A Code for Sports Governance

UK Sport Guidance Note

Requirement 2.7 – Business Continuity and Succession Planning

uk sport

powering success
inspiring impact

Contents

Guidance Notes

Foreword

The revised Code for Sports Governance (the Code) was released by UK Sport and Sport England in December 2021. The requirement relating to an organisation's responsibilities towards business continuity, data recovery and succession plans was revised, giving renewed prominence to this important area.

Requirement 2.7 sets out that "The Board shall have in place continuity plans for the organisation and succession plans for orderly appointments to the Board and to key posts within the organisation."

This revised Requirement is accompanied by a detailed Commentary within the Code which is included in this guidance note. The Commentary is not prescriptive and does not contain any mandatory requirements, criteria or approaches. However, it is important to consider it when reviewing how you will comply with the Requirement.

The guidance in this note builds on that Commentary to further explore some of the key elements of this Requirement and to help with the development of your organisation's continuity, data recovery and succession plans, including templates and further resources that may be helpful.

It is important to note that the purpose of this guidance is to prompt thinking about what is right for your organisation. It is not a list of requirements but a guide to support you in working through how your organisation can strengthen its resilience and in meeting the requirement set out at 2.7 of the Code for Sports Governance.

This document provides:

- Guidance to help organisations develop business **continuity, data recovery and succession plans** in order to strengthen their resilience whilst seeking to comply with Requirement 2.7 of the Code. The guidance is separated into three sections – one for each of the three elements
- Links to examples of these plans that can be adapted and other useful sources of information
- Templates to enable Boards to develop plans that are right for their organisations

Code Requirement and Commentary

2.7 The Board shall have in place continuity plans for the organisation and succession plans for orderly appointments to the Board and to key posts within the organisation.

Code Commentary

A continuity plan is a document that outlines how an organisation will continue operating during an unplanned disruption in service.

Although often compiled by the Senior Management Team, the Board has overall responsibility as part of its risk management duties. Many Boards appoint one of its Directors to champion these matters.

Typically, the continuity plan outlines the risks as well as the structure of how to prevent, respond and recover from a disruptive event. Generally, this involves identifying the possible disruption risks and potential impact if they occur, planning an effective response to their occurrence, allocating roles and responsibilities, communication responses, testing the plan and training in response to that testing, to ensure an effective response. There are often three parts to this plan: an organisation's continuity plan; a data recovery plan; and a succession plan.

It is important that organisations take the time to plan ahead for both foreseen and unforeseen eventualities, be they positive or negative. There are typically three pillars to this kind of planning – continuity, data recovery and succession. They will sit alongside, and be informed by, the organisational strategy, operational plan and risk register, looking to the future, being mindful of plans the organisation has for the short, medium and long term, and being prepared for potential negative (or positive) situations that may arise. Whilst operational staff are likely to be involved in putting these plans together, it is important that the Board has oversight of these.

This guidance will look at each strand of Requirement 2.7 in turn:

1. **Business continuity**
2. **Data recovery**
3. **Succession planning**

There is clearly overlap between the three strands, and the approaches taken to effective planning for each are similar.

Business Continuity

Business Continuity

Content and Scope

This section provides advice and guidance on preparing, writing and maintaining a **business continuity plan** for your organisation. It's important that all organisations take the time to think carefully about what your organisation does, how it does it (the business processes), how those processes are supported and plan appropriately for how to resume a state of business as usual in the event of an interruption or disaster. This guidance takes you through the steps to putting in place an effective business continuity plan that is right for your organisation. Specifically, we look at how to take stock of the systems, people and resources that enable your organisation to function, consider the impact of the loss or an interruption to any of those, how to mitigate those risks, and how to get things back up and running again.

Code Commentary

Continuity Plan

An organisation's continuity plan is a broad plan designed to keep an organisation running, even in the event of a disaster. This plan focuses on the organisation as a whole but drills down to specific scenarios that might create operational risks. With organisation continuity planning, the aim is to keep critical operations functioning, so that your organisation can continue to conduct regular organisation activities even under unusual circumstances.

When followed correctly, an organisation's continuity plan should be able to continue to provide services to stakeholders, with minimal disruption, either during or immediately after a disaster. A comprehensive plan should also address the needs of an organisation's partners.

The continuity plan itself should live as a written document that outlines the organisation's critical functions. This is likely to include a list of critical supplies, crucial organisation functions, copies of important records, and employee contact information.

The information included in the plan should allow the organisation to be up and running as soon as possible after a disruptive event has occurred.

What is business continuity?

Business continuity refers to planning designed to keep your organisation running in the event of a major disruption or disaster, be it a flood or snowstorm, sudden absence of your CEO, a power outage or a cyber-attack.

In light of the Covid 19 pandemic, effective business continuity plans should also consider how to manage staff absences, the ability to quickly work from home and adapting services to online delivery, for instance.

There is no one-size-fits all approach to business continuity planning. Each organisation needs to carefully consider what the organisation does, how it does it, who is involved, and where those activities are based.

The information below is not intended to be detailed guidance, but to provide support to enable organisations to demonstrate that the Board and relevant parts of the organisation have taken the time to consider potential incidents, what impact they might have, how you might reduce that impact, and how the organisation will recover from it.

What should a continuity plan cover?

An effective continuity plan should cover the following:

Responsibilities – Identify who is the lead in each area in the event of a major disruption and allocating responsibilities to them. Whilst the Board should have oversight and sign off on plans, the executive will have responsibility for leading on planning the process, most often supported by a committee/group from across the organisation. It is important that all staff be made aware of the plan; and that you ensure you have proxies in place in the absence of a lead member of the team.

