aphore

30-WEEK CYBERSECURITY TRAINING PROGRAM

1300 041 042
www.aphore.com
Level 2, 1 Southbank Boulevard,
Melbourne, Victoria 3006

TABLE OF CONTENTS

About Us.

Introduction

Aphore represents the union of SiD (Aus), Tech in Depth, Aphore Security and Aphore Technology—a strategic convergence driven by our shared vision: to deliver exceptional managed IT, incident response and cyber security solutions tailored to local needs, with the scale and capability to meet global demands. This integration is more than a merger; it is a commitment to empowering organisations worldwide with trusted, innovative, and comprehensive solutions that ensure resilience, security, and growth. Whilst Aphore is a new brand, the team and business have been established since 2011 and is one of the most trusted, experienced teams working in today's technology world.

We operate across three high-level areas—**Cybersecurity, Managed Services, and Training**—offering world-class technological solutions designed to protect, empower, and inspire businesses. We understand that, in today's complex and interconnected world, companies need more than just reactive services; they need a trusted partner who will be with them every step of the way. That's who we are—***guardians of progress, enablers of growth.***

Mission & Vision.

MISSION

Empowering Confidence Through Cybersecurity and Technology

At Aphore, our mission goes beyond providing services; it's about empowering businesses to operate with unwavering confidence. We believe that security and innovation should go hand in hand, enabling organisations to thrive without fear. Whether safeguarding against cyber threats, managing complex IT environments, or delivering cutting-edge training, our focus remains the same: building trust, driving growth, and enabling progress.

VISION

Setting the Global Standard in Technology and Security

We aspire to set the benchmark for excellence in cybersecurity, managed services, and training. Aphore envisions a world where businesses of all sizes can harness the power of technology without compromise—secure, efficient, and future-ready. Our vision drives us to innovate relentlessly, ensuring we remain at the forefront of an ever-evolving digital landscape.

Program Structure Overview

This structured cybersecurity training program provides a balanced mix of theoretical knowledge, hands-on practice, and real-world industry exposure. Designed to prepare students for key certifications and practical roles in cybersecurity and risk management, the program follows a step-by-step approach:

MONDAY NIGHT SESSIONS (3.5 HOURS/WEEK)

Core training lectures covering ISO 27001 Lead Auditor, ISO 27035 Lead Incident Manager, the CARR (Cyber Assurance Risk Review) methodology, and MCP (Microsoft Certified Professional) topics. These sessions build foundational knowledge and prepare students for relevant certifications (ISO 27001 Lead Auditor, ISO 27035 Incident Manager, CARR program certification, and a Microsoft certification).

SECOND STUDY DAY (3.5 HOURS/WEEK PER GROUP)

Hands-on practice and real-world application. Students work on implementing an ISO 27001 ISMS in a case study organization, conduct mock CARR assessments, perform IT security tasks, and review case studies. This practical day reinforces Monday's theory with concrete exercises and group projects.

WEEKLY MENTOR MEETINGS

A separate weekly session with an assigned mentor for guidance, Q&A, and feedback. Mentors review project deliverables, ensure students meet learning objectives, and provide career advice. These check-ins solidify understanding and keep students on track.

CARR PROGRAM INTERNSHIP (WEEKS 29–30, PART-TIME)

In the final two weeks, students intern with partner companies to perform real-world CARR cybersecurity reviews. Under supervision, they apply the full spectrum of learned skills in a live environment – interviewing stakeholders, evaluating security controls, and delivering a risk rating report – gaining invaluable industry experience

WEEK 1-10:
ISO 27001 LEAD AUDITOR TRAINING & ISMS IMPLEMENTATION

OVERVIEW

In the first 10 weeks, students will become proficient in ISO/IEC 27001 (Information Security Management System standard) and auditing techniques. Monday sessions follow the ISO 27001 Lead Auditor curriculum – from ISMS fundamentals to audit planning, execution, and reporting.

The second study day each week is used to implement a mock ISMS for a case study organization, giving practical insight into how ISO 27001 is applied. By the end of Week 10, students will be prepared to take the ISO 27001 Lead Auditor certification exam and will have hands-on experience equivalent to conducting an internal audit

Week 1

Introduction to ISO 27001 and ISMS Basics

MONDAY SESSION

Overview of Information Security & ISO 27001

- Explain what an ISMS is and why it's important.
- Discuss the ISO 27001 standard structure (clauses 4–10 and Annex A) and key principles like the risk-based approach and continuous improvement.
- Introduce the certification process and the role of a Lead Auditor.

Learning Objectives: Understand the purpose of ISO 27001, key terminology, and the PDCA (Plan-Do-Check-Act) cycle for managing information security. Students should grasp how an ISMS helps organizations protect information assets and meet regulatory/customer requirements.

STUDY SESSION

Case Study Kick-off – ISMS Scope & Context

In groups, students are given a fictional company profile. They begin real-world ISO 27001 implementation by defining the ISMS scope and context for that company. Activities include identifying business objectives, critical assets, stakeholders, and regulatory requirements.

Practical Application: Students draft an "ISMS Scope Statement" and list of stakeholders, simulating how a company starts ISO 27001 compliance. They also outline how top management support will be obtained (e.g. a brief presentation to the "board" about ISMS importance)

MENTOR MEETING

The mentor reviews each group's ISMS scope document and provides feedback. They answer questions about interpreting ISO 27001 clauses and share insights on real companies initiating ISO 27001 projects.

