DR. JOSEPH MAGUIRE

ENTERPRISE CYBER SECURITY

University of Glasgow

OVERVIEW

- overview of enterprise cyber security and what sort of topics will be explored in the course.
- aim of the course and intended learning outcomes of the course.
- consider the demographic of the audience and motivation for taking the course.
- assessment approach covered as well as general housekeeping.

COURSE COORDINATOR

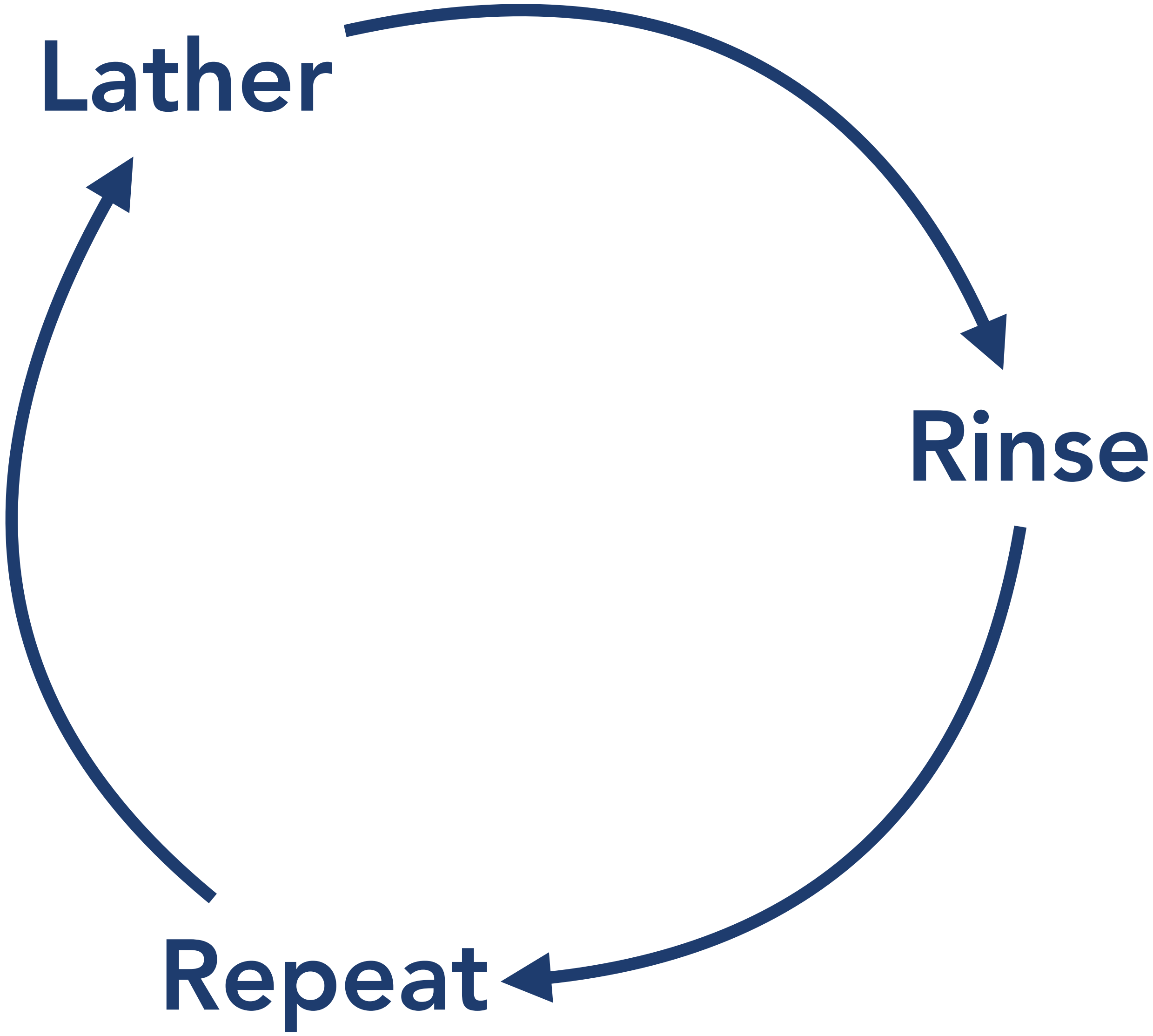
- Dr. Joseph Maguire
- Email address: **joseph.maguire@glasgow.ac.uk**
- Office 410, Sir Alwyn Williams Building
- Office hours appointment can be booked through course Moodle.

ENTERPRISE CYBER SECURITY

"Security is a **process**, not a product"

– BRUCE SCHNEIER

SHAMPOO ALGORITHM



Lather

Rinse

Repeat

SECURITY AS PROCESS

- gather data and perform an analysis to better understand the problems.
- develop solutions to address these problems and apply them.
- determine what success looks like and continually improve.
- avoid continually lathering and rinsing, but never getting clean.

TENANTS OF CYBER SECURITY

- prevent, detect, respond - consider emergency services as an example.
- people, process, technology - security is the responsibility of everyone not just professionals.
- confidentiality, integrity and availability - information security important to enterprises.

PRE-HISTORY

- understand the evolution of enterprise architecture from monoliths to distributed systems.
- explore some of the significant cyber security incidents that have shaped responses in enterprises.
- understand that cyber security is not a new challenge but one that is often neglected.

SYSTEM THINKING

- consider complex, distributed enterprise systems holistically.
- determine the elements, interconnections and purpose of systems within enterprises.
- identify patterns of feedback and the unforeseen consequences of countermeasures.
- consider not only the enterprise systems but the systems attacking them.

CYBER RISK ASSESSMENT

- understand the context of systems and how they interact with cyber space and their attack surface.
- identify the malicious and non-malicious risks to systems connected to cyber space.
- analyse and understand the likelihood of a threat and its consequences to the enterprise.
- evaluate the risk from the compound of several threats and determine the form of treatment.

POLICY

- policy attempts to mitigate the problems that emerge between offering more and more functionality and need to remain secure.

- policy can refer to many things from information security, business objectives to laws and compliance.

- policies are not procedures, they do not prescribe specific implementation details.

- policies present security goals, rather than specifications.

METRICS

- cyber risk management processes are typically strong in terms of **identification** and **treatment**.
- alternative perspective is that cyber risk management should be strong in **quantification** and **value**.
- **assets** should be considered as well as the risk, that is the denominator as well as the numerator.
- the concern is that we are following the shampoo algorithm - an endless loop without ever getting clean.