Inventory – Where applicable, involve staff from across the organisation to form a complete picture; detail what you have in place now that enables your organisation to function; and think about your critical supplies, organisational functions, parts of your business, services you provide.

Determine your organisation's key resources, which may include:

- People – staff, coaches, volunteers, athletes, participants, other 'customers', suppliers, funders, landlord
- Premises (including for instance daily training environments for athletes, offices for staff)
- Systems (including finance, HR, payroll, databases)
- Data (including passwords, contact databases to enable your work to continue). This links also to your data recovery plan
- Equipment (including eg. laptops, supplies)
- Documents (including banking information, HR documents, utility bills, other key documents you hold either on paper or electronically)
- External contacts (funders, suppliers, bank, accountants, insurance, utility companies)

Involve staff at different levels from across the business in plotting this information – they may be aware of risks that more senior colleagues won't be aware of. The Board should ultimately have responsibility for this whole process.

Impact analysis – Consider what the potential impact is on each of the things you have identified in your inventory. Think in terms of, for example, loss of income, increased expenses, disruption to service, damage to reputation, delay in activities, regulatory fines, safeguarding issues. It is important to consider interdependencies, for example, if a major disruption arose with a supplier of sports equipment, what impact would that have on your ability to carry out your organisation's operational functions?

Risk analysis – Think of the potential risks that may result in a major disruption, along with the likelihood of that risk occurring, for example, a natural disaster, cyber attack, infectious disease, biological hazard, gas leak or power cut. Think about how your different systems or resources interact with others when considering the risks.

Preventing/mitigating risk – Consider the steps that should be taken to prevent entirely, or to mitigate or minimise the risks that have been identified. Taking the examples above, this might include, for example, data security systems to prevent a cyber attack, infectious disease policies and processes.

How to manage impact – This might include the ability to quickly move to homeworking, backing up systems, temporarily moving offices or delivering services in a different way. If you're reliant on third parties for delivering your systems, talk to them about their continuity plans. Think of having key information in multiple places, potentially in hard and electronic format.

Prioritise – Work out how long you can tolerate each element of your business being down, with priority given to those with the least amount of time tolerated. Note that this may change throughout the week/month/year. For instance, a problem impacting payroll systems which will be more time critical at different times of the month to ensure that staff are paid in a timely way.

Consider too in practical terms how long it will take to fix the interruption. If realistically that takes longer than can be tolerated, think about what back-up plans you can put in place now to reduce that time.

Emergency contact – Identify key contacts, both internally and externally, who need to be informed of the disruption. This may change over time so it will be important to think of different scenarios and review this regularly. This contact list is likely to include all staff, volunteers, linked organisations, funders, suppliers, insurance company, etc.

Cascading information – Develop a communication plan/pyramid to inform employees about the incident and keep them updated as to progress with resolving the incident. This should include employee contact information. Consider developing an external communication plan (or building this into an existing communication plan) with nominated spokespersons available to engage with the media if appropriate.

Contingencies – Consider what contingency plans can be put in place, for instance, regarding equipment (eg. hiring laptops), temporarily moving to a new premises. Consider the costs for these. It may be possible to put in place reciprocal arrangements with other organisations.

Action log – It is important to keep a log of all actions taken. This will help review where improvements can be made for the future, and is also useful in any insurance claim. In this regard, keep a note of any costs incurred.

Test – The continuity plan should be periodically tested in a simulated environment to ensure that it can be implemented in emergency situations and that the management and staff understand how it is to be executed. Your plan should be written in plain, jargon-free language. Ensure as a minimum that everyone in the business has read it and, ideally received training.

Ownership – Accountability for business continuity should be clear, detailing who is responsible for which aspect (with appropriate training). The business continuity plan should have executive level sponsorship, with the plan reviewed and signed off by the Board. This should include contingencies, with a second named deputy in the event of the absence of the lead.

Storage and accessibility – Store the plan in multiple locations so if, for instance, a shared drive is compromised, the plan can be accessed from another system and/or in hard copy.

Regular review – Business continuity plans should be regularly reviewed, as a minimum annually. The plans should also be reviewed when any key changes are made, such as moving to a new premises. Further, the plan should be reviewed after any need to have enacted the business continuity plan to assess what worked well and what didn't.

We would recommend where possible to seek professional guidance on your continuity planning. The above is intended as guidance on the general themes to consider. It is important for any organisation carrying out a continuity planning exercise to consider carefully what is appropriate for your organisation.

Some useful links

Here are some links to useful guidance giving more detailed information on data recovery planning which we would encourage you to look at. This also includes some useful templates you may want to adapt for your organisation:

How to write a business continuity plan

Introduction to Business Continuity

ISO 22301 – Business continuity

Guide to implementing the ISO standard

Data Recovery

Data Recovery

Content and Scope

This section provides advice and guidance on preparing, writing and maintaining a **data recovery plan** for your organisation. It's important that all organisations take the time to think carefully about what your organisation does, how it does it (the business processes), and how those processes are supported (by software, hardware and people), and plan appropriately for how to mitigate an interruption to those systems. This guidance takes you through the steps to putting in place an effective data recovery plan that is right for your organisation. Specifically, we look at how to identify those data systems, consider the impact of the loss of that data, how to mitigate those risks, and how to get things back up and running again.