Key Takeaway: Students gain clarity on setting ISMS boundaries and learn that management buy-in is critical for success

DELIVERABLES

ISMS Scope Statement and Context Analysis for the case-study organization.

Preparation for Next Week: Read ISO 27001 clauses 4–5 (Context and Leadership) and come with ideas on information security policies needed.

Week 2

ISMS Requirements and Risk Management Planning

MONDAY SESSION

ISO 27001 Clauses 4–6 & Risk Management

Dive into key ISO 27001 requirements – Clause 4 (Context), Clause 5 (Leadership and ISMS Policy), and Clause 6 (Planning). Emphasis on risk management planning: how organizations identify and assess information security risks and set objectives. Introduce ISO 27005 as guidance for risk assessment.

Learning Objectives: Be able to interpret ISO 27001 requirements for defining ISMS scope, writing an Information Security Policy, and establishing a risk assessment methodology. Students should understand the concept of risk appetite and the need for risk criteria before an audit.

STUDY SESSION

Risk Assessment Workshop (Part 1)

Students apply a step-by-step risk assessment process to their case study org. They create an asset inventory and identify potential threats and vulnerabilities. Working in teams, they perform a preliminary risk assessment: brainstorming what could go wrong (security incidents) and how likely/severe each scenario is.

Practical Application: This mirrors real-world ISMS implementation steps, as well as what auditors look for – a defined process for risk identification and evaluation.

MENTOR MEETING

The mentor discusses common pitfalls in risk assessments and reviews the teams' threat/vulnerability lists. They share examples of risk registers from industry.

Key Takeaway: Students learn that a structured risk assessment is foundational to ISO 27001 – auditors will verify that risks to information are identified and managed systematically. Mentors ensure students' risk lists align with business context.

DELIVERABLES

Draft Risk Register (asset list with identified threats, vulnerabilities, initial risk ratings).

Preparation: Refine risk analysis and read Annex A control domains to prepare for selecting controls next week.

Week 3

Risk Treatment and Control Selection (ISO 27001 Planning)

MONDAY SESSION

ISO 27001 Clauses 4–6 & Risk Management

- Focus on Clause 6 continued – developing a Risk Treatment Plan. Students learn how to determine which risks to mitigate, accept, transfer, or avoid, and how to choose security controls (safeguards) to treat risks.
- Provide an overview of Annex A controls (information security control categories) and the requirement to produce a Statement of Applicability (SoA).

Learning Objectives: Be capable of recommending appropriate controls for identified risks and understand how to justify those choices in an SoA document. Also, recognize that auditors check if chosen controls correspond to assessed risks.

STUDY SESSION

Risk Treatment Plan Development

Each group uses their Week 2 risk register to decide on treatments. They map risks to relevant Annex A controls. For example, if “unauthorized access to client data” was a top risk, they might choose controls like access control policies, user access reviews, and encryption.

Practical Application: Students create a Statement of Applicability, listing which Annex A controls are implemented or not, with justifications. This hands-on task mirrors real ISO 27001 implementation and gives insight into how organizations tailor the standard to their needs.

MENTOR MEETING

The mentor reviews the draft SoA and risk treatment plans. They ensure students justify control selections in business terms (e.g. “Control A.9 (Access Control) chosen to mitigate risk of data leakage”).

Key Takeaway: Students see how ISO 27001 bridges identified risks with concrete controls, a process auditors will scrutinize for completeness and alignment

DELIVERABLES

Risk Treatment Plan and initial Statement of Applicability for the case org.

Preparation: Teams prepare to draft or update actual security policies corresponding to selected controls (e.g. an Access Control Policy) for next week.

Week 4

ISMS Documentation and Implementation

MONDAY SESSION

Implementing Controls & Documented Information

Cover Clause 7 (Support) and Clause 8 (Operation) of ISO 27001. Discuss required documented information: security policies, procedures, training records, etc., and how to implement controls in practice. Topics include developing policies for key areas (access control, incident management, business continuity) and conducting staff security awareness training.

Learning Objectives: Learn the essential documents an ISMS needs (Acceptable Use Policy, Incident Response Procedure, etc.) and how to implement controls effectively. Students should be aware that auditors will sample these documents and evidence of control operation (e.g. firewall configuration, training attendance) to verify compliance

STUDY SESSION

ISMS Policy Development

Students create or refine one or two key ISMS documents for their case company. For example, Group A drafts an **Access Control Policy** detailing user account management and authentication rules, while Group B drafts an **Incident Response Procedure** aligned with ISO 27001 and anticipating ISO 27035 concepts.

Practical Application: This exercise gives experience in writing policies – a common real-world task. It also prepares students for the incident management training coming up. Each group also implements a simple security control if possible (e.g. setting up a demo password policy on a test system) to see implementation challenges.

MENTOR MEETING

The mentor reviews the drafted policies, checking they meet ISO 27001 requirements and are practical. They share tips on keeping policies clear and enforceable.

Key Takeaway: Well-documented policies are the backbone of an ISMS; students learn how to articulate controls in writing. This experience will help them audit documentation in the future, as Lead Auditors often check if policies address the standard's clauses and identified risks

DELIVERABLES

Two key ISMS documents (e.g. Access Control Policy, Incident Management Procedure) for the case study, and evidence of at least one implemented control (which could be a screenshot or description of a configured setting).