BUSINESS CONTINUITY AND PLANNING

- perform business impact analysis to identify window of recovery, resources that need to be recovered and mission critical activities.
- clear benchmark of the quantitive and qualitative losses that act as justification for contingency plans.
- understand the dependencies between business processes and infrastructures.
- the aspiration is to return to business as usual as quickly as possible after an incident.

COURSE SPECIFICATION

INTENDED LEARNING OUTCOMES (1)

- describe different deployment concerns for a specific context.
- design security policy to address perceived concerns for a specific context.
- argue appropriate approaches to business continuity and resilience.

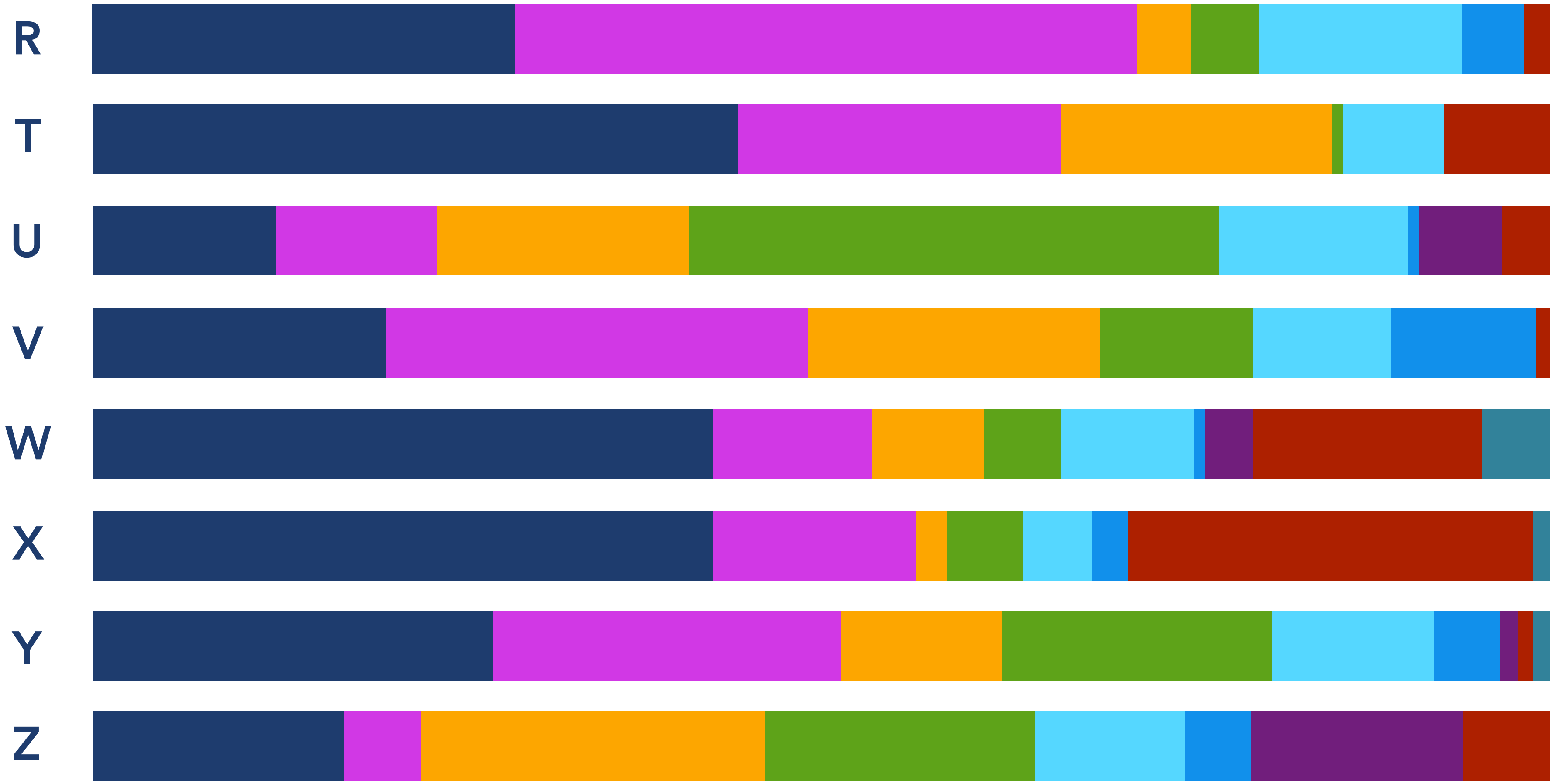
INTENDED LEARNING OUTCOMES (2)

- predict legal, social and ethical concerns in the security management of information.
- effectively communicate cyber security imperatives to decision makers in an organisation.
- identify and critically assess threats in a specific context
- critique security policy and justification for a given context.

NON-TECHNICAL

- enterprise cyber security is a non-technical course, there is **no programming** assignment.
- the focus is not technical brilliance, but understanding how to manage cyber security within an enterprise.
- the non-technical focus is valuable for technical and non-technical students alike.

TASKS BY TIME FOR PROFESSIONAL DEVELOPERS



EIGHT JUNIOR SOFTWARE DEVELOPERS

COHORT DEMOGRAPHIC

- individuals that have **knowledge and experience in other disciplines**, but know little of computing science.
- individuals that have **industrial insight and experience of computing science**, but have little specialist knowledge or insight.
- individuals that have **solid computing science knowledge**, but lack specialist knowledge.
- most will have **little to no knowledge or experience of cyber security**.

MOTIVATION

- gain knowledge and insight into managing cyber security within an enterprise context.
- passion for computing science and the difficulties of delivering it within a challenging environment.
- cyber security challenges touch you every day in terms of security and privacy.
- generate future research and/or industrial products that have some security thinking to them.

RESEARCH LINKAGE

- research in the areas of enterprise and cyber security are considered within the course.
- students will typically be expected to read and consider a research paper each week.
- team exercise expects students to consider research and emergency thinking when developing policy.

LECTURE SLIDES

- slides will typically become available after each session, URL to slide repository through course Moodle.

- type **http://goo.gl/yZYGnQ** into web browser, username:**ecs** and password:**slides**

WHERE DOES THE SUBJECT FIT WITHIN THE SECURITY OPTIONS?

- consider authentication or passwords as a cyber security process.