Code Commentary

Data recovery plan

A data recovery plan is a more focused, specific part of the wider organisation's continuity plan. It has a narrow focus on the data and information systems of an organisation. In simple terms, a data recovery plan is designed to protect data with the sole purpose of being able to recover it quickly in the event of a disaster. With this aim in mind, data recovery plans are usually developed to address the specific requirements of the IT department to get back up and running, which ultimately affects the organisation as a whole.

Depending on the type of disaster that occurs, the plan could involve everything from recovering a small data set to an entire data centre. Most organisations are heavily reliant on information technology, which is why the data recovery plan is such an important part of successful organisation continuity planning.

In some cases, data recovery planning may also refer to protocols that exist outside the IT department. For example, data recovery plans could include steps for initiating a backup location, so critical operations can be resumed. This might be useful in the event of an environmental disaster, such as flooding, which might render the existing organisation premises unusable. The plan might also include guidance on how to restore communication between emergency staff if the usual communication lines are unavailable. If your IT department is creating an IT-focused plan, you should include all non-IT recovery protocols in the wider organisation continuity plan.

What is data recovery?

Data recovery is closely linked to business continuity planning, and should form a part of your data protection policies.

Data recovery planning has a narrow focus on IT and data systems – planning for how to keep your organisation's data secure in the event of a major disruption, be it a natural disaster, a power outage or a cyber attack. Effective planning will enable your organisation to keep running in the event of a significant disruption, and be able to get back up and running as soon as possible.

An incident management plan (IMP) focuses on protecting sensitive data **during** an event, and defines the scope of actions to be taken during the incident, including the specific roles and responsibilities of the incident response team.

In contrast, a data recovery plan (DRP) focuses on defining the **recovery** objectives, and the steps that must be taken to bring the organisation back to an operational state after an incident occurs

There is no one-size-fits-all approach to effective data recovery planning. It is crucial to ensure plans are appropriate for what your organisation does, your IT systems and your infrastructure.

The purpose of this guidance is not to provide detailed, technical advice, but to support you in demonstrating that your Board and relevant parts of the organisation have taken the time to consider potential incidents, what impact that might have, how you might reduce the impact, and how to recover from it.

Why is data recovery planning important?

A loss of data can have serious consequences, from disrupting core services to impacting the organisation financially or damaging its reputation.

Key to effective data recovery planning is a thorough consideration of what the organisation does and how it does it, and then identifying what IT and data systems support that work. In many cases, more than one IT system will support an individual activity.

This will include everything from data which supports operational activity, to payroll systems, to email. Taking payroll as an example, to ensure that staff are paid on time, both the payroll and finance systems need to be working effectively, so it will be important to consider both.

Please note that for many organisations, at least some of the IT infrastructure is outsourced to external providers. Many core IT systems will also be hosted by external providers, eg. Office 365, cloud data storage, accounting software, contact management systems, etc. This should be factored into your planning.

What should a data recovery plan cover?

An effective data recovery plan enables the organisation to get IT systems back online, and data secured and available, thereby supporting business continuity. It should detail:

Inventory – Where applicable, involve staff from across the organisation and create an inventory of the work that your organisation does, and the systems and data you have in place to support it. Identify what data you have and where it is stored.

This should start from the more obvious things like email, payroll, HR and finance software and include any databases or other IT systems specific to your organisation. List out all laptops, computers, servers, cloud systems.

This inventory should include internally-hosted systems as well as ones that are externally-hosted and/or outsourced. Where an IT system is outsourced, the third party should have their own data recovery plan, although be aware that they may need to be asked to develop one.

When carrying out an inventory of IT systems, it is important to think of key software that, for example, may only be installed on only one person's laptop. Whilst this should be avoided, where this may be unavoidable, it is important to ensure adequate back-up and alternative log-ins. This might include, by way of example, installing the software on a separate laptop, stored off site or in a fireproof safe, installing it on someone else's computer, ensuring passwords are held securely but accessible in the event of need.

Responsibilities – IT systems aren't just about the software or hardware involved, but the people that use them. Identify who is the lead in each element of your IT and data systems in the event of a major disruption and what responsibilities they have.

Whilst the Board should have oversight and sign off on plans, the executive will have responsibility for leading on planning the process, most often supported by a committee/group of those involved in data recovery to plan the process.

The planning group should be from across the organisation where IT systems are used, including colleagues with responsibility, for example, for HR/Payroll, finance, CRM or other databases, as well, of course, as IT. It is important that all staff be made aware of the plan.

Where possible, include proxies in case of the absence of the lead. Think too about different levels of authority. For instance, if the finance system were to go down, are specific people only authorised at specific levels – how will you manage that?

Risk analysis – Identify the risk to each element in the event of a major disruption. It should be noted that a major disruption to data should be included in your organisation's risk register. Think about what could go wrong with each element you've identified in the inventory.

Impact analysis – Having completed the inventory and the risk analysis, the next step is to take each of the elements that have been identified in turn and consider the impact on each of these if they were compromised in a disaster. This should include the potential impact of an incident effecting something which is outsourced but would have an impact on your internal systems. Taking each system in turn, think about what aspects of your organisation's work would be affected.

Prioritisation – Identify how long your organisation can tolerate each element of your IT systems being down, with priority given to those with the least amount of time tolerated. It should be noted that this may change throughout the week/month/year. Consider for instance a problem impacting payroll systems which will be more time critical at different times of the month to ensure that staff are paid in a timely way. This prioritisation exercise should include how frequently each system should be backed up. For example, a system which you have identified as having a maximum tolerated down time of four hours, will need to be backed up at least every four hours. Other systems may be able to be backed up once overnight.