Preparation: Read ISO 27001 Clauses 9–10 (Performance Evaluation and Improvement) for next week.

Week 5

ISMS Monitoring, Internal Audit and Management Review

MONDAY SESSION

ISO 27001 Clauses 9 & 10 – Measuring and Improving ISMS

Focus on how organizations monitor and measure their ISMS. Topics include selecting ISMS metrics, conducting internal audits (ISO 27001 Clause 9.2), management review meetings, handling nonconformities, and continuous improvement (Clause 10).

Learning Objectives: Understand the audit cycle within an ISMS – how to plan and perform internal audits in accordance with ISO 19011 guidelines, and how management reviews drive improvements. Students should learn what evidence a Lead Auditor expects for performance evaluation (audit reports, incident logs, KPIs)

STUDY SESSION

Mock Internal Audit Exercise

Students simulate an internal audit on their case company's ISMS. One team acts as auditors and another as auditees. They use an internal audit checklist (covering a few ISO 27001 clauses or controls implemented in prior weeks) to find any gaps. For instance, audit whether the Access Control Policy drafted in Week 4 is being "followed" (did everyone set strong passwords in the test system?).

Practical Application: This role-play gives insight into audit techniques in a low-stakes setting. It reinforces ISO 27001 requirements and builds student confidence in asking audit questions and collecting evidence

MENTOR MEETING

The mentor debriefs the internal audit exercise. They discuss any "nonconformities" found by students and how to write them up. The mentor also emphasizes the importance of **continuous improvement** – even after certification, companies must regularly audit and refine their ISMS.

Key Takeaway: Students experience both sides of an audit, learning that auditing is about verifying effectiveness, not just existence, of controls. This directly prepares them for the Lead Auditor role by practicing audit principles in a real scenario

DELIVERABLES

Internal Audit Checklist used and a short **Internal Audit Report** or summary of findings/recommendations from the mock audit.

Preparation: Study ISO 19011 (audit principles) summary and sample ISO 27001 audit questions for next week's deep dive into the auditing process.

Week 6

Audit Principles and Planning (ISO 27001 Lead Auditor Training)

MONDAY SESSION

Audit Fundamentals & Stage 1 Audit Planning

- Transition fully into the ISO 27001 Lead Auditor training content.
- Cover fundamental audit principles (per ISO 19011): integrity, fair presentation, due professional care, evidence-based approach, and risk-based auditing.
- Discuss the audit process stages and focus on **Stage 1 Audit** (audit preparation and initial review).
- Students learn how to develop an audit plan, define audit scope and objectives, and review ISMS documentation as an auditor.

Learning Objectives: Be able to plan an ISO 27001 compliance audit – including creating an audit plan/schedule and checklist – in line with ISO 19011 and ISO/IEC 17021-1 requirements. They should grasp how to perform a Stage 1 audit (document review) to assess readiness.

STUDY SESSION

Audit Planning Workshop

Each student team creates an audit plan to audit a (simulated) company's ISMS. They use their case study ISMS as the target. This includes defining what locations and departments are in scope, what clauses/controls will be audited when, and assigning roles (lead vs co-auditor). They also list documents they would request in advance (SoA, policies, risk assessment, etc.).

Practical Application: This exercise mirrors real pre-audit preparation. By examining their own ISMS through an auditor's lens, students reinforce their understanding of ISO 27001 requirements and how an audit would check each area

MENTOR MEETING

The mentor reviews the audit plans, ensuring they are realistic and cover critical ISMS elements. Discussion includes how to tailor audit scope based on a company's risk (e.g., focus more on higher risk areas).

Key Takeaway: Careful planning is crucial for effective audits – students learn to scope audits properly and see that **audit planning** itself is a skill domain in the ISO 27001 Lead Auditor exam

DELIVERABLES

ISO 27001 Stage 1 Audit Plan (including scope, agenda, and document request list).

Preparation: Students read about audit evidence and interview techniques to prepare for conducting a Stage 2 audit in the next session.

Week 7

Conducting the Audit – Evidence Collection & Interviews

MONDAY SESSION

Stage 2 Audit Execution

- Focus on the on-site audit activities of a Stage 2 certification audit.
- Train students on how to con**duct effective interviews** with process owners and staff, observe operations, and sample evidence to verify compliance.
- Cover techniques for evidence gathering (reviewing logs, records, configurations) and how to trace audit trails.
- Emphasize communication skills during an audit – being objective, asking open-ended questions, and taking notes.

Learning Objectives: Become competent in executing an audit plan: conducting interviews, collecting audit evidence, and maintaining professionalism. Students learn how to identify nonconformities by comparing evidence against ISO 27001 criteria. They also learn how to handle challenging situations (e.g. uncooperative auditees or discovering a sensitive issue).

STUDY SESSION

Audit Role-Play and Case Study

In pairs, students role-play auditor and auditee for specific controls. For example, one student audits the user access management process: they interview the "IT manager" of the case company (another student) about how user accounts are created and removed, and ask to see an example record of access approval. Each pair rotates through a couple of scenarios (physical security, incident handling, etc.).

Practical Application: This simulation builds real-world auditing experience in a safe environment. Students practice verifying compliance (e.g., checking if an incident reported in logs was handled per the procedure). This directly prepares them for audit tasks they will perform in the field and aligns with the hands-on approach of Lead Auditor training

MENTOR MEETING

The mentor facilitates a debrief of the audit simulations. Students share challenges they faced and evidence they collected. The mentor provides tips on evidence quality (sufficiency and appropriateness) and reminds them that **audit findings must be based on objective evidence.**

Key Takeaway: Students gain confidence in conducting audits. They realize an auditor's role is to verify explicitly that policies and controls are working – a mindset that will serve them in the certification exam and real audits.

