# Basic Assessment Appendix

Each module of this course had recommended assessment goals. The aim of these is to help each individual:

* Take notes on useful information they have learned throughout the course
* Benefit from from the unwritten peer learning that they gain during group work and conversations
* Have a starting point for increasing the security of the organisations that they are working with

The suggested basic assessement questions are examples and participants should feel free add/remove information on each module that they feel will be relevant. While filling out this assessment in a digital format is recommended, we suggest that any participants take security precautions to protect it’s sensitive information.

## [Mapping information, assessing the threat environment and modelling](mapping.md)

* Create an information map for your organisation
* Add generic and localised threat resources (where available) that you can use to be able to measure risk in your specific circumstances
* Develop an easily understandable information security traffic light map with corresponding mitigation measures for your organisation

## [Privacy regulation and requirements](privacy.md)

* Which legal and other best practice policies affect your organisation?
* What actions must your organisation take to be able to meet these requirements?

## [User Education](education.md)

* What new techniques and tools can you use to enhance user education within your organisation?
* What techniques and tools and can you use to measure implementation of user education within your organisation?

## [Encryption, Patching, Licensing](encryption.md)

* What is the current status of encryption, patching and licensing across your organisation?
* How can encryption, patching and licensing be better managed across your organisation?
* If you don’t already have one, can you benefit from a relationship with an organisation that provides discounts for non-profits such as TechSoup
* What would be the rough costs or resources needed to implement new software or services for security management into your organisation?

## [Network Management, Monitoring and Logs](network.md)

* Draw a map of your current infrastructure and architecture
* What tools and techniques could be used for better monitoring of security risks and logs within your organisation?
* What steps would you need to take to implement better security monitoring within your organisation?

## [Communications](communications.md)

* Develop a communications plan for your organisation based on the scenarios they face - day to day, internal, first contact, working with partners etc.

## [Web and Email Management](webandemail.md)

* Add any necessary changes to security and privacy features your their organisations email service
* Add any necessary changes to your organisation’s web hosting service (e.g. Wordpress) that you need to increase security.
* Add DDoS protection service (if needed)

## [Password Management](passwords.md)

* Add your organisation’s recommended tool for password management - including resources useful for teaching. Even if the tool is individual (e.g. KeepassXC) vs. centrally managed
* Identify any services your organisation uses that allow for two factor authentication but are not already enabled
* What steps might be necessary within your organisation for implementing better management of passwords?

## [Mobile Device Management / BYOD](byod.md)

* What would a policy for MDM/BYOD for your organisation neeed to contain?
* If you don’t already have one, what MDM/BYOD tools might work best for your organisation?

## [Travel](travel.md)

* During what times or in what locations are people within your organisation most at risk during travel?
* What basic travel security advice are you most likely going to have to give to people within your organisation?
* If you don’t already have one, list the main features you will need in a travel security policy.

## [Resilience and Backups](resilience.md)

* If you don’t already use one, which backup solution might be best for your organisation?
* Write a short business continuity process and plan

## [Policy Creation and Implementation](policy.md)

* What policies are my organisation missing?
* What templates can I use to build policies?
* List the main likely obstacles to implementation within their organization and their corresponding potential solutions

## [Physical Security](physical.md)

* What physical controls might I need to add to my own home/office environment?

## [Responding to Incidents](incidents.md)

* What types of incidents do I expect that my organisation may face?
* Who else needs to be involved in responding to an incident? (e.g hosting provider, social media manager, partner organisations)
* What is my incident response plan for major information security risks?

## [Basic audits](audits.md)

* What tools and resources can I use for basic auditing within my organisation?
* What regular checks and basic audit will I do on a regular cycle?
* What steps to I need to take to ensure I regularly conduct a basic audit?
* How can I ensure that issues identified in the basic audit are addressed?

## [Community structures and resources for further learning](community.md)

* What new community structures can I use?
* When and and how can I connect to them?
* What can they provide?
* What can I provide back to the community?

## Top 10 Things I am going to do this week

## Top 10 Things I am going to do this month

## Top 10 Things I am going to do this year

## Notes