It is important to think of how systems interrelate, for instance, finance systems impacting on payroll. What is the impact if each of these stopped working, and what is the amount of time your organisation could tolerate them being out of operation?

Consider too in practical terms how long it will take to fix the problem. If realistically that takes longer than can be tolerated, think about what back-up plans you can put in place now to reduce that time. For instance, if a key piece of software is installed on only one person's laptop that, if damaged, could take weeks to replace (new laptop needed, specialist support in installing the software, reuploading the data), could you minimise that impact by installing the software on another laptop that is stored somewhere securely?

How to prevent/manage impact – Develop a plan to deal with the loss of each system. This is likely to include backup systems that you can bring back online, for instance, the use of webmail in the event of Outlook being compromised but could also include hiring laptops or other workarounds. This part of your plan should, for each element you've identified, detail the steps you would take to restart the system, reconfigure, and recover any lost data.

Emergency contact – Identify key contacts, both internally and externally, who need to be informed of the disruption. This may change over time so it will be important to think of different scenarios and review this regularly. This contact list is likely to include all staff, volunteers, linked organisations, funders, suppliers, insurance company, etc.

Cascading information – Develop a communication plan/pyramid to inform employees about the incident and keep them updated as to progress with resolving the incident. This should include employee contact information. In more serious cases, you may need to consider having an external communications plan and lead person in place.

Contingencies – Consider what contingency plans can be put in place, for instance, backing data up on the cloud if your organisation doesn't have its own data centre . Larger organisations may have their own data centre, smaller organisations are unlikely to.

Action log – It is important to keep a log of all actions taken. This will help review where improvements can be made for the future, and is also useful in any insurance claim. In this regard, keep a note of any costs incurred.

Test – The data recovery plan should be periodically tested in a simulated environment to ensure that it can be implemented in emergency situations and that the management and staff understand how it is to be executed.

Ownership – Accountability for data recovery should be clear, detailing who is responsible for which aspect (with appropriate training), with named deputies in the absence of the lead person. The data recovery plan should have executive level sponsorship, with the plan reviewed and signed off by the Board.

Regular review – Data recovery plans should be regularly reviewed, as a minimum annually. The plans should also be reviewed when any key changes are made, such as new software being implemented. Further, the plan should be reviewed after any need to have enacted the data recovery plan to assess what worked well and what didn't.

We would recommend where possible to seek professional guidance on your data recovery planning. The above is intended as guidance on the general themes to consider. It is important for any organisation carrying out a data recovery planning exercise to consider carefully what is appropriate for your organisation.

Some useful links

Here are some links to useful guidance giving more detailed information on data recovery planning which we would encourage you to look at. This also includes some useful templates you may want to adapt for your organisation:

What is a Disaster Recovery Plan (DRP) and How Do You Write One?

12 key points a disaster recovery plan checklist must include

Data backup plan template (Download PDF)

How to write a disaster recovery plan

Disaster recovery planning template (Download PDF)

IT Disaster Recovery Plan and Process Guide

National Recovery Guidance: common issues

Disaster recovery guidance

Recovery plan guidance template (Download Word doc)

Disaster recovery plan

Succession Planning

Succession Planning

Content and Scope

This section provides advice and guidance on preparing, writing and maintaining a **succession plan** for your organisation. It's important that all organisations take the time to think about how the business would manage in the absence of a member of their senior team, as well as setting out a strategy for identifying and developing future leaders at your organisation.

Code Commentary

Succession plan

In addition to continuity planning, organisations should have succession plans in place. Succession plans often focus on the longer term and may cover areas such as the development of junior colleagues into more senior roles.

They can also help in the event of a short-notice departure or temporary, unexpected absence from the Board by indicating how best to assign temporary responsibility for the roles and responsibilities of the Director in question.

Effective succession planning reduces the risks associated with the loss of experienced leadership and helps maintain a diverse and appropriate balance of skills, backgrounds and experience within the organisation and on the Board.

It also ensures progressive refreshing of the Board and enables swift action in response to abrupt changes to the Board or senior management, helping to reduce any associated risks or costs.

Succession plan continued

Succession plans should include, but are not limited to, a record of term end dates for each Board member; any key roles and responsibilities (e.g. Senior Independent Director, Welfare and Safety lead and Audit Chair); an agreed process and timeline for recruitment of new Directors linked to term end dates; an agreed process and timeline for onboarding and induction of new Directors, including provision for handover between incoming and departing Directors; and links to the skills and diversity needs of the Board to support consideration of these factors during recruitment.

It is for the organisation to determine which positions within senior management should be captured by the succession plan, but at the very least the plans should include the CEO (or equivalent) and any members of the Senior Leadership Team.

Senior leaders are employees and not subject to term limits like Board roles, therefore changes will be less predictable. When considering succession planning for senior leaders it is also important to be conscious of employment law rights and the organisation's own human resources policies and procedures (e.g. in relation to recruitment and talent development). To mitigate the risk when a senior employee departs it is helpful to ensure key organisational information is shared rather than retained by a single individual.

Succession planning for senior management typically considers how a critical function would be covered if an individual leaves as well as identifying the potential and development needs of individuals already in the organisation.

Oversight of succession planning may be the responsibility of the HR function but the Board (in particular, the Nominations Committee) and CEO will generally need to be involved.

What is succession planning?