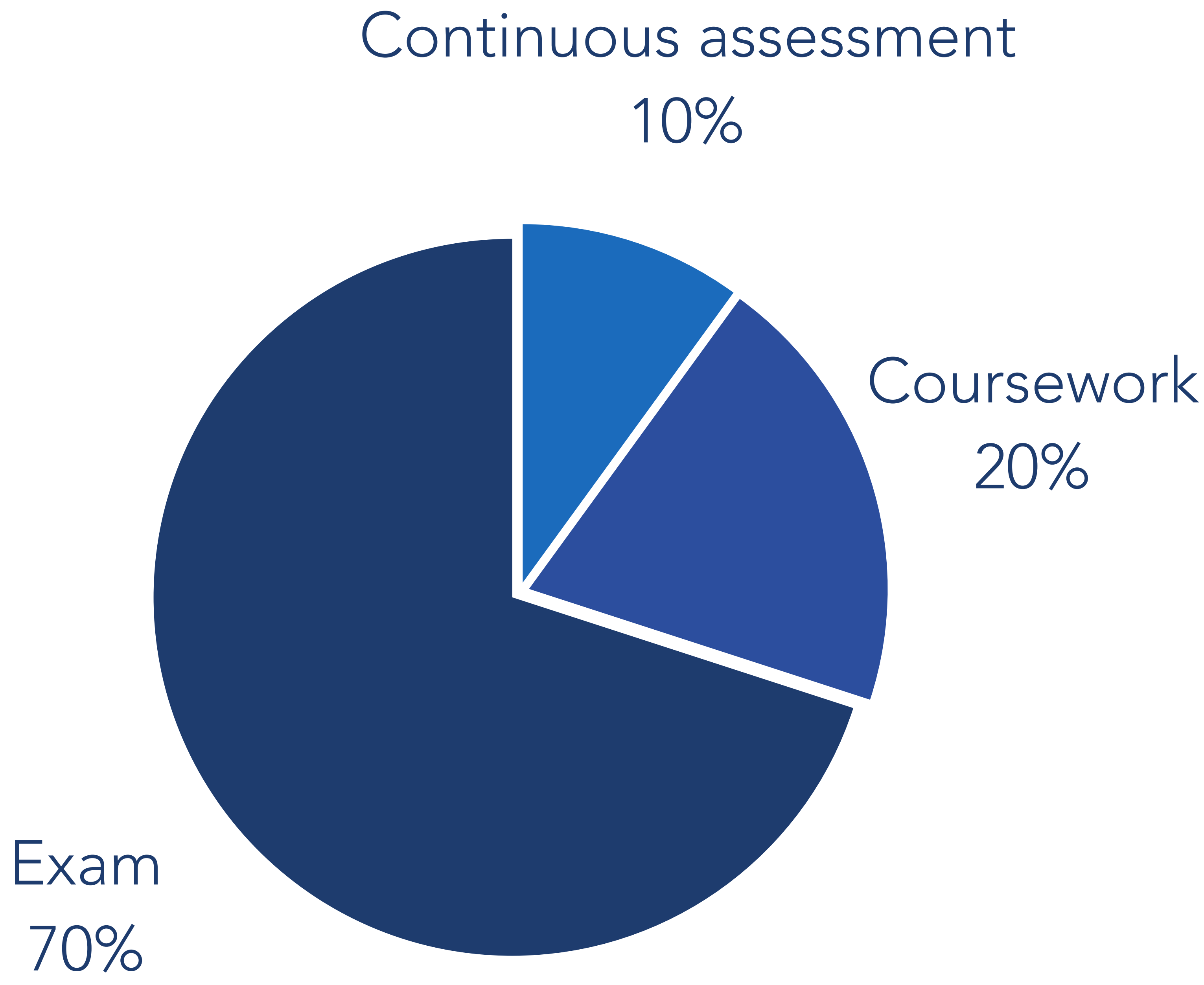
- enterprise cyber security is primarily concerned about how the process meets security objectives of an enterprise.

- cyber security fundamentals is primarily concerned with technical aspects of the process.

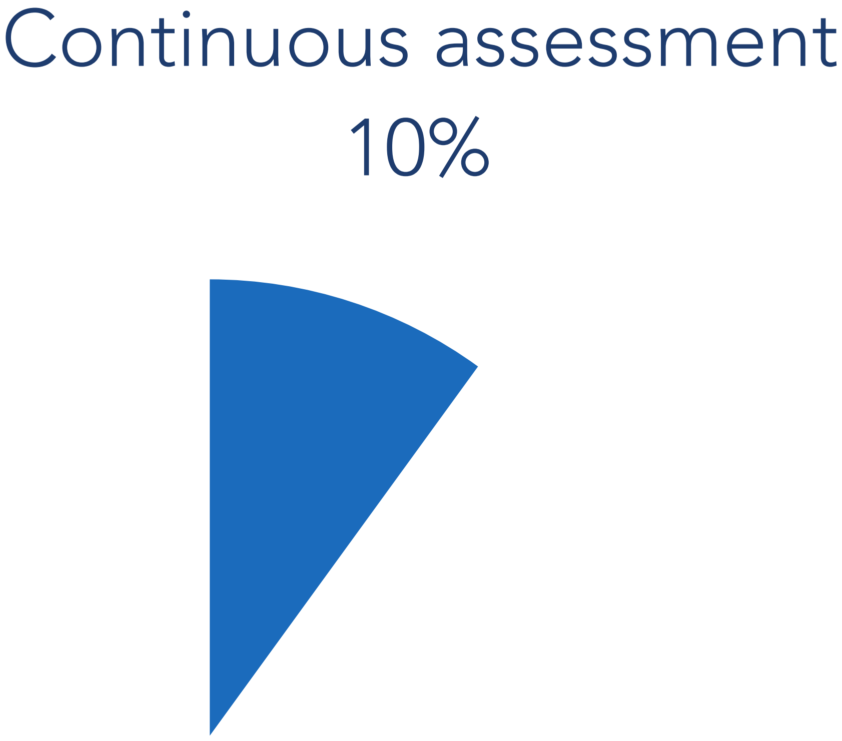
- human centred security is concerned with the human challenges of using the process.

