The Cyber Collective Eight-Week Uplift Workbook

Thank you for becoming a member of The Cyber Collective! We appreciate your support, and we look forward to stepping you through the Cyber Uplift Process.

This workbook is for new members about to embark on an eight-week uplift journey, in preparation for annual reviews and audits.

There is a lot to get through in this process, and some time will need to be set aside to finalise items.

We will endeavour to make this process as straightforward. However, it is likely during the process that you will have questions and we welcome the opportunity answer them along the way.

Let's get started!

Fraser Jack & Damien Cunningham

Fraser Jack and Damien Cunningham

Founders – The Cyber Collective

Process Overview

Cyber security in any organisation comprises three equally essential pillars that must work together.

1. Compliance
2. People, and
3. Technology

Using a structured approach and following a regulatory backed cyber security framework such as:

- ASIC Guidance
- NIST (National Institute of Standards and Technology)
- ACSC (Australian Cyber Security Centre)
- Essential Eight Cyber Security Strategies

Across the three pillars of People, Tech, and Compliance, the planning is structured across six topics relating to, before, during, and after any incident. (Governance, Identify, Protect, Detect, Respond and Recover)

Governance - Leadership and Accountability

Track the Truth (Compliance)	Train the Team (People)	Tick off the Tech (Technology)
✓ Plans (ISM and CIRP) ✓ Risk Assessments ✓ Policies ✓ Auditing and Reporting ✓ Structured Approach – Starting with Regulatory Guidance	✓ Directors taking responsibility and accountability ✓ Appointment of cyber champion or cyber leadership team ✓ Processes and Behaviours ✓ Demonstration of understanding ✓ Team engagement ✓ Commitment to helping clients	✓ Directors and management commitment to providing required recourses ✓ Directors' cyber literacy upskilling

Identify – Risk Assessment

Track the Truth (Compliance)	Train the Team (People)	Tick off the Tech (Technology)
✓ Cyber Plan (ISM) Risk Assessment ✓ Third-party Supply Chain Risk Assessment	✓ Test the Team (Gap Analysis) ✓ Train the Team (Cyber Awareness Training)	✓ Check the Tech (IT Checklist)

Protect – Implement

Track the Truth (Compliance)	Train the Team (People)	Tick off the Tech (Technology)
✓ Implement Cyber Plan ✓ Cyber Liability Insurance ✓ Audit and Report	✓ Train the Team (Cyber Awareness Training) ✓ Test the Team (Vulnerability and Phishing)	✓ Tune the Tech (IT Checklist)

Detect

Track the Truth (Compliance)	Train the Team (People)	Tick off the Tech (Technology)
✓ Cyber Incident Response Plan (CIRP)	✓ Team Detection ✓ Train the Team (Cyber Awareness Training)	✓ Tech Detection Systems

Respond, React and Report

Track the Truth (Compliance)	Train the Team (People)	Tick off the Tech (Technology)
✓ Follow your CIRP ✓ Insurance	✓ Legal ✓ Public Relations and Corporate Communications ✓ Regulatory Reporting ✓ Team Training (Cyber Drill)	✓ Tech Teams