The Code defines succession planning as a management exercise intended to ensure the organisation will be stable and still have the skills it needs when people at a senior level leave. Organisations should identify and develop potential future leaders. Plans should cover cases where an individual is due to finish their final term on the governing committee or will retire soon but also what happens if somebody leaves unexpectedly. For example, an organisation should work out who would cover the functions of the chief executive if they leave.

Typically CEO succession planning includes both the immediate response, such as identifying others internally who would take on the work on a temporary basis, as well as the longer-term approach. In this case, the organisation might search for a replacement through open recruitment.

Note – in this guidance, we are using the terms Board member and Director interchangeably

What should a succession plan cover?

The importance of succession planning in a sport organisation is not to be underestimated. Most sport organisations rely on specialist skills and organisational knowledge amongst a relatively small number of personnel. As such it is common for the loss of personnel to be identified as a strategic risk, particularly within smaller bodies. Since term limits apply to members of the Board and a certain level of staff turnover is to be expected, succession planning is an important component of responsible governance.

The objective of the succession plan is to ensure:

- The successful functioning of a sport organisation now and in the future as part of the overall risk management strategy;
- Adequate planning for changes in Board membership and key personnel, both foreseen and unforeseen;
- Identification and development of future leaders.

Succession planning should be carried out alongside business continuity planning, both of which are informed by:

- The Board skills audit – identifying what skills the Board collectively currently has, and where there are any gaps
- Tthe organisation's Diversity and Inclusion Action Plan
- The organisation's People Plan
- The organisation's strategic plan, looking ahead to what skills are needed around the Board table to achieve that strategy
- The risk register

A succession plan typically includes:

- Dates of terms for each member of the Board
- Key roles and responsibilities of each Board member (eg. Senior Independent Director, Welfare and Safety Lead, Chair of Audit Committee, etc.)
- Timing of expected vacancies, skills gaps and diversity needs. This will be linked to your strategic plan, skills audit.
- Process and timeline for the recruitment of Board directors, linked to term end dates (this may tie in with your Board recruitment policy and Diversity and Inclusion Action Plan)
- Process and timeline for onboarding and induction of new Board members, including provision for handover between departing and incoming Board members. This will be your Board member induction process.
- In addition to handover, provision for ensuring knowledge and information isn't lost with the departing Board member, eg. ensuring files are stored centrally rather than on personal PCs
- Succession and development planning for senior staff
- Succession planning for staff – further detail by function
- Priorities for identifying and developing potential future leaders
- Emergency succession planning for departure of Chair or CEO (or absence of more than three months)
- Emergency succession planning for departure of Director with a specific role which risks the Board breaching the provisions of the Articles

Defining the scope

The first step in succession planning is to define its scope.

Directors

The Code provides that Board members should be subject to term limits.

Code Requirements

1.6 Subject to the exceptions set out in Requirement 1.7 below, a Director may serve on the Board for a number of consecutive terms, each term being no more than four years in length, up to a maximum of nine years continuous service.

The choice of term limits will set a clear time structure in which to plan for succession of Directors and it is recommended that a table is used to provide an at a glance summary of Board member terms.

It is however possible that a Board member may not complete the available term and the succession plan must be sufficiently flexible to deal with such unplanned changes.

Senior Management Team

The succession plan should also cover the Senior Management Team and any other role where a sole individual possesses critical skills and/or organisational knowledge.

Such roles, unlike Board roles, are not subject to term limits and changes are therefore less predictable. In addition, the personnel will be employees and accordingly it is important to be conscious of employment law rights.

Nevertheless, it is advisable for the organisation, where possible, to balance individual expertise and operational knowledge with a collaborative team approach. In particular, steps should be taken to ensure that key information for the organisation is shared rather than retained by a single individual. It is important to consider the organisation's Diversity and Inclusion Action Plan.

Point to note

- It is important to keep in mind that the act of succession planning itself, such as identifying "deputies" or pools of successors for different roles, impacts on staff and Board members. The potential effect on individuals should be considered sensitively when conducting the succession planning exercise.

Process

Succession planning typically combines a process-centric approach (identifying how to cover a critical function if an individual leaves) with a people-centric approach (identifying the potential and development needs of individuals already in the organisation).

Oversight of succession planning may be the responsibility of the HR function. However, the Board and CEO will generally need to be involved, and should maintain oversight.

Process summary and checklist

No.	Action
1.	Ensure strategy is up-to-date and informs requirements for skills and expertise
2.	Ensure Board skills audit is up-to-date
3.	Update Board membership table with dates of terms and eligibility for re-appointment, plotting out sufficient lead-in time for appointing replacements
4.	Identify potential skills gaps which will arise and committee roles that will become vacant when Board members leave. Think also of the diversity make-up of the Board, as well as key stakeholder contacts that individuals hold
5.	Update table of Senior Management Team, identifying immediate / emergency cover, resources to be put in place in 0-1 year, a 1-3 year plan and considerations for 3-5 years, if appropriate
6.	Where needed, identify pools of substitutes for specific areas of responsibility of the Senior Management Team
7.	Linked to the People Plan, develop plans for identifying and developing potential future leaders.
8.	Develop emergency succession plans in the event of the unexpected departure of the Chair, CEO or a Director where this would risk the Board breaching the provisions of the Articles
9.	Prioritise succession planning and talent development activity based on budget availability
10.	As with all policies, include the date the policy is signed off by Board, and when it is next due for formal review. Note that the succession plan should be a live document and, as a minimum, referred to with sufficient time ahead of planned turnover.