DELIVERABLES

Auditor's notes from the role-play (evidence observed and any potential nonconformities noted).
Preparation: Begin drafting audit findings based on role-play results; review ISO 27001 Lead Auditor sample exam questions provided by the instructor.

Week 8

Audit Reporting and Nonconformity Management

MONDAY SESSION

Closing the Audit – Findings & Reports

Teach how to formally document audit results. Students learn to write nonconformity statements that clearly explain which requirement is not met and the evidence. Cover how to grade findings (major/minor nonconformities) and the process for corrective action plans. Then discuss writing the Audit Report and conducting the closing meeting.

Learning Objectives: Be able to draft clear audit findings and compile an audit report that provides value to the auditee. Understand the follow-up process: how auditors evaluate corrective actions and what happens in surveillance audits. This knowledge directly maps to ISO 27001 Lead Auditor competencies (reporting and follow-up is a key domain).

STUDY SESSION

Audit Report Drafting

Students individually or in teams write a short Audit Findings Report for their case study ISMS based on all the prior exercises (internal audit, role-plays, document reviews). They must include at least 2 nonconformities or observations – for example, “Minor Nonconformity: Password policy not enforced – 2 of 5 sampled accounts had weak passwords, violating ISO 27001 A.9.2.3.” They also craft an executive summary and some positive notes (strengths).

Practical Application: This task hones real auditor skills in articulating results. It also finalizes their ISO 27001 project: they see how an auditor would view the ISMS they built.

MENTOR MEETING

The mentor reviews and critiques the audit reports. This feedback helps students refine their writing to be factual and concise. The mentor also shares examples of actual audit reports and how findings are presented to management.

Key Takeaway: Students learn that clear communication of audit results is vital – a skill tested in the Lead Auditor exam and crucial in consulting engagements. They also see how their weeks of work translate into auditable outcomes, cementing the link between theory, practice, and professional audit responsibilities.

DELIVERABLES

ISO 27001 Audit Findings & Report (draft).

Preparation: Study for ISO 27001 Lead Auditor exam – review all key ISO 27001 clauses, controls, and audit principles. Practice with additional sample questions.

Week 9

Certification Exam Preparation & Review of ISMS Project

MONDAY SESSION

ISO 27001 Knowledge Review and Q&A

- A comprehensive review session covering the full ISO 27001 Lead Auditor syllabus.
- Instructors run through a high-level recap of ISMS concepts, audit process stages, and sample scenarios.
- Students engage in a Q&A to clarify any remaining doubts. A set of practice exam questions (simulating the certification exam format) is administered under timed conditions.

Learning Objectives: Ensure students consolidate their knowledge and can recall key points quickly – from ISMS clause details to audit technique – as required for the exam. Emphasize tricky areas (e.g., distinguishing Clause 9.2 internal audit vs external audit roles).

STUDY SESSION

Practice Exam & Project Retrospective

Students take a mock ISO 27001 Lead Auditor exam (covering all domains) and then review answers together with the instructor to understand any mistakes. Afterwards, they finalize their case study ISMS project documentation as a portfolio (Scope, Policies, Risk Assessment, SoA, Audit report, etc.). They prepare a short presentation summarizing how they implemented ISO 27001 in the case study, as a way to reflect on lessons learned.

Practical Application: This retrospective ties the theoretical learning to the practical project, reinforcing how each piece of the ISMS fits together. It also mimics what a Lead Auditor might do post-audit – summarizing findings and recommending improvements.

MENTOR MEETING

The mentor focuses this meeting on exam readiness and confidence-building. They share exam-taking tips and, if they are certified themselves, personal anecdotes of the test. The mentor also listens to students practice explaining their project (as if reporting to a client), giving feedback on clarity and professionalism.

Key Takeaway: Students feel prepared to pass the **ISO 27001 Lead Auditor certification exam**, having addressed any weak areas. They also appreciate the real-world experience gained – by now they have essentially performed an end-to-end ISMS implementation and audit in miniature, which is exactly the practical understanding a good auditor needs

DELIVERABLES

Completed ISMS Project Portfolio and a brief presentation. Mock exam results (for self-assessment).

Preparation: Finalize studying for the official ISO 27001 Lead Auditor exam, which is scheduled at the beginning of Week 10.

Week 10

ISO 27001 Lead Auditor Exam and Transition

MONDAY SESSION

Certification Exam & Transition to Next Module

Students take the ISO 27001 Lead Auditor certification exam (typically a 2-hour written exam) under formal conditions. This exam, administered by an accredited body or the training provider, tests the knowledge and skills gained in Weeks 1–9. Upon completion, the class has a debrief (without discussing specific exam content, to maintain integrity). The instructor then introduces the next phase of the program – Incident Management (ISO 27035) – drawing connections between ISMS and incident response (e.g., how ISO 27001 clause on incident management leads into ISO 27035 best practices).

STUDY SESSION

Light Session & Knowledge Sharing

Since the exam is intensive, the study session is lighter. Students participate in a workshop on continuing ISMS maintenance: how to keep improving security post-certification. They also share any insights from the exam (generically, like which topics they felt strong in or not). The instructor might start a short introductory exercise for incident management – for example, brainstorming recent cybersecurity incidents in the news and how an ISMS might handle them.