ASSESSMENT

ASSESSMENT OVERVIEW



ASSESSMENT OVERVIEW



CONTINUOUS ASSESSMENT

- 10% of the individual final grade will be gained from continuous assessment.
- will typically take the form of a weekly quiz that probes research paper(s) reading.
- research paper(s) will be issued via Moodle and students are expected to prepare for a quiz the following week.
- research paper(s) may also prove a valuable resource for answering exam questions.

YACRS

- need to have a WiFi enabled device and connect to **eduroam**.
- individuals can also use their own data connection.
- instructions about how to connect your device to eduroam can be found online at **http://www.gla.ac.uk/services/it/eduroam/**
- graded quiz will be next week at the **2.00 pm lecture** on **Thursday** the **5th of October**.

YACRS

- classroom response system, developed at Glasgow, affording individuals the ability to respond to questions in lectures using their wifi enabled device.

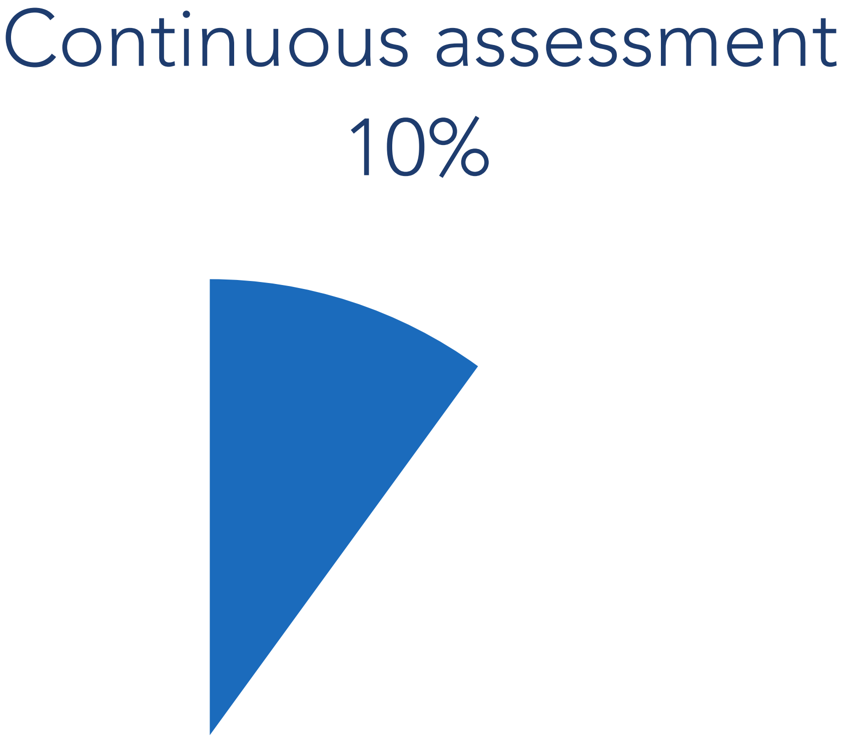
- individuals access platform via **http://classresponse.gla.ac.uk** and join a specific session.

- individuals are not allowed to access material or discuss questions during quizzes, unless otherwise stated.

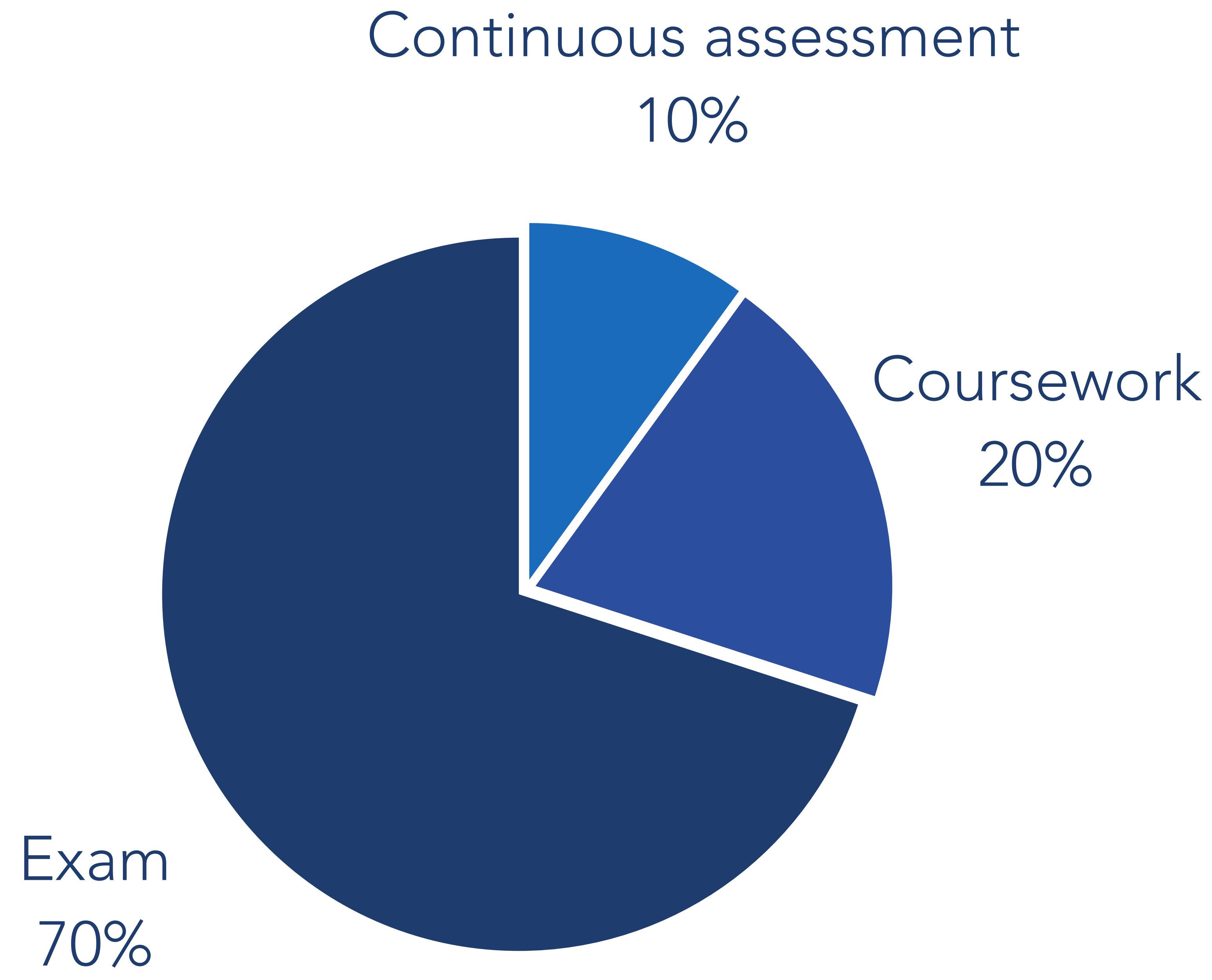
QUIZ RESULTS

- **individual performance** will also be published through YACRS website.
- not all quizzes contribute to your final grade, but it is still important to check and verify your responses.
- if you spot any errors in your responses, please contact to inform me.
- **answers** to quizzes will typically be published a few days after individual performance.