Some useful links

Here are some links to useful guidance giving more detailed information on data recovery planning which we would encourage you to look at. This also includes some useful templates you may want to adapt for your organisation:

Factsheets | CIPD

Importance of a Good Leadership Transition

A guide to get it right

Business Continuity Planning
Templates

Below are some examples of business continuity planning tools that you can adapt for your own organisation. **These are just examples. As highlighted in the guidance, you will need to take time to carefully develop your own plans, which may need to be more complex than these simple examples.**

Example of a simple inventory and risk/impact analysis

Function/ Resource	Lead Directorate	Risk	Impact	Likelihood	Length of time tolerated before alternative arrangements in place	Mitigation	Contingency	Priority	Owner	Interacts with other functions?
Eg. Offices	Corporate services	Flooding	Inability to use premises. Damage to property and resources	Low	4 hours	Ensure flood defences are implemented.	All staff have laptops. Switch to homeworking	High	Chief Operating Officer	All
Eg. Payroll	HR	System outage	Inability to pay staff		2 days. 1 day or less if outage occurs within 1 day of pay run		Backup payroll system, manual payments	High	HR Director	Finance

Example of a simple continuity planning document to be used for each function/resource

Function/resource	Office premises
Directorate	Corporate services
Location	Address of office
Risk score	Medium
Impact	High
Lead contact (name, email, phone)	Xxxx
Second contact (name, email, phone)	Xxxx
Priority rating	High

Immediate actions	Responsibility	Log of actions taken	Estimated cost
Inform all staff and board Evacuate office Inform landlord Inform utility providers Inform insurance company			
Interim actions	**Responsibility**	**Log of actions taken**	**Estimated cost**
Switch to home working with use of laptops Manage insurance process Potential move to alternative premises if necessary			
Subsequent actions	**Responsibility**	**Log of actions taken**	**Estimated cost**
Repair damage to premises Replace damaged equipment Return to office			
External contacts	**Responsibility**	**Log of actions taken**	**Estimated cost**
Landlord Utilities providers Key stakeholders/funders Insurance provider			

Example of a simple contact sheet

Setting out leads for each area. Each lead would then be responsible to cascading to their teams

Name	Role/Title	Lead area(s)	Alternative email address	Work Phone Number	Mobile Phone Number	Home Phone Number

Example of a simple contact sheet for key external contacts

Name	Role/Title	Organisation and IT system responsible for	Email address	Phone Number	Mobile Phone Number

Data Recovery
Templates

Below are some examples of business continuity planning tools that you can adapt for your own organisation. **These are just examples. As highlighted in the guidance, you will need to take time to carefully develop your own plans, which may need to be more complex than these simple examples.**

- **Example data recovery plan template:**

Data recovery plan for x organisation

Purpose

This document sets out our policies and procedures for technology disaster recovery, as well as our process-level plans for recovering critical technology platforms and the telecommunications infrastructure. This document summarises our recommended procedures. In the event of an actual emergency situation, modifications to this document may be made to ensure physical safety of our people, our systems, and our data. Our mission is to ensure information system uptime, data integrity and availability, and business continuity.

Data recovery policy statement

The organisation shall develop a comprehensive IT and digital disaster recovery plan.

- A formal risk assessment shall be undertaken to determine the requirements for the disaster recovery plan.
- The disaster recovery plan should cover all essential and critical infrastructure elements, systems and networks, in accordance with key business activities.
- The disaster recovery plan should be periodically tested in a simulated environment to ensure that it can be implemented in emergency situations and that the management and staff understand how it is to be executed.
- All staff must be made aware of the disaster recovery plan and their own respective roles.
- The disaster recovery plan is to be kept up to date to take into account changing circumstances

Objectives

The principal objective of the disaster recovery program is to develop, test and document a well-structured and easily understood plan which will help the organisation recover as quickly and effectively as possible from an unforeseen disaster or emergency which interrupts information systems and business operations. Additional objectives include the following:

- The need to ensure that all employees fully understand their duties in implementing such a plan
- The need to ensure that operational policies are adhered to within all planned activities
- The need to ensure that proposed contingency arrangements are cost-effective
- The need to consider implications on other organisation sites
- Disaster recovery capabilities as applicable to key stakeholders

Potential risk areas

There are several areas of risk specific to IT and digital. [X organisation] considers the following to be the most significant for our context:

- Data storage and recovery
- Cyber attack which compromises our data
- Business systems, including HR systems, coaching course systems, athlete records, finance systems, email systems, website

Cyber security training and accreditation

All staff are required to complete online cyber security training. This should be at a level appropriate to their responsibilities in terms of data handling and management.

Example of a simple inventory and risk/impact analysis

Function/ Resource	Lead Directorate	Where hosted	Risk	Impact	Likelihood	Length of time tolerated before alternative arrangements in place	Mitigation	Contingency	Priority	Owner	Interacts with other functions?
Eg. Outlook email system	IT	Office 365	System outage/ cyber attack	Inability to carry out normal business across all functions	Medium	4 hours	IT security systems	Ensure have alternative contact for all staff ie. phone numbers, stored in multiple locations. Temporary switch to webmail. Contact all staff via alternative contact using phone numbers stored	High	IT director	All
Eg. Payroll	HR	Outsourced payroll provider	System outage	Inability to pay staff		2 days. 1 day or less if outage occurs within 1 day of pay run		Backup payroll system, manual payments	High	HR Director	Finance

Example of a simple data recovery planning document to be used for each function/system