Practical Application: This bridges to incident response by getting students to think of real breaches and the importance of having an incident plan (setting the stage for ISO 27035).

MENTOR MEETING

The mentor checks in on students' exam experience and well-being. They congratulate students on completing the first certification. The meeting also covers goal-setting for the next phase: mentors help students see how their new auditing skills will complement incident management (e.g., they'll audit incident processes or help create them).

Key Takeaway: Achieving the ISO 27001 Lead Auditor credential is a major milestone – students now have proven skills to audit ISMS. With that success, they are motivated to tackle incident management. The mentor reinforces how **real-world experience** from the ISMS project will inform their approach to handling security incidents in the next weeks.

DELIVERABLES

ISO 27001 Lead Auditor Exam completion (and hopefully certification award if results are immediate). There is no new project deliverable this week aside from transition notes.

Preparation: No specific homework other than optional reading of an incident management case study to prepare for Week 11.

WEEK 11-15:
ISO 27035 INCIDENT MANAGEMENT TRAINING

OVERVIEW

In Weeks 11–15, the program focuses on Information Security Incident Management per ISO/IEC 27035. Building on the ISMS foundation, students learn to establish and lead effective incident response processes. Monday lectures cover the incident management lifecycle – from preparation and detection to response, recovery, and continuous improvement.

The second study day involves hands-on incident response exercises, such as drafting incident plans and handling simulated cybersecurity incidents. By the end of Week 15, students will be ready for an ISO 27035 Lead Incident Manager certification exam and have practical experience managing incidents (through tabletop simulations and analysis of case studies). This module ensures students can not only set up security controls (from Phase 1) but also react effectively when those controls are tested by real incidents.

Week 11

Incident Management Fundamentals and ISO 27035 Overview

MONDAY SESSION

Introduction to Incident Management & ISO 27035

- Explain what constitutes a security incident and why systematic incident management is crucial (to minimize damage and recover quickly).
- Provide an overview of the ISO/IEC 27035 standard, which outlines principles and processes for incident management.
- Cover the **incident lifecycle stages**: Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned. Relate this to the real world with examples (e.g., a data breach timeline).

Learning Objectives: Grasp the key concepts and definitions of incident management and the structure of ISO 27035. Students should understand that incidents are inevitable and that preparation and having a defined process can drastically reduce impact.

STUDY SESSION

Dissecting a Cyber Incident

Students analyze a famous cybersecurity incident (for example, the Target retail breach or a recent ransomware attack). They work in teams to map the incident to the stages of the incident lifecycle: How was it detected? What containment steps were taken? What could have been done better in preparation?

Practical Application: By examining a real incident post-mortem, students connect theory to reality – seeing how in practice an incident response might succeed or fail. This also highlights the importance of each lifecycle phase (e.g., lacking preparation can worsen an incident).

MENTOR MEETING

The mentor leads a discussion on the chosen case study, filling in details and corrections to student analysis. They share first-hand experience or war stories of incidents they've handled, emphasizing the value of preparation and a clear process.

Key Takeaway: Students learn that incident management is not ad-hoc firefighting; it requires planning and roles defined in advance. This session sets the stage for them to create their own incident response plans in upcoming weeks.

DELIVERABLES

Incident Case Study Analysis (a brief report or presentation outlining the incident timeline and lessons learned).

Preparation: Read ISO 27035-1 sections on principles of incident management and prepare to draft an Incident Response Policy next week.

Week 12

Establishing an Incident Response Capability (Preparation Phase)

MONDAY SESSION

Incident Response Planning and Team Structure

Deep dive into the **Preparation phase** of incident management. Topics include forming an Incident Response Team (IRT) with defined roles (incident manager, communicators, technical leads, etc.), creating an Incident Response Policy, and equipping the team with tools and training. Students learn what an Incident Response Plan (IR Plan) contains – contact lists, communication protocols (including escalation and regulatory reporting), and procedures for common incident types. Also discuss coordination with external entities (law enforcement, cyber insurance, etc.).

Learning Objectives: Be able to develop and document an incident management policy and plan for an organization. Understand the importance of clear roles and communication channels before an incident occurs. This aligns with ISO 27035 guidance to implement and manage an ongoing incident management program.

STUDY SESSION

Drafting an Incident Response Plan

Students create an **Incident Response Plan** for their case study company. Using a template or outline provided, they define the incident severity levels, roles and responsibilities (who leads the response, who contacts customers, etc.), and step-by-step procedures for at least one incident scenario (e.g., malware outbreak or data leak). They also outline a training/drill schedule to keep the team prepared.

Practical Application: This exercise simulates real-world consulting work – developing an IR Plan tailored to a company. It reinforces planning skills and integrates knowledge from ISO 27001 (e.g., linking this plan to the ISMS's incident management requirement).

MENTOR MEETING

The mentor reviews sections of each team's Incident Response Plan, providing feedback especially on clarity and completeness. They might role-play as a CEO or regulator to ensure the plan includes communication to stakeholders.

Key Takeaway: Students produce a tangible incident management deliverable. They learn that **good preparation** (a thorough, well-communicated plan) can make the difference in handling incidents smoothly. Auditors (like their future selves) would also check for such plans, so this ties back to their ISO 27001 auditing perspective too.