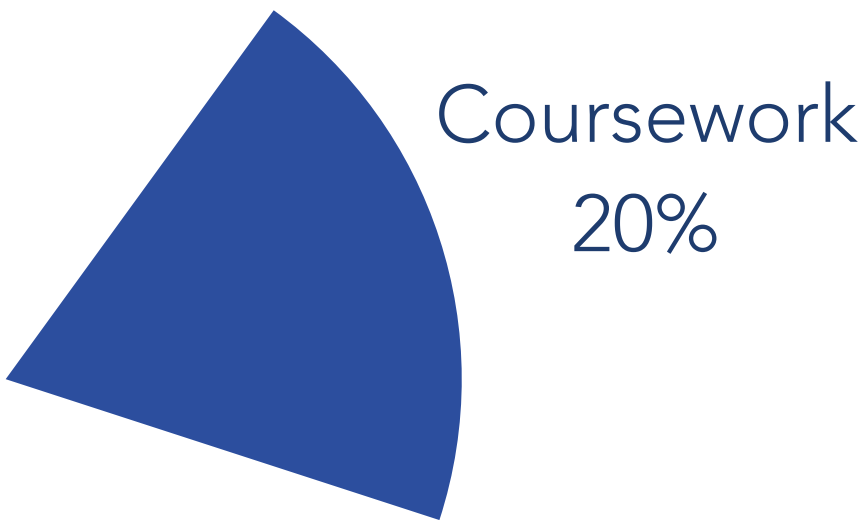
ASSESSMENT OVERVIEW



ASSESSMENT OVERVIEW



ASSESSMENT OVERVIEW



TEAM COURSEWORK

- design policy to address cyber security concerns of personal clouds, such as Dropbox and OneDrive, within an enterprise.
- coursework is non-technical and involves no programming.
- assessed specification will be released shortly, alongside team allocation.

TEAM COURSEWORK

- 20% gained through individual performance on a group coursework.

- team members are **allocated** and task can be completed by no more than five members and no less than four.

- teams submit workload report that is used to generate the **final individual grade** for coursework.

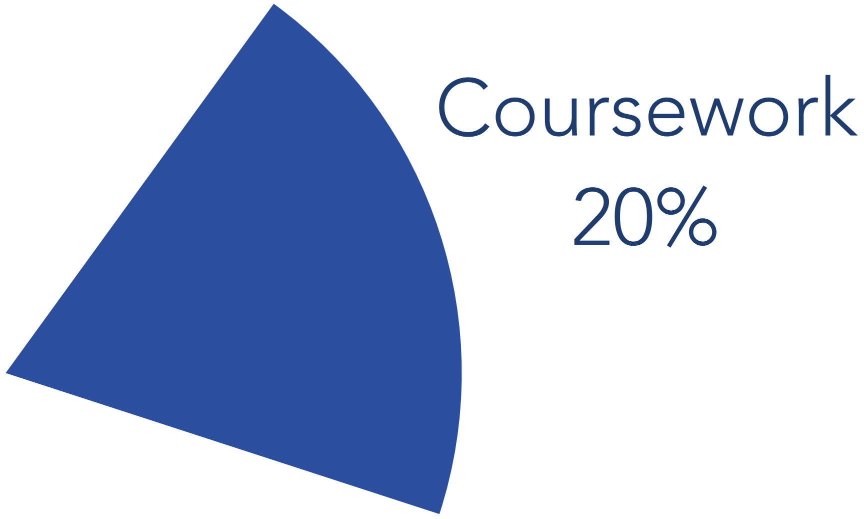
- every team member must submit by **4.30pm on Friday the 1st of December 2017.**