Recover – Repair, Review and Report

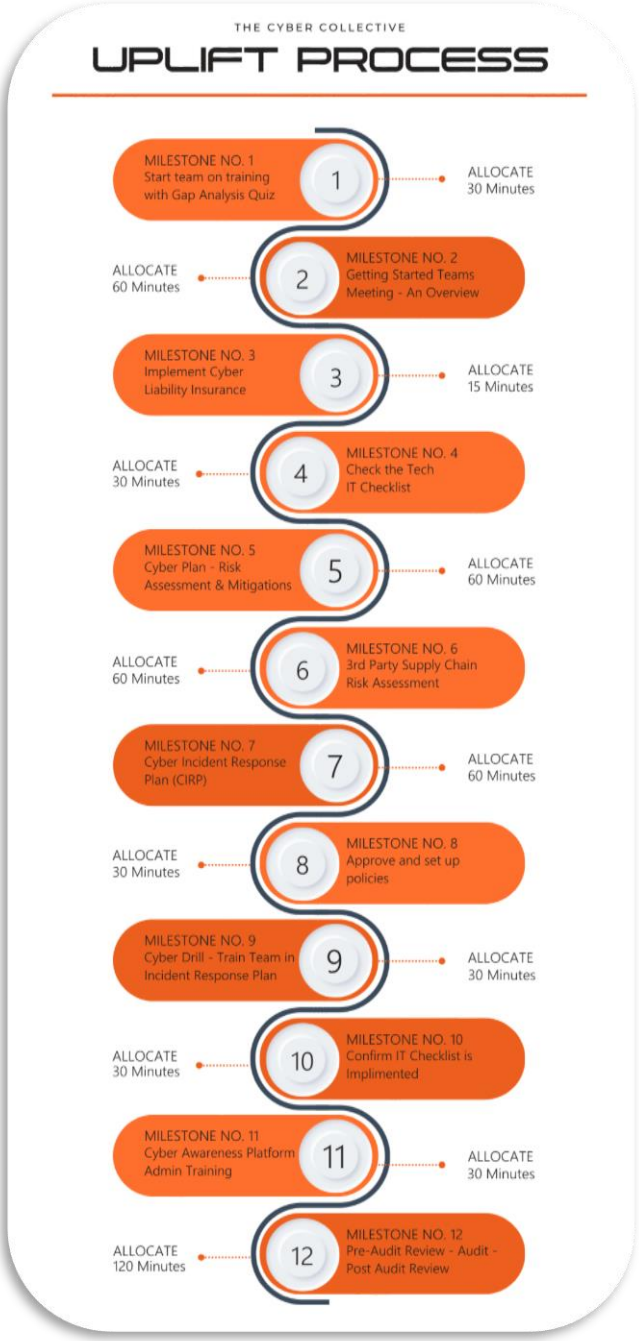
Track the Truth (Compliance)	Train the Team (People)	Tick off the Tech (Technology)
✓ Follow CIRP ✓ Review Everything ✓ Regulatory Reporting	✓ Make Good ✓ Support Clients	✓ Restore

Cyber Uplift Process (Inc Audit)

In practical terms, we have eight weeks to get through a bunch of things, detailed below.

We have set them out in this order for good reason, so please do your best to follow the process, and tick off the items as you go along.

The Infographic below is the short version, to get your head around the different steps in the process, it includes generous time allocations, and as you can see, we are already part way through the process.



Week One:

After becoming a member of The Cyber Collective, we requested two things, a list of your team members (names and email address') and to book in our first meeting to get started.

❑ Step One - Time Allocation [30 min]

Setting you your team on the Cyber Awareness Platform to begin training, testing, and reporting.

We do this early in the process, so when we get to the audit in week eight, we have a history of training and testing to report on.

Your team members will start with our Gap Analysis Quiz – 12-20 min 36 question quiz to assess current cyber literacy so we can set up individual learning plan for each team member.

Can you please:

1. Ensure we have an accurate list of all team members including first, last names and email addresses
2. Inform your team the quiz will be emailed to them
3. Ask your team to prioritise the time and get the quiz completed ASAP
4. Ask your team to engage with and prioritise the time to complete the fortnightly "habit building" awareness training

❑ Step Two - Time Allocation [2 min]

Confirm you have booked the first meeting.

We call this the "Getting started with The Cyber Collective" 60 min meeting

Weeks One - Two:

❑ Step Three - Time Allocation [60 min]

Attend the "Getting Started with The Cyber Collective" 60 min Teams meeting

Agenda:

1. Book Audit
2. Book Week Four Meeting
3. Discuss Tech Guru Relationship
4. Run through the workbook
5. Cyber Champion and Leadership
6. Director's demonstration of understanding
7. Commitment to the resources required
8. Engage with your Tech Professional (Guru) to inform/introduce them to us.
9. Cyber Liability Insurance – Check
10. Cyber Awareness Platform (CAP)
11. Next Steps – Email with attachments
    - IT Checklist
    - Cyber Plan

- 3rd Party Risk Assessment
- Cyber Incident Response Plan (CIRP)

❑ **Book Audit**

We book the 90 min audit around 8 weeks from now, and we are flexible on dates, and you will have an opportunity to change the date if needed. Although, if you follow this process, you will have plenty of time to get everything done well within the eight-week period.

❑ **Book Week Four Meeting**

Halfway through, we have a meeting to make sure everything is on track, and you are ready to start the second half of the process.