DELIVERABLES

Incident Response Plan document (initial draft with policy statement, team roles, and procedures for at least one incident type).
Preparation: Read about incident detection techniques (IDS/monitoring) and think of how one would identify different types of incidents for next week.

Week 13

Incident Detection, Analysis, and Response Execution

MONDAY SESSION

Detection and Response Strategies

Focus on the **Identification** and **Response** phases. Teach how organizations detect incidents – through monitoring systems, IDS/IPS alerts, user reports, etc. Cover initial triage: validating an incident and assessing its severity. Then detail **Response actions**: containment strategies (isolating affected systems, e.g. disconnecting a server), eradication (removing malware, disabling compromised accounts), and recovery (restoring systems from backups, verifying integrity). Include guidance on documenting the incident as it unfolds (incident logs) and maintaining chain-of-custody for forensic data if needed.

Learning Objectives: Know how to recognize signs of an incident and initiate an effective response.Be familiar with common techniques for containing different incident types (like disconnecting network cables for ransomware, or applying patches for a vulnerability being exploited). Understand how to balance swift action with thorough analysis.

STUDY SESSION

Tabletop Incident Simulation

Students participate in a facilitated tabletop exercise simulating a cyber incident. For example, the scenario could be: “Monday 9am, the company’s web server is defaced by hackers, and customer data might be stolen.” The class is divided into incident team roles and must work through the simulation: How do they detect it (perhaps a monitoring alert)? What steps do they take in the first hour? How do they contain the breach? The instructor feeds additional developments as time “advances” (e.g., hackers demand ransom, or malware spreads).

Practical Application: This simulation forces students to apply their Incident Response Plan under time pressure. They practice communication (drafting an email to alert all staff, for instance) and decision-making with incomplete information – exactly the challenges of real incidents. It builds teamwork and exposes any weaknesses in their plan or understanding, which is a safe learning opportunity rather than a real business loss.

MENTOR MEETING

The mentor debriefs the simulation. They ask each role what went well and what was challenging. The mentor highlights best practices observed and points out any missed steps (e.g., “No one thought to check the firewall logs early – in real life that could help trace the attack path”). They also tie back to ISO 27035: how formalizing these steps ensures consistency and improvement.

Key Takeaway: Students gain confidence in their ability to handle incidents in real-time. They realize incident response is hectic but manageable with a clear plan. This exercise also prepares them for the incident management exam by reinforcing practical application of ISO 27035 concepts (which cover detection and response processes)

DELIVERABLES

Incident Simulation Report – each team writes a brief report of what actions they took during the exercise, including a timeline of events and decisions.
Preparation: Teams update their Incident Response Plan with any improvements noted (if, for example, the simulation revealed missing steps). Read ISO 27035 guidance on post-incident activities for next week.

Week 14

Post-Incident Activities and Continuous Improvement

MONDAY SESSION

Recovery, Reporting, and Lessons Learned

Cover the final phases of the incident lifecycle: Recovery (return to normal operations securely) and Post-Incident Review. Teach students how to verify that threats are eradicated (e.g., ensure malware is truly gone, vulnerabilities closed) and safely bring systems back online. Discuss formal incident reporting obligations (both internal reports to management and possibly external notifications to regulators or affected customers, depending on breach laws). Then focus on Lessons Learned: conducting a post-incident analysis meeting to identify what went wrong, what was handled well, and how to improve. Introduce the concept of updating policies and plans based on incidents – feeding into the continuous improvement loop (which links back to ISO 27001 Clause 10).

Learning Objectives: Be able to organize a post-incident review process that results in concrete recommendations. Understand the importance of documenting incidents and reporting to stakeholders (transparency and compliance). Recognize that every incident is an opportunity to strengthen the security posture.

STUDY SESSION

Lessons Learned Workshop

Students revisit the tabletop exercise from Week 13 or choose another incident scenario they've studied. They conduct a mock "lessons learned" meeting for their case company. Each team creates a brief Incident Report that includes: summary of what happened, root cause analysis (e.g., "phishing email allowed access – root cause was lack of MFA on that account"), and a list of corrective actions (e.g., "implement MFA for all remote accesses, improve staff phishing training, update IR plan to include law enforcement contact info").

Practical Application: Writing this report reinforces how organizations turn an incident into actionable improvements. It also yields a tangible artifact akin to what an Incident Manager would produce for executives or auditors after a breach. Students see how this ties back to governance: these recommendations might update the ISMS or risk register, demonstrating the interlink between ISO 27035 and ISO 27001.

MENTOR MEETING

The mentor reviews the draft Incident Reports and root cause analyses. They ensure students dug deep enough to find underlying issues (sometimes non-technical, like "poor security awareness training" as a cause of a successful phishing attack). The mentor also discusses how to present such findings diplomatically to management – focusing on solutions rather than blame.

Key Takeaway: Students learn the value of continuous improvement in cybersecurity – a core theme of all these standards. By completing the incident lifecycle, they have experienced how a mature organization not only handles incidents but grows from them. This perspective will be valuable in the CARR risk review phase and in real jobs, where learning from mistakes is key.

DELIVERABLES

Post-Incident Report and Lessons Learned document for the simulated incident.

Preparation: Consolidate all incident management documentation (policy, plan, simulation report, lessons learned) into a study packet. Review the ISO 27035 domains and be ready for a practice quiz in Week 15.

Week 15

Incident Manager Certification Prep and Capstone Exercise

MONDAY SESSION

ISO 27035 Exam Preparation & Integration

Review the full incident management framework in preparation for the ISO/IEC 27035 Lead Incident Manager exam. The instructor highlights how the course content maps to the exam domains (e.g., incident management concepts, designing an incident management process, responding to incidents, and improving processes). Students complete a set of practice exam questions covering scenarios like “What is the best course of action during incident containment...” etc. The session also revisits how incident management ties into overall security management – setting the stage for the upcoming CARR (risk review) module by noting that trends from incidents inform risk assessments.

Learning Objectives: Solidify knowledge so that students can confidently attempt the incident management certification exam. Ensure they can articulate the incident management plan they created and the rationale behind each step.

STUDY SESSION

Integrated Drill and Wrap-Up

As a capstone, students participate in an integrated cyber drill that combines ISMS and incident management. For instance, they might be given a new mini-scenario like a lost company laptop. They must go through incident handling steps (report, contain – e.g., remotely wipe the laptop) and consider ISMS implications (update asset inventory, consider if policy changes are needed for encryption). This exercise reinforces that security domains are interconnected. After the drill, any remaining questions on ISO 27035 are answered. If the actual certification exam is scheduled separately (e.g., at week’s end), the study session can be partly an open Q&A and last-minute clarification.

MENTOR MEETING

The mentor uses this final meeting of Phase 2 to ensure each student is ready for the ISO 27035 exam and to reflect on their growth. They encourage students to recall how at the start of the program they hadn’t conducted an incident response before, and now they have done multiple simulations.

Key Takeaway: Students are now equipped to achieve the ISO 27035 Lead Incident Manager certification, having covered the entire incident lifecycle from planning to lessons learned. They also appreciate how theory (ISO standards) translated directly into practice via the drills. The mentor sets expectations for the next phase: using their audit and incident skills to perform broad security assessments in the CARR program.

DELIVERABLES

Completion of a mock Incident Management exam (graded for feedback). All incident management project artifacts compiled for submission.

Preparation: Take the official ISO 27035 Lead Incident Manager exam (timed ideally end of this week or beginning of next, depending on scheduling). Begin reading an overview of risk assessment frameworks (like NIST CSF or others) to prepare for the CARR module.

WEEK 16-20:
CARR PROGRAM (CYBER ASSURANCE RISK REVIEW) AND APPLIED RISK ASSESSMENT

OVERVIEW

Weeks 16–20 introduce the **CARR (Cyber Assurance Risk Rating) program**, a methodology for comprehensive cybersecurity assessments. In this module, students step into the role of a cybersecurity assessor, leveraging their auditing and incident knowledge to evaluate an organization's overall security posture. Monday sessions teach the components of a CARR review – governance, technical controls, culture, third-party risks – and how to assign a quantitative risk rating.

The study days are very hands-on: students will conduct a mock CARR assessment of a new case study organization (or possibly their own institution), reviewing documents, interviewing (simulated) staff, and using tools to gather data. This culminates in producing a CARR report with a score and recommendations. By week 20, students will effectively act as consultants preparing to do real client reviews during their internships. They will also earn a **CARR program certification** from the training provider upon successful completion of a practice assessment.

Week 16

Introduction to CARR and Assessment Frameworks

MONDAY SESSION

What is CARR? Understanding the 360° Risk Review

Introduce the purpose and scope of the CARR program. Explain that CARR provides a 360-degree view of an organization's cybersecurity environment, covering technical controls, governance, culture, internal and external factors. Students learn how CARR differs from a strict compliance audit: it's more of a holistic maturity assessment and risk rating. Discuss the structure of a typical CARR assessment – areas evaluated (e.g., policy maturity, identity & access management, threat protection, data security, incident readiness, vendor risk, etc.) and the scoring mechanism (how findings translate into a numeric score/grade).

Learning Objectives: Understand the goals of CARR – to quantitatively measure cybersecurity performance and produce a risk rating. Recognize the domains of security it covers and how it aligns with industry best practices (ISO 27001, NIST CSF, and regulatory requirements like ASIC guidelines)

STUDY SESSION

Mapping Standards to CARR Domains

Students take a set of security domains (for instance: Asset Management, Access Control, Incident Management, Vendor Management, etc.) and map which ISO 27001 controls or ISO 27035 practices relate to each. This helps them see overlap and coverage. They then review a sample CARR questionnaire or checklist (if provided) to familiarize with the kinds of questions or evidence sought. If available, they might also explore a demo of a CARR scoring tool (spreadsheet or software) with dummy data.

Practical Application: This exercise bridges prior learning with the CARR framework, showing that their ISO knowledge is directly applicable in performing a CARR review. It also preps them to gather the right information in upcoming assessments.

MENTOR MEETING

The mentor discusses how comprehensive reviews like CARR are conducted in practice – typically as short engagements where assessors must quickly gather info across many areas. They emphasize time management and communication: setting up interviews, requesting documents, etc., within a limited timeframe.

Key Takeaway: Students grasp that CARR assessments are broad in scope and require a strategic view. Unlike the narrow focus of an ISO audit or incident response, here they'll evaluate everything at once. Mentors assure them their combined skills from the first 15 weeks have built a foundation to do this.

DELIVERABLES

A domain mapping document (CARR domains <-> relevant controls/standards) and summary of insights from sample CARR materials.

Preparation: Identify a new case study (or use an external organization's profile) for the mock CARR assessment starting next week – gather any background info available about its industry, size, and known cybersecurity context.

Week 17

Assessing Governance and Security Culture

MONDAY SESSION

CARR Deep Dive: Governance & Documentation Review

Teach how to evaluate an organization's security governance and culture as part of CARR. This includes examining policies, organizational structure, leadership involvement, and overall security strategy. Students learn to assess if an organization has an ISMS or similar governance framework, how regularly management reviews security, and if there's a positive security culture among employees. Discuss techniques: interviews with leadership, employee surveys for security awareness, and reviewing documentation (policies, compliance reports, audit findings).

Learning Objectives: Be able to determine the maturity of an organization's governance (e.g., presence of security steering committees, documented strategies) and the level of security awareness among staff. Understand that these "soft" aspects are crucial to the risk rating (poor security culture can lead to high residual risk even if tech controls exist).

STUDY SESSION

Mock Assessment – Governance

Students begin their mock CARR assessment on the selected case organization focusing on governance and culture. They review the org's security policies (the instructor provides a packet of sample policies or descriptions), incident records, and past audit results if any. They also conduct a simulated interview with management – an instructor or mentor can role-play a CIO answering their questions about security priorities and resources. Students might also design a short security awareness survey and speculate on results (or use provided hypothetical survey data).
Practical Application: This hands-on assessment trains students to quickly appraise how committed an organization is to security beyond just ticking boxes. They identify gaps such as "no regular security training program" or "policies exist but employees aren't aware of them." These will later feed into their CARR recommendations.

MENTOR MEETING

The mentor reviews the governance assessment findings each team has so far. They help interpret responses from the management interview (reading between the lines – e.g., if a CIO says "we discuss security when needed," what does that imply about governance maturity?).

Key Takeaway: Students learn to analyze qualitative information and make judgments on maturity levels. They see how an assessor must sometimes identify issues like lack of top-level support or poor communication, which directly affect the organization's risk posture. This skill is different from strict compliance checking – it requires insight and sometimes delivering hard truths to leadership (which they'll practice in reporting).

DELIVERABLES

Governance & Culture Assessment Notes – including interview notes, list of governance strengths/weaknesses, and a preliminary "maturity rating" or score for governance domain.
Preparation: Plan for technical controls assessment next week: decide which areas to focus on (network security, identity management, etc.) based on the case org's profile, and request any necessary data in advance (e.g., sample network diagram or vulnerability scan results if available).

Week 18

Technical Security Controls and Operations Assessment

MONDAY SESSION

CARR Deep Dive: Technical and Operational Controls

Cover how to assess the technical side of security in a CARR review. This includes evaluating network security (firewalls, segmentation), endpoint security (antivirus, patch management), identity and access management (password policies, multi-factor authentication), application security, and security operations (monitoring, incident response readiness which they are already familiar with). Also consider external posture: penetration test results, vulnerability management, cloud security if applicable. Students learn to interpret evidence like configuration standards, tool outputs (scan reports), and incident logs to gauge effectiveness.

Learning Objectives: Develop the ability to quickly gauge an organization's technical security maturity – e.g., do they follow best practices such as regular patching and least privilege? Understand how to identify red flags (unsupported systems, excessive admin accounts, no detection capabilities) that would lower the risk rating. Emphasize that the assessor is not reconfiguring anything, but reviewing and questioning the current state.

STUDY SESSION

Mock Assessment – Technical Controls

Students continue the CARR assessment on the case org, now focusing on technical areas. They might be given a sanitized vulnerability scan report or audit report for the organization's network and have to summarize key findings (e.g., many critical vulnerabilities unpatched = low maturity in patch management). They also review user access lists or an Active Directory policy excerpt (to see if MFA is in use, etc.), and check what incident response capabilities exist (tying back to Phase 2 work). If possible, the instructor can provide a dummy network diagram or inventory to analyze. Students conduct a simulated interview with IT/security staff (instructor role-play) to ask about practices like backup routines, incident monitoring, and third-party management. **Practical Application**: This exercise trains students to analyze technical data and ask probing questions, much like a security consultant would. For example, if the org claims "we have a firewall," the students will ask "do you review firewall rules regularly? Can we see a recent review report?" By doing so, they distinguish between presence of controls and effectiveness of controls – crucial for an accurate CARR rating

MENTOR MEETING

The mentor helps interpret any technical data provided. They might walk through a sample vulnerability scan with the team, teaching how to prioritize issues. They ensure students are considering both the presence of controls and the quality of implementation.

Key Takeaway: Students improve at conducting a security assessment across IT domains. They learn not to be intimidated by technical details – even if not deeply expert in each technology, they can still assess maturity by asking the right questions and looking for key indicators (like frequency of patches, or whether multiple layers of defence exist). This skill is directly transferable to real CARR engagements and is supported by their earlier training (e.g., they know what good incident response looks like, so they can spot if this org is lacking it).

DELIVERABLES

Technical Assessment Findings – bullet list of key security control gaps or strengths identified (e.g., "Network: Firewall in place, but no network segmentation of sensitive data (gap)"; "IAM: MFA enabled for admins (strength), password policy is weak (gap)"; etc.).

Preparation: Think about risk level of each finding and possible recommendations. Next week they will learn how to translate these into a score and report, so have a sense of what the org's overall posture might be (e.g., "below average in X, above average in Y").

Week 19

Risk Rating, Reporting, and