DELIVERABLES

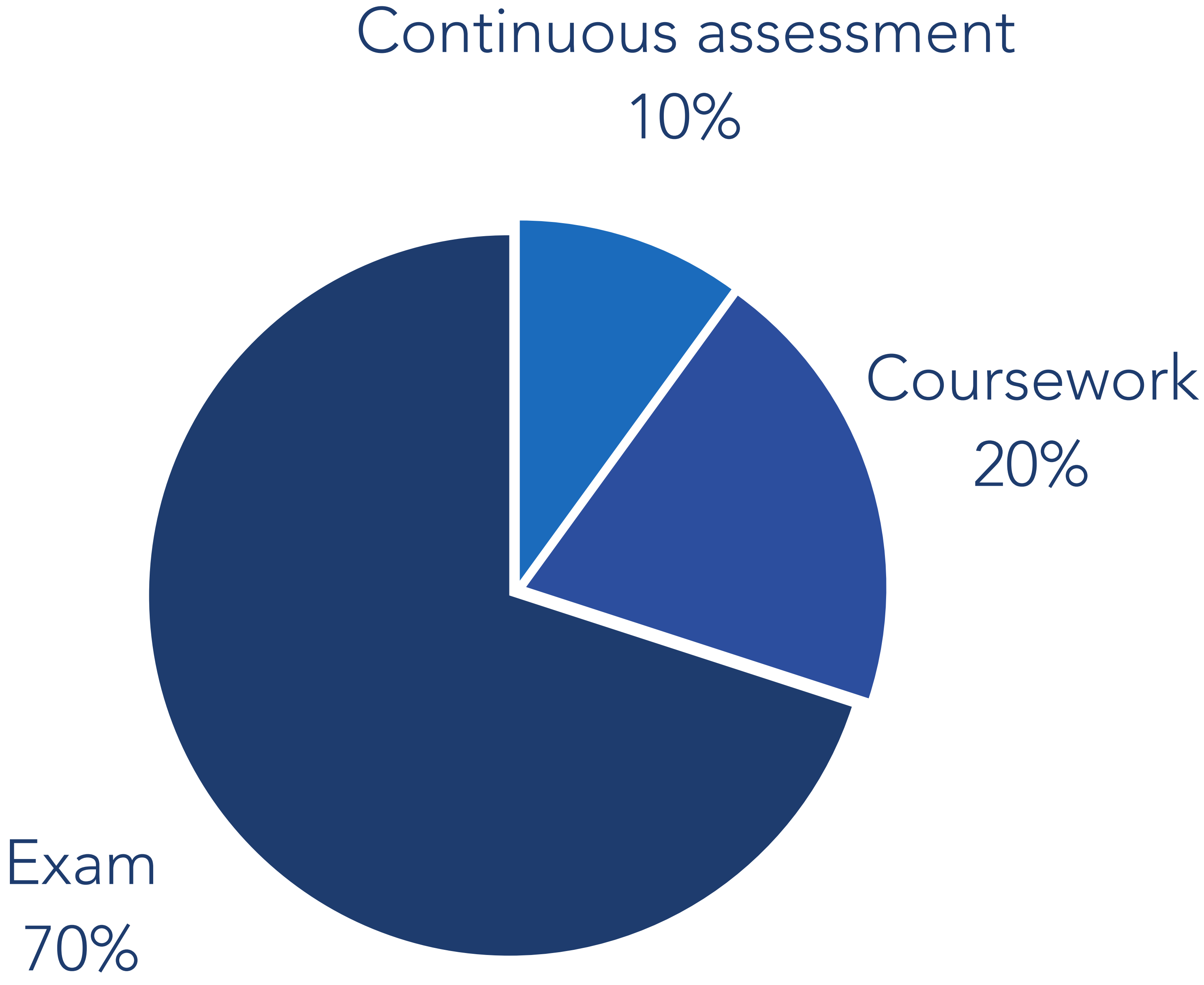
DELIVERABLES

- **draft written report**, forms the basis of peer-review, weighted at 0 or 1.
- **three reviews**, generated as a team, supports peers in improving work.
- **plans for action** in response to the three reviews you receive from other teams.
- **final written report**, generated as a team, should reflect improvement from peer-review.