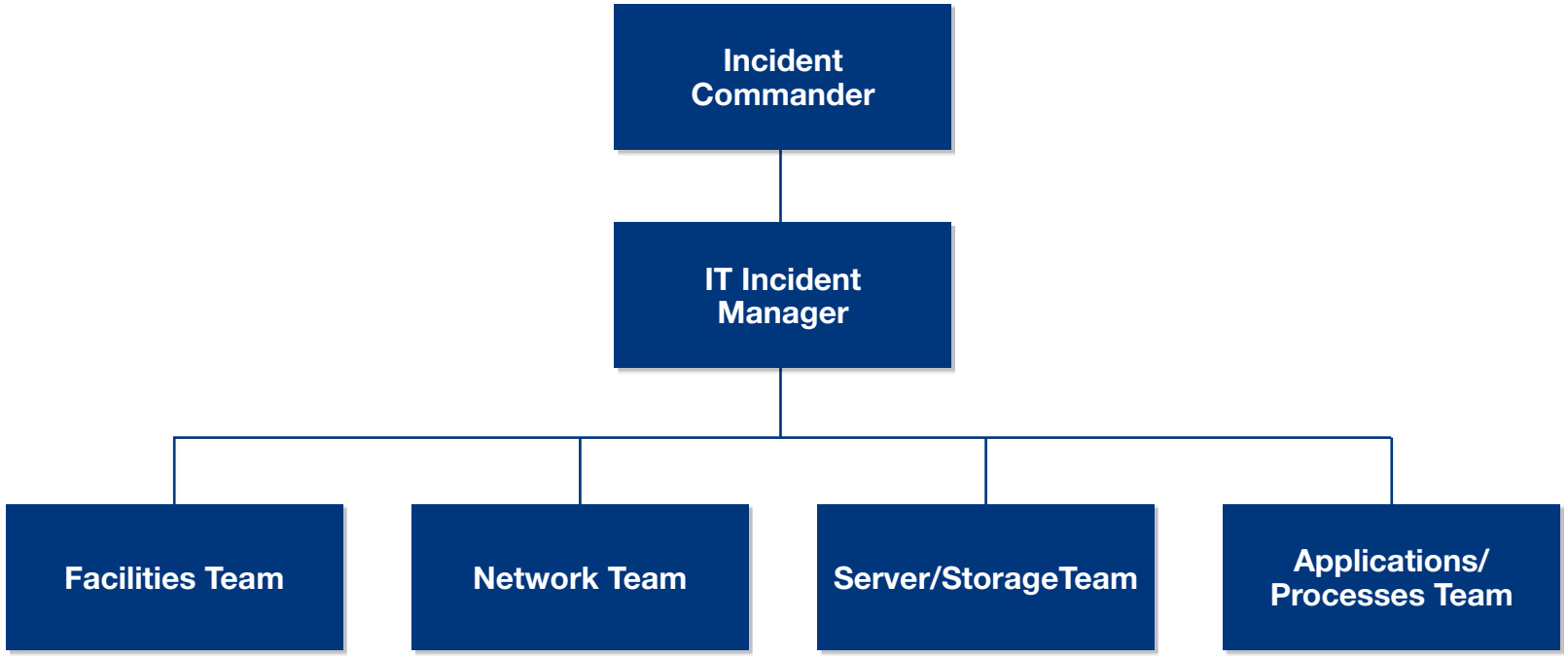
Function/system	Outlook email system
Directorate	IT
Location	Office 365
Risk score	Medium
Impact	High
Maximum tolerated down time	4 hours
Lead contact (name, email, phone)	Sally Smith
Second contact (name, email, phone)	Annie Other
Priority rating	High

Immediate actions	Responsibility	Actions taken log	Estimated cost
Ensure webmail is unaffected. Switch to webmail			
Interim actions	**Responsibility**	**Actions taken log**	**Estimated cost**
Communicate switch to staff using alternative contacts (eg. phone). Liaise with Microsoft			
Subsequent actions	**Responsibility**	**Actions taken log**	**Estimated cost**
Outlook restored. Communicate resolution to all staff			
External contacts	**Responsibility**	**Actions taken log**	**Estimated cost**
Office 365 Key stakeholders			

Example of a simple contact sheet

Name	Role/Title	Lead area(s)	Work Phone Number	Mobile Phone Number	Home Phone Number

Example hierarchy for each function/system identified



Succession Planning
Templates

Succession planning for the Board and senior staff

Below are some examples of succession planning tools that you can adapt for your own organisation. **These are just examples. As highlighted in the guidance, you will need to take time to carefully develop your own plans, which may need to be more complex than these simple examples.**

1. Dates of terms of members of the Board

The table below can be used to set out the dates of terms of members of the Board

Board member	Type	Appointed date	End of 1st term date	End of 2nd term date	End of 3rd term date	End of final term
1	Eg. Chair/Welfare and Safety lead/ Treasurer					
2						
3 etc…						

2. Timing of expected vacancies and skills gaps

The table below will assist the Nominations Committee to identify in good time dates when vacancies may arise and to note potential skills gaps that will result, informed by the findings of a skills audit exercise.

When the term of an individual with key knowledge about the organisation is due to come to an end, a process should be put in place to enable information sharing.

The table may also be of use if there is an unforeseen change to the Board.

