

05 May 2020

## Governance controls during COVID-19

Most entities have recently made changes to their internal controls in response to COVID-19, including expanding work from home arrangements to support social distancing requirements.

With any change in working arrangements comes an increased risk of controls failing, particularly manual controls and where controls previously operated with a high level of management oversight within an office environment.

We encourage all entities to remain vigilant with their monitoring of internal controls during this time.

Key areas that entities need to consider as they change their working arrangements to respond to COVID-19 are highlighted below.



### Information systems

Changing to remote working arrangements may lead to additional strain on key information technology systems and resources, such as additional access to systems being required across an entity. All staff must ensure that system access controls continue to be followed, or where these cannot be fully implemented, additional monitoring of access and approvals is performed.



### Monitoring of manual controls

The risk associated with controls, particularly manually performed controls, may change in a remote working environment. Entities may need additional oversight or checks to monitor these controls.



### Record keeping

Evidence of controls operating may not be as easy to obtain or store for some entities when staff work remotely. Adherence to organisational policies and legislation is still needed during these arrangements.



### Changes to staff roles and responsibilities

Some staff may take on additional or changed responsibilities to help facilitate business as usual operations. Processes to help staff get up to speed with the new responsibilities are important such that any key controls they are now responsible for are not missed or incorrectly performed.



### **Supervision of roles performed remotely**

Risks around staff having more access to areas of the business may also increase the risk of fraud or error. This means supervision of staff in changed and existing roles is increasingly important. Technology should be used where possible to assist in this supervision, for example access exception reporting, and limiting ability to read, edit or amend data.



### **Risk of external attacks**

External parties may see an increased opportunity to infiltrate systems while staff are working with remote working arrangements. Entities should monitor closely the use of new or changed systems to facilitate working remotely, to reduce the risk of external attacks.

Authored by Brydie Morris, Senior Manager, Queensland Audit Office.

Reproduced with permission from Queensland Audit Office.