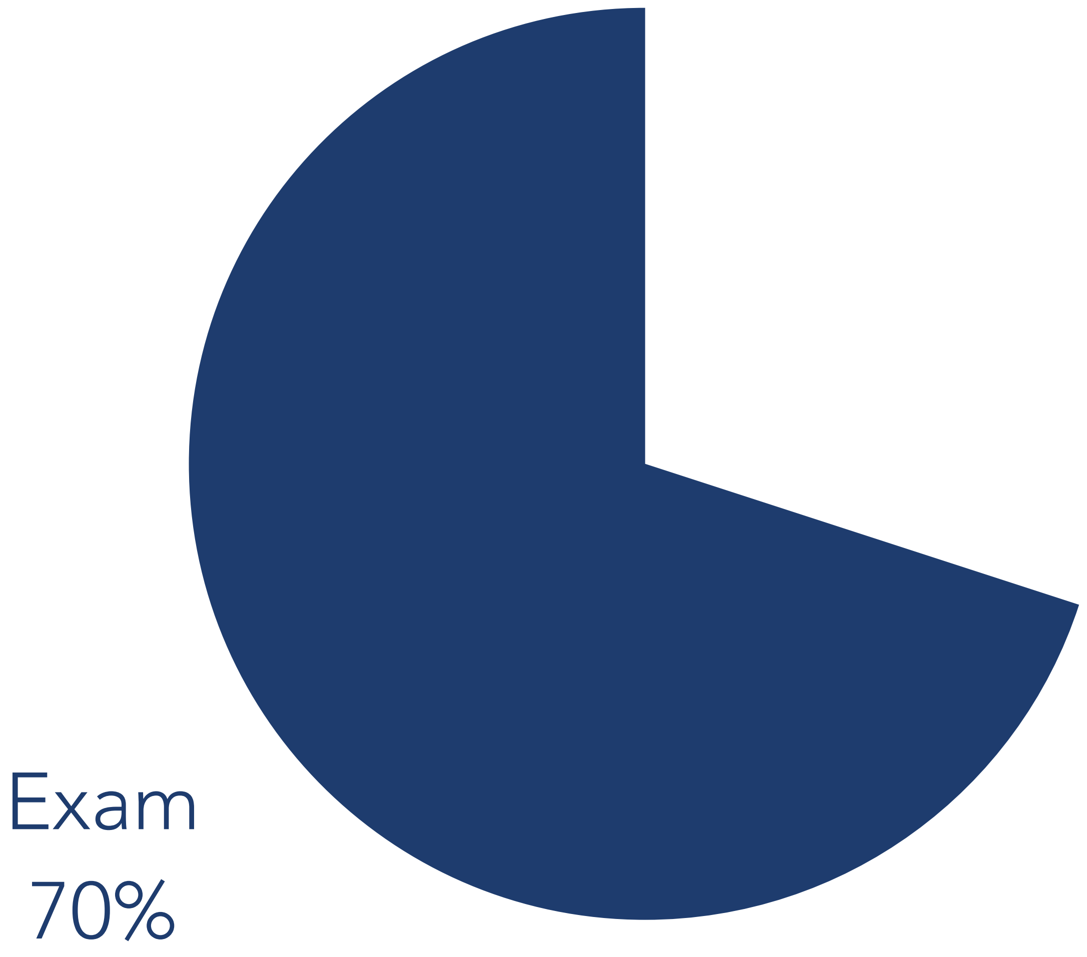
ASSESSMENT OVERVIEW



ASSESSMENT OVERVIEW



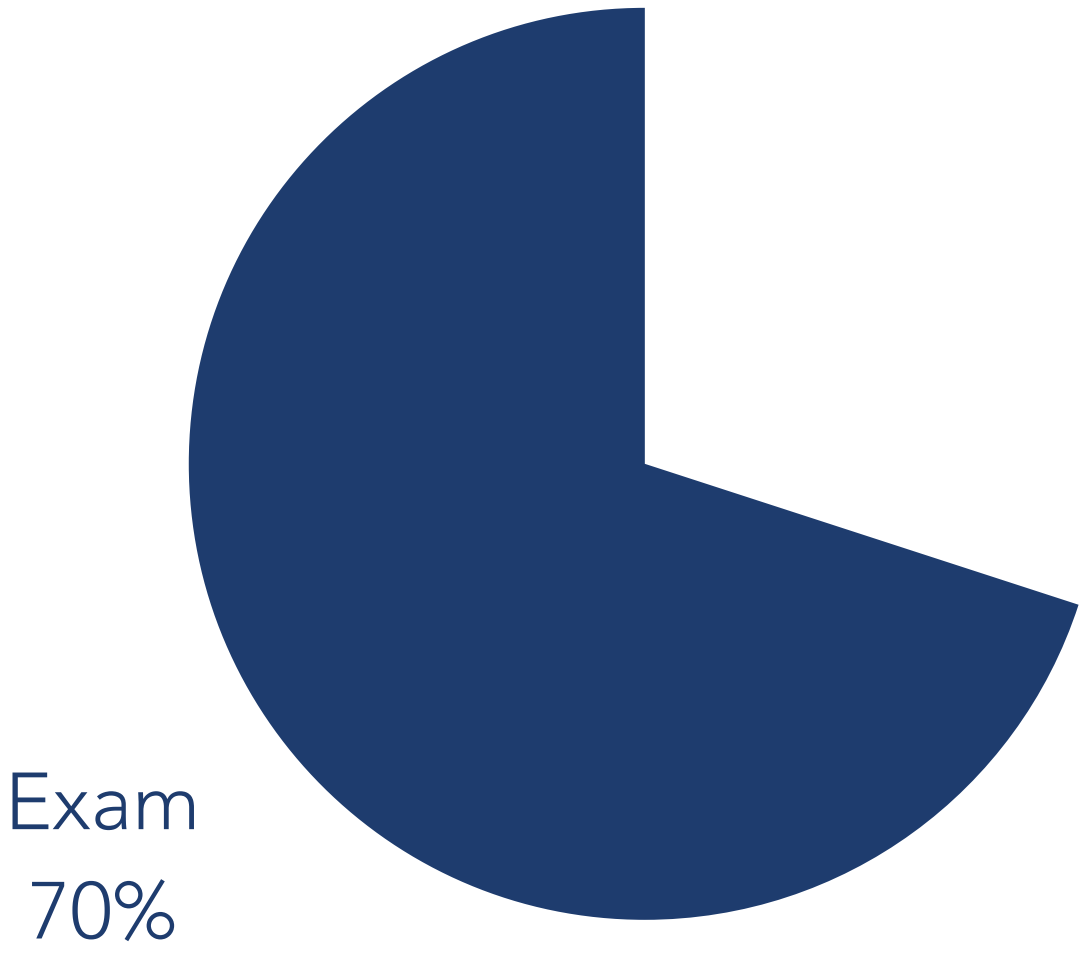
ASSESSMENT OVERVIEW



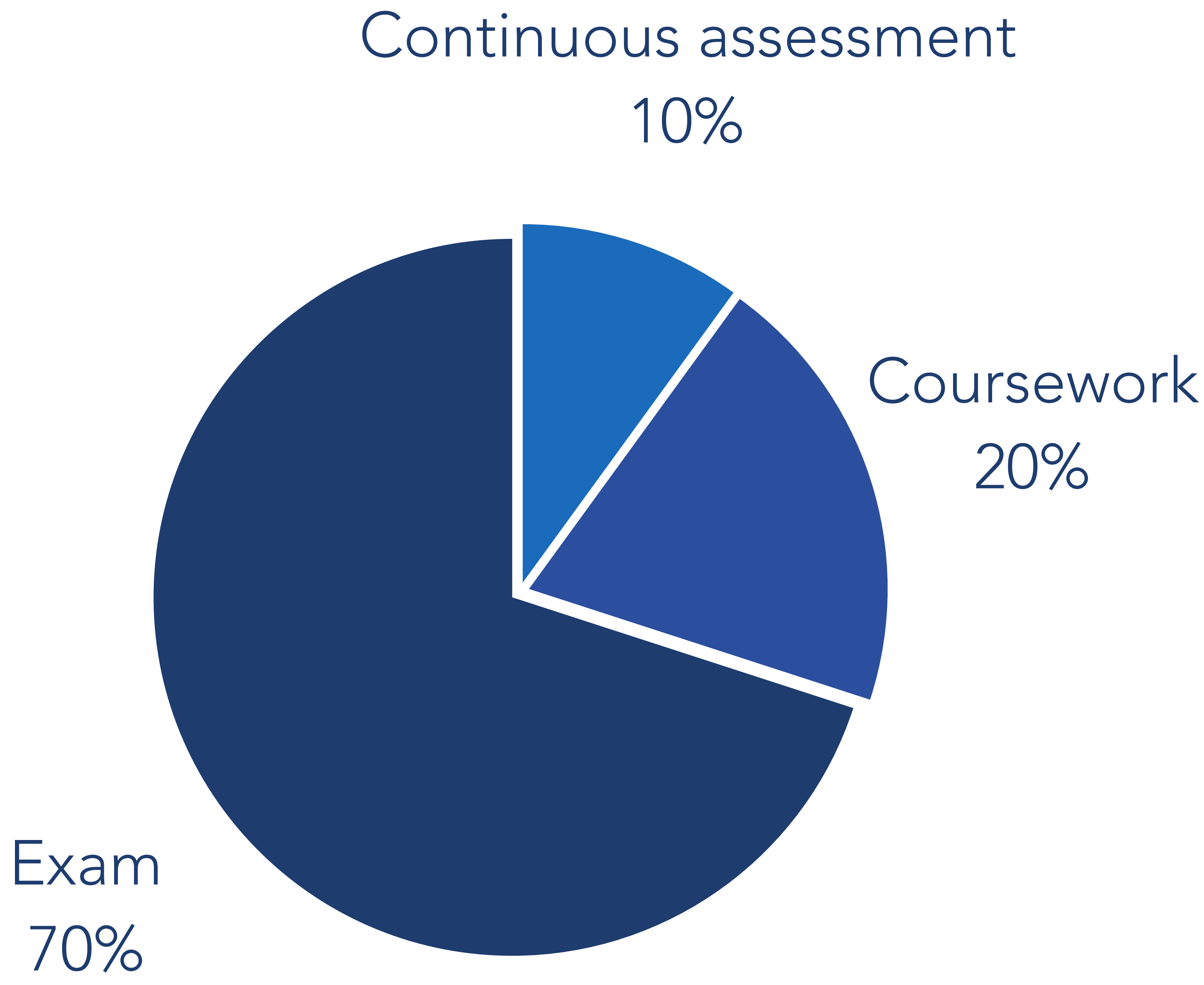
EXAM

- 70% of grade will be gained from individual performance on summer exam.
- individuals most attempt at least 80% of course to obtain final grade.
- sample paper provided for the exam near the end of the course.
- revision session typically offered nearer the exam.