Date vacancy will arise	Date for Nominations Committee to begin activity	Board member name and, if appropriate, role	Potential skills gap(s)	Committee role(s)	Relationships with key stakeholders
1/12/2023	1/7/2023	[NAME] Treasurer	Financial expertise	Audit Committee Strategy Working Group	Key contact with major funder
1/12/2024	1/7/2024	[NAME], Nominated Director	Social media marketing	Communications	Local council

3. Succession and development planning for senior staff

The table below is intended as a guide to responding to abrupt changes in the Senior Management Team (SMT) and to help to reduce any associated risks or costs. The immediate task in each case would be to identify business critical priorities for that role which require immediate/emergency cover. The next step would be to put in place resources which can be ready in 0-1 year. It may also be appropriate to consider what the organisation will need in 1-3 years. For staff roles some thought may be given for 3-5 years into the future.

Staff member	Position	Appointed date	Immediate / emergency cover	0-1 years	1-1-3 years	3-5 years
[NAME]	CEO		Chair of Board	Interim CEO appointed	Permanent recruitment	
	Performance Director		Head of Performance Operations	Interim PD appointed	Recruitment	[Any consideration linked to long-term strategy]
	Finance Manager		Chair of Finance	Interim Appointed	Recruitment	
	HR Manager		Secure Temp / Secondment with assistance of Chair of HR	Interim Appointed	Recruitment	
	Head of Media and Communications		PR and Media Officer	Interim Appointed	Recruitment	

4. Succession planning for staff – further detail by function

In some cases, the most practical solution may be for specific functions that are currently the responsibility of a single individual to be allocated to different colleagues to manage workloads. Appropriate talent development activity to develop capacity can then be identified and prioritised. It is important that information is actively shared among relevant staff so that key knowledge is held by more than one individual. For example, the CEO and an executive Director should maintain regular dialogue.

Talent development activity should take full account of the organisation's Diversity and Inclusion Action Plan.

Staff role	Functions	Immediate / emergency cover	Talent development activity
CEO	Chairing SMT	Director of Operations	Other members of SMT gain experience chairing internal meetings, or SMT if the CEO is unavailable
CEO	Representing SMT at Board	Director of Operations	
CEO	Accounting Officer	Finance Director	Finance Director participates in Accounting Officer duties
CEO	Spokesperson for the organisation	Head of Media and Communication	Identify opportunity for Head of Media and Communication to act as spokesperson on a particular project or topic
Finance Director	Director functions	Finance Manager	Specific training, as needed

5. Development priorities, based on succession planning needs

Area of expertise	Date when skills gap may arise	Example of suggested action
Governance	1/3/2023	Induction for new director(s), training for existing director(s)
Experience of the sport at elite level from a non-traditional background – recommendation from Diversity and Inclusion Action Plan	1/1/2023	Mentoring for committee members [NAME] identified as having potential to join the board
		Opportunity for staff identified as having potential to join senior management team to join/lead a project group
		Invitation to candidate for a Board vacancy who are identified as having great potential but not successful on this occasion, to participate in another committee or project

Suggestions for further development activity should emerge as part of the appraisal process. The organisation seeks to foster a culture of ongoing development among staff and to ensure that critical knowledge is shared rather than being limited to specific individuals.

6. Emergency succession planning for departure of Chair or CEO (or absence of more than three months)

Immediate action	Responsibility	Timescale
Agree who will be the spokesperson for the organisation	Chair for CEO; Board for Chair	Week 1
Agree a communication plan for key funders and stakeholders, including staff and contractors	Board (supported by CEO and senior management)	Week 2
Identify the interim CEO or Chair and consider additional temporary compensation	Board	Week 2/3
Define the interim CEO's responsibilities, authority and decision-making limitations	Board	Week 2/3
Identify board support for and supervision of the interim CEO	Board	Week 2/3
Start recruitment process for new CEO or Chair (see separate guidance on recruitment)	Nominations Committee	Week 2/3
Confirm that the CEO or Chair will not return to their post	Board	Week 4

7. Emergency succession planning for departure of Director

with a specific role which risks the Board breaching the provisions of the Articles (e.g. number of Nominated Directors) (or absence of more than three months)

Immediate action	Responsibility	Timescale
Agree on legal position in relation to Articles of Association / Terms of Reference	Chair, with legal advice as needed	Week 1
Agree communications plan for the board, key funders and stakeholders, including senior staff	Board (supported by CEO and senior management)	Week 2
Identify an interim solution	Board	Week 3
Start recruitment process for new Board member (see separate guidance on recruitment)	Nominations Committee	Week 4
Communicate plan more widely	Board	Week 4

Budget commitment

The agreed budget allocation for talent development in the current financial year is X, of which Y is ring-fenced for succession planning in particular.

The budget allocation for executive recruitment in the current financial year is X, of which Y is earmarked for roles A and B.

Approval and review

This succession plan has been considered and approved by the Senior Management Team / Board / other committee.

Last reviewed: [DATE]

Due for next review by: [DATE]

Legal disclaimer

This guidance has been prepared and made available for general information purposes only. The information herein does not constitute legal advice, nor should you rely solely on this guidance or the templates provided to assess risk or make plans.The content may be, or may become, inaccurate or incomplete and particular facts unique to your situation may render the content inapplicable to your situation. This guidance is but one source of information available to you. You may wish to consider multiple sources in order to develop practices and procedures which are relevant for your organisation.

UK Sport do not accept liability for any loss or damage arising from, connected with, or relating to the use or reliance on this guidance and templates by you or any other person. Organisations using this guidance remain wholly responsible for evaluating the completeness and effectiveness of their own practices and procedures.

This guidance has been issued by UK Sport, with thanks to Governance United for contributing to the content and thinking.
http://governanceunited.com


uk
sport
powering success
inspiring impact