

Navigating COVID-19 crisis – NFPs – cyber & technology



Communications

Guidance & Policy

Awareness & Alerts

Compliance Culture



Access

Access rights

Credentialling

Continuity plans

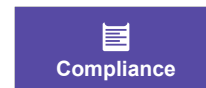


Supplier

Guidance & Policy

Service & Priority levels

Awareness & Alerts



Compliance

Monitoring

Privacy & Safety

Data sharing



Recovery

Capacity & Plans

Incident response

Restore

COVID-19 will expose your cyber vulnerabilities and place you 100% dependent on your technology for business survival

Your COVID-19 cyber and technology risks to monitor:

- You are responding and extending access to your working from home users including staff, contractors, community and suppliers
- You are relying heavily on your technology for business continuity
- Your ICT support may not be highly skilled to respond to these increasing threats and/or are busy on support and response and will need assistance to monitor the cyber risks and be ready to have capacity to recover against breaches
- You are at increased risk of placing your donor privacy and payment data at risk with a breach of your systems
- You will be revisiting access rights, user functionality, and providing maximum flexibility which may elevate fraud, breach and misappropriation risks
- Your staff will be in a different working environment and under stress leading to them relaxing their approach to financial controls, privacy and data sharing
- It is likely you will experience a breach you need to be ready to recover as your organization now depends on it.

How we can help?

Promote culture of compliance, assure your controls are effective and protect you

- We can provide you with a cyber and technology monitoring controls review to assure
- Alert you in a timely manner to gaps, emerging risks and escalating issues for mitigation
- Leverage our experience, capacity and templates to protect your organisation
- Provide assurance on your security so you can focus on business survival issues

Approach

- We will check in at agreed frequency on the status of your controls against the key focus areas of Communications, Access, Supplier, Compliance and Recovery for your cyber security and technology related risks
- We will interview your key staff, review your documents, incidents, monitoring data and assess your controls effectiveness
- We will provide you with a one page immediate actions and controls status report
- We will support you with templates that you may need for guidance, policy and recovery plans
- We will provide you with the communications to send to your staff to remind, on key emerging risk areas and their compliance.

MOORE STEPHENS