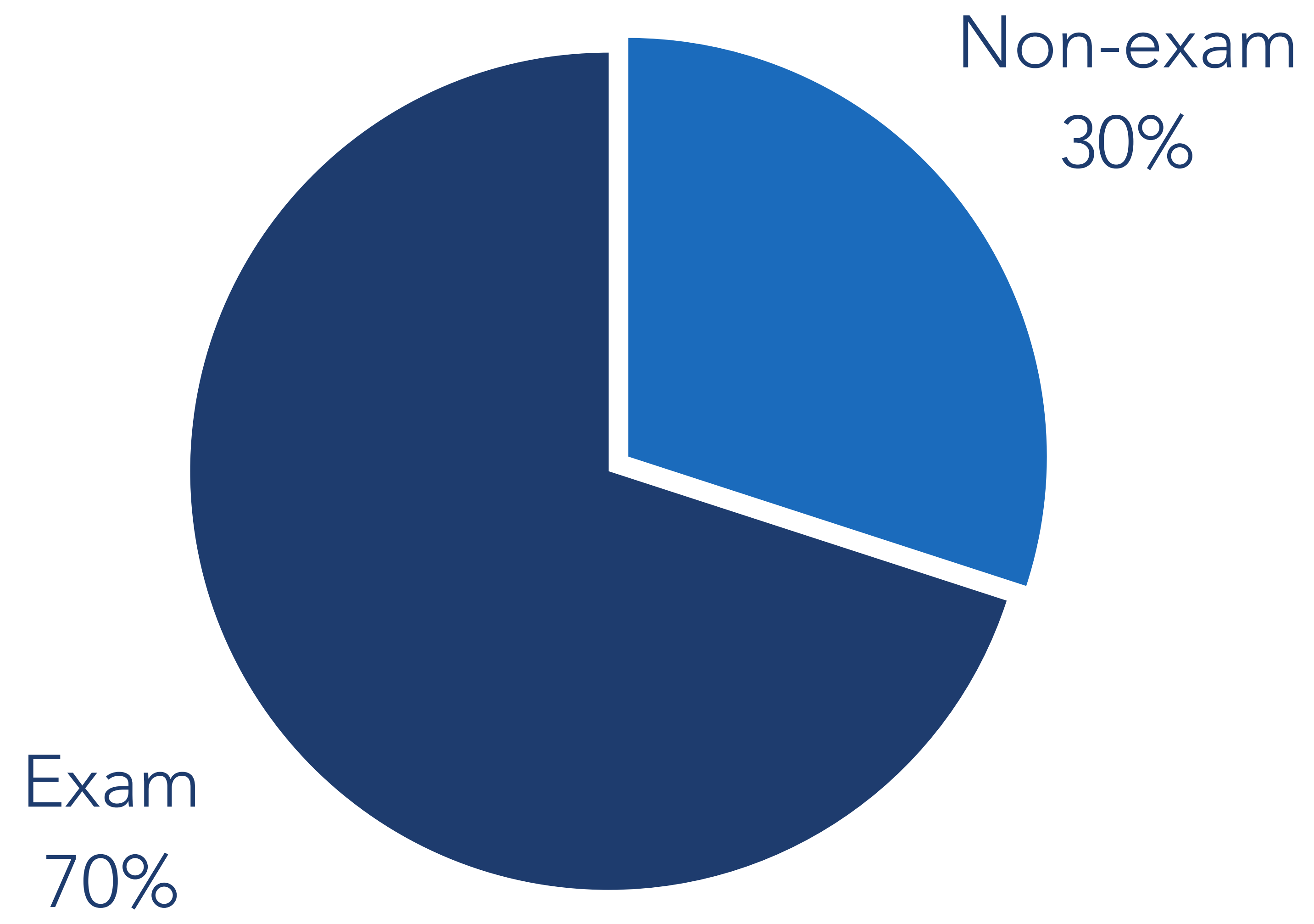
ASSESSMENT OVERVIEW



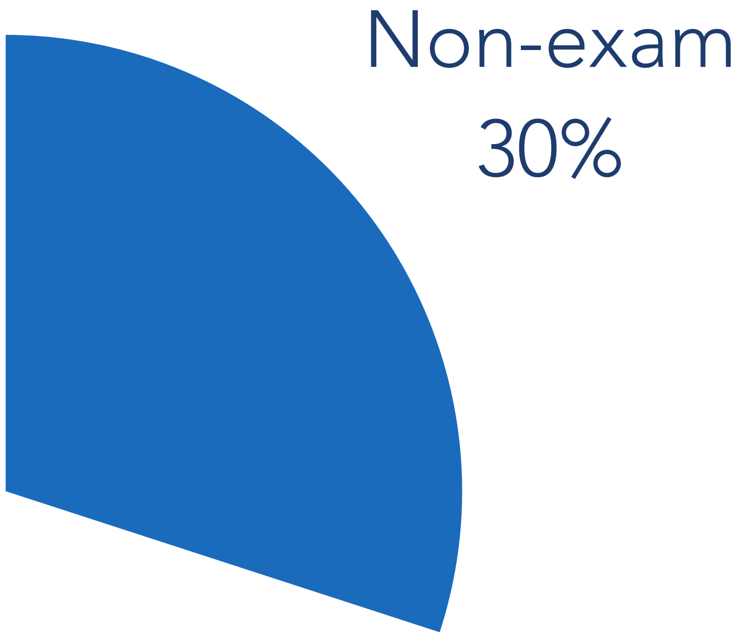
ASSESSMENT OVERVIEW



ASSESSMENT OVERVIEW



MINIMUM REQUIREMENT FOR THE AWARD OF COURSE CREDIT



SUMMARY

- define enterprise cyber security and what sort of topics will be explored in the course.
- outline the aim of the course and intended learning outcomes of the course.
- consider the demographic of the audience and motivation for taking the course.
- cover the assessment approach as well as general housekeeping.

DR. JOSEPH MAGUIRE

ENTERPRISE CYBER SECURITY

University of Glasgow