



# Cyber Security Tool Kit

Level 2 • Identity  
& Access Management  
Securing your business.

0330 174 9996

[info@start-digital.co.uk](mailto:info@start-digital.co.uk)

[start-digital.co.uk](https://start-digital.co.uk)





# What is this Document?

## What is this document?

This document is a cyber security audit; you will filter through and answer each question to improve your business's cyber security one easy step at a time.

We describe **what to do**, as well as **what not to do**. This is labelled as **Good Practice** and **Bad Practice**. You may find that some of your current practices or behaviours fall in to the **Bad Practice** category. This cyber security audit will be a key part of your cyber security journey, and show you what you are missing to secure and protect your business online.

## This document's core topics will help you know how to answer questions similar to:



*What can I do to keep my network secure?*

*How can I understand the big-picture of my network?*

*Do I have the right processes in place to make my network stay secure?*

*Do I have support systems in place in case of a cyber-attack?*

*Am I handling data correctly?*

*Am I keeping an eye on my network where possible?*



## Why these core topics are Important:

This document will cover the core topics listed above, as some of them can be easily overlooked by many people. From unskilled all the way up to people who are very skilled with technology. This document will help give you and understanding of your goals and aims regarding these topics. Using the topics covered in this document is a good baseline to help you plan your business's future cyber security plan of action.

## What you hope to achieve by completing this document:

The goal of this document is to get you started on your cyber security journey, no matter how small or big the first steps are, any step in the right direction is important.

**This is a document you may want to refer back to before and after you've implemented your business's new cyber security policies and procedures.**





# Performing an Audit

## How to Use this Document:

This document is laid out in a very simple user-friendly way, with four core columns to focus on. The four columns are set out for you to follow from left to right in the following way:

1: Do You Have?	2: Yes/No	3: Good Practice	4: Bad Practice
<b>Example Question:</b> Do you have a secure password?		<b>Example Good Practice</b> A combination of the below: <ul style="list-style-type: none"><li>• Capital Letters</li><li>• Lower Case Letters</li><li>• Numbers</li><li>• Special Characters.</li><li>• Minimum 12 characters</li><li>• Long Phrases</li></ul>	<b>Example Bad Practice:</b> <ul style="list-style-type: none"><li>• Names</li><li>• Dates</li><li>• Numbers</li><li>• Predictable Sequences</li><li>• Short Single Words</li><li>• Short Phrases</li></ul>
This is a question to <b>assess</b> if you have a <b>specified cyber security</b> practice in place  Some of these questions may have a simplified version which may be easier to understand.	You will answer with a <b>Yes/No</b> in this box	This will be <b>our recommendation</b> of what you should do to solve your lack of cyber security labelled as a <b>Good Practice</b> .  A <b>Good Practice</b> is a behaviour that is <b>identified</b> as an <b>industry standard way</b> of doing particular things.	This is a section where we go over common <b>Bad Practices</b> . If any of your <b>current</b> behaviours are listed in the <b>Bad Practice example</b> , then you should put a <b>no</b> in the <b>Yes/No</b> box and look at the <b>Good Practise</b> for an idea of what you should be doing instead.

## How to Use the Total Score Table:

At the end of every module, there is a **Total Score** table. This table is where you **total up** all your **yes/no** answers **for each module** you complete:

<b>Total Score:</b>	<b>Y:</b> <b>N:</b>	<b>Notes:</b>
This is the <b>total number</b> of <b>yes/no</b> answers in the boxes to the <b>right</b> .	This is where you will put the <b>amount</b> <b>yes</b> and <b>no</b> answers you have <b>totalled</b> up per section.	You can use this box for any <b>additional notes</b> you want to make for each unit you have covered.



# Identity & Access Management

## Identity and access management:

Administrator rights are a very important subject, ensuring administrator rights are set up, and administrator accounts are used correctly. Admin accounts should not be used on a regular basis for everyday tasks. It's an important step in keeping most networks/systems safe from harm. If you use your administrator account for daily tasks, it creates a higher risk of a vulnerability being exploited and causing major damage that could have been avoided.

Follow the questions below while keeping in mind your business and its needs.

**Administrator Rights:** Tick off once complete.



Create a second account for administrators of the network/device for normal use.

Implement multi-factor authentication on administrative accounts.

Check other user accounts regularly to reduce their permission for what they need.

## Module Notes:

You can use this box to add any notes you feel are necessary to help you work through this module.

Notes: