodically measured against intended purpose to ensure risks are managed effectively

**Improve -** controls are monitored and enhanced to address changes in risks and to ensure controls are suitable, adequate and effective in maintaining or modifying risk levels

1. Improving control effectiveness and assurance

An effective control is one that performs to specification, functional requirements and expected standards to achieve the desired effect of maintaining or modifying the likelihood and/or consequences of the risk. Control assurance refers to the confidence that the control is operating effectively through formal testing undertaken by an independent reviewer. Controls can be clarified and improved by:

* ensuring control descriptions emphasise how the control modifies the risk, using the formula: *the* strategy (e.g. committee) + *how it effectively manages the risk* (e.g. scrutinises performance reports) + *a KPI* (e.g. quarterly)
* ensuring controls are formally documented and communicated to staff
* seeking stakeholder feedback on the performance of controls and possible areas for improvement
* establishing monitoring processes
* engaging a control reviewer independent of the control owner
* reporting on control effectiveness and assurance to executive management
* using the department’s risk register (currently Risk Express) as part of the quarterly review of risks
* working with the department’s risk team to improve control effectiveness and assurance

1. Control and action types

|  |  |  |  |
| --- | --- | --- | --- |
| **First line of defence –** Routine management action to identify, implement and assess the operation of:   * internal control strategy * policies and procedures | | | |
| **Control/Action Type** | **Explanation** | **Goal** | **Examples** |
| Internal Controls | The methods, processes or procedures implemented to:   * ensure compliance with prescribed requirements including legislation and regulation * safeguard assets * check the accuracy and reliability of accounting information | An effective and efficient internal control structure provides reasonable assurance to the accountable officer that:   * the activities are being conducted in a manner that facilitates the achievement of objectives and the delivery of outputs in an orderly and efficient way, avoiding waste, extravagance and other potential causes of risk or loss * error, fraud and other irregularities are prevented as far as possible and promptly detected if they do occur * assets are safeguarded from unauthorised use or disposal and are adequately maintained * operational activities and individual transactions are complete and accurately reflected in the accounting period to which they relate * financial management information is timely, relevant, and fairly presented | * Segregation of duties * Preparation of purchase orders * Approval of expenditure * Acquittal of corporate credit cards * Preparation of timesheets * Reconciliations by independent officers * Controls over the custody and security of accountable forms |
| Frameworks, Policies and Procedures | Ensuring outcomes are delivered in a controlled and consistent way by clearly specifying the department’s policy intent and the way that the intent is to be implemented | Increase confidence by specifying the way particular activity or outcome is to be delivered | * Workplace Health and Safety Procedure * Student Protection Procedure * Governance Framework |

|  |  |  |  |
| --- | --- | --- | --- |
| Monitoring and Review | * Observing the effectiveness of business processes and systems against expectation / performance indicators * Testing to ensure that processes and systems are fit for purpose and continuously deliver desired outcomes | Observing the operation of internal controls and/or processes to ensure they are:   * achieving the intended outcome * in place and operating effectively and efficiently * compliant with legislation and policy * effectively managing the risk | * Review of system access to IT systems to ensure it aligns to approved user access profiles and position * Review of the completion of timesheets * Review of monthly performance reports including variance analysis |
| Reporting | * Documenting the results of checks on the effectiveness of processes and systems * Formally presenting the results to a committee or working group for scrutiny | Preparation of particular information to provide the user with advice as to the outcome of a situation, process or event | * Preparation of financial reports * System access reports * Preparation of quarterly performance reports |
| Information Technology (IT) Systems | Sets of [tools](http://www.businessdictionary.com/definition/tool.html), [processes](http://www.businessdictionary.com/definition/process.html), and [methodologies](http://www.businessdictionary.com/definition/methodology.html) and [associated](http://www.businessdictionary.com/definition/associated.html) [equipment](http://www.businessdictionary.com/definition/equipment.html) used to collect, process and present [information](http://www.businessdictionary.com/definition/information.html) | IT systems aim to improve the efficiency and effectiveness of operational processes and procedures using electronic systems and structures | * OneSchool * SAP * Risk Express |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Second line of defence** **-** Executive oversight of the first line of defence | | | | | |
| **Control/Action Type** | | **Explanation** | | **Goal** | **Examples** |
| Compliance and Assurance | | * Ensuring systems, processes and practices are compliant with requirements of legislation * Scrutinising the quality of a system, process or output against policies, procedures, standards and expectations * Documenting compliance and assurance checks | | * Increase certainty that the department’s services and products are of the highest quality and meet legislative requirements | * Legislative and Administrative delegations and authorisations * The department’s induction strategy and mandatory training * Emergency response plan and testing * Online approvals for purchase orders |
| Governance | | Committee or working group oversight, including:   * scrutiny of performance reports * assessing effectiveness of risk controls and actions * requesting reviews to be undertaken * ensuring timeframes are met * assuring the quality of program/project outputs | | A culture of accountability for improving performance and managing risk | * Executive Management Board * Audit and Risk Management Committee |
| Education and Awareness | | Increasing awareness through targeted and effective messages to staff and stakeholders | | Create a corporate culture where risk is understood and effectively managed | * Stakeholder engagement and information sessions * Information sheets and guidance materials |
| Building Capability and Training | | * Enhancing the ability of systems and processes to control the risk * Increasing the level of resources used to control the risk * Increasing the ability of staff to control the risk | | * An agile, flexible approach that can control risk within a changing operating environment * Empowered staff who manage to reduce risk effectively | * Coaching and support for staff * Policy development and analysis training * Financial management support and training * Driver training courses for staff traveling in rural and remote areas |
|  | |  | |  |  |
| **Third line of defence** **-** Independent Assurance | | | | | |
| **Control/Action Type** | **Explanation** | | **Goal** | | **Examples** |
| Independent Review | | Review by an independent expert including consultants | Expert advice to provide management assurances as to the operation of a particular process, unit, system or division | | * Information security review by an independent consultation process * Independent workplace health and safety review |

For further information refer to the [Enterprise Risk Management Framework](https://ppr.mpe.qed.qld.gov.au/attachment/enterprise-risk-management-framework.pdf) or [Policy and Procedure Register](https://ppr.mpe.qed.qld.gov.au/pp/enterprise-risk-management-procedure) or email [enterprise.riskmanagement@qed.qld.gov.au](mailto:enterprise.riskmanagement@qed.qld.gov.au)