❑ **Discuss Tech Guru Relationship**

We are not here to replace your relationship with your IT Professional (Tech Guru). We are here to enhance the relationship you have with them. However, if you are not happy with your current Tech Guru relationship or services, we are happy to introduce you to some alternative providers should you need someone.

❑ **Cyber Champions and Leadership**

Appoint the appropriate people within the firm to be responsible and accountable for delivering the results.

❑ **Director's demonstration of understanding**

As with providing financial advice to retail clients, this requires a demonstration of understanding by the clients. The liability of any cyber process sits with the directors, we will do our best to explain complex cyber security items in layperson terms. However, if you do not understand anything you are implementing, please speak out.
The audit is there for two purposes, firstly that you have the compliance, training, and technology in place, and secondly that you understand what that means and why that is important.

❑ **Commitment to the resources required**

This process will include the commitment to providing resources needed. We do not know what this is just yet, but things like additional upfront and ongoing security software and monitoring may be needed. Or Cyber Liability Insurance may need to be funded.

❑ **Cyber Liability Insurance**

Do you have Cyber Liability Insurance already? Or,
Do you still need to get Cyber Liability Insurance set up?
If you still need to get this set up, we can help you immediately. We cannot make any recommendations on the insurer or the level of cover you have, as we are not a General Insurance Broker.
We do have a 10 minute YouTube Video on this here:
Here is a link to a Cyber Liability Insurer that will give you an instant quote

- Note: This link will apply a 50% reduction in the excess for any business where the team members are engaged in The Cyber Collective team training.

- You can also apply for the cover directly from this link, and have the policy issued immediately

Once you have a policy, you should print out or have a physical copy of the policy and schedule, in preparation for your cyber incident response plan. (CIRP)
If you have an incident you will need to locate a copy of your policy ASAP, and you may not be able to get into your computer at that time.

❑ **Cyber Awareness Platform (CAP) Admin Login**

Your training platform is set up, and you are set as the 'admin' on the platform. Here is the URL: https://app.user-training.com/
We suggest you save this to your favourites list in your browser for future reference.
Note there are two areas to this platform, your "Admin" login and your "team member" login, you will do your courses through a link from your email, however the admin login is where you will see your teams' activities.
We will run through some training on your CAP and show you around. At this point there will not be enough information in here to provide many insights, however, we will go through this again in the week four "Halfway Meeting" and can do so again during the Audit.
Chick here, to watch a 7 minute YouTube video demo of the platform.

❑ **Next Steps – Email with attachments**

We will send you an email with the following attachments to be completed in weeks two to four.

- IT Checklist
- Cyber Plan
- 3rd Party Risk Assessment
- Cyber Incident Response Plan (CIRP)

If you do not receive this email, please reach out to one of our team members at The Cyber Collective ASAP.

Weeks Two – Four:

❑ Step Four - Time Allocation [5 min]

Reserve time in your diary over the next few weeks and commit to completing the items required including:

- ❑ Two x 30 min blocks to discuss the IT Checklist with your IT Provider
- ❑ 60 min to complete the Cyber Plan template
- ❑ Two x 30 min blocks to complete the 3rd Party Risk Assessment
- ❑ 60 min to complete the Cyber Incident Response Plan (CIRP)

Note: you may require additional time.

❑ Step Five - Time Allocation [30-60 min] over 2-4 weeks

Information Technology (IT) Checklist Table

We provide you with our IT Checklist. It is a list of items we believe all professional firms should have as a minimum to protect their clients.

1. The first step in this process we call “Check the Tech” is to send this Checklist to your current IT Guru to fill out as a “Fact Find” exercise to understand what you currently have in place. There is a good chance that you will have most of the items in place already.
2. The second step in this process is when you get this list back, is to ask your IT Guru to quote you on implementing the items you currently do not have set up.
3. You can then request they do the work involved
4. Lastly, request they fill out the checklist again with the new information.

Please note, we are happy to speak to your IT Teams directly if they do not understand any of the items on the list, or why they are important.

As the leadership team or Cyber Champion of the business, you will need to familiarise yourself with the IT Checklist information and understand what the items are and why they are important.

❑ Step Six - Time Allocation [60 min]

Cyber Plan – Information Security Manual (ISM)

We provide you with a template plan to complete.

The purpose of the plan is to set out the security standards and frameworks, do a risk-assessment to i**dentify** the risks to your business/clients allowing you to then consider and **implement** the mitigation's you require to put in place to help avoid these risks to your business and clients.

- Appoint person with the responsibility to complete the template.
- Get the plan completed.
- Get the plan approved and signed off by the directors

❑ Step Seven - Time Allocation [60 min]

Third Party Supply Chain Risk Assessments

We provide you with a template plan to complete.

The purpose of this plan is, if you have not already done this, to demonstrate your due diligence in choosing to trust third party suppliers in relation to protection your client's personal information. Under the privacy act you are responsible for the safe upkeep of your clients Personal Identifiable Information (PII) and to just assume the providers you use are security focused is dangerous.

This process requires you to:

- Make a list of your third-party Supply chain
- Contact each one of your third-party supply chain and ask them to demonstrate their security standards and capabilities
- When they provide the information, use the template to do a risk assessment of the products
- Keep this document as part of your compliance, and asses any new products before you start using them

❑ Step Eight - Time Allocation [60 min]

Cyber Incident Response Plan (CIRP)
We provide you with a template plan to complete.

The purpose of the plan is to set out what you and your team will do in the event of an incident, the best time to make this plan is well before you have an incident, and whilst thinking with a logical mind.

This process requires you to:

- Go through the template and fill in the contact details of important stakeholders
- Complete the plan and get the directors to sign off on the plan
- Print out the plan or keep a physical copy, so you have it when needed, and you don't rely on your computer working to access the plan
- Train you team in where to find the plan and what to do. (This is also covered in the Cyber Drill section in weeks 4-8)

Week Four:

❑ Step Nine - Time Allocation [30 min]

Attend the "Halfway Through" 30 min Teams meeting

Agenda:

1. Check in - How are you going so far?
2. Set up Company Cyber Policy
3. Cyber Drill - CIRP
4. IT Checklist update
5. CAP Training and Team Engagement (stragglers)
6. Set up team member behaviour policies on the CAP
7. Discuss Time Commitments for finishing any tasks.

❑ Check In

Let's back it up and see how you are going so far; do you need help with anything?

❑ Company Cyber Policy

We will provide a template for your main company cyber security policy, that states your policy is to follow the new plans, processes, and mitigation strategies you have just implemented.

❑ Cyber Drill

Just as we have all done a fire drill, or first responders train in first aid, running a cyber drill allows your team to calmly walk through the process of **detecting** and **responding** to a cyber incident, whilst having the ability to react with a sound mind.

They should go through the Emergency Response Steps as well as being able to locate the physical copy of the Cyber Incident Response Plan (CIRP).

This training session, along with who attended should be noted in you CIRP and should be done at least yearly.

Team members should be able to demonstrate what they specifically should be doing and who they should be notifying.

- ❑ **IT Checklist update**

Where are you at with the IT Checklist items, do you have any questions or comments for us?

- ❑ **CAP Training and Team Engagement (stragglers) and team member behaviour policies**

Check in on your Cyber Awareness Platform Admin Portal. Check which team members are engaged and those who need some encouragement.

Check the phishing campaigns to see if your team have been compromised.

Set up the team members behaviours policy to send to your team for signing.

Weeks Four – Seven:

❑ Step Ten - Time Allocation [5 min]

Reserve time in your diary over the next few weeks and commit to completing the items required including:

- ❑ Any outstanding tasks not completed from the first half of the process
- ❑ Review and approve Cyber Business Policy [30 minutes]
- ❑ Perform Team Cyber Drill Training [30 minutes]
- ❑ Meeting with IT Guru to confirm the completion of the IT Checklist [30 minutes]
- ❑ Follow up any team members not engaging in the training [15 minutes]
- ❑ Follow up to team members signing your team behaviours policy [15 minutes]

Week Seven:

❑ Step Eleven - Time Allocation [5 min]

Online Pre-Audit Check in

We will send you a link to our Pre-Audit Quiz.
Complete the quiz to judge your readiness for the comprehensive cyber audit.

Week Eight:

❑ Step Eleven - Time Allocation [90 min]

90 min Teams meeting to go through the comprehensive cyber audit.
Covering the three pillars of people, technology, and compliance. The Audit is structured on the ASIC regulatory guidance, ACSC Essential Eight and NIST Framework.
Within a few days of the Audit, you will receive your audit report.

❑ Step Twelve - Time Allocation [5 min]

Book in next year's audit

- Book in Audit date in 12 months
- Book in Policy and Plans Review in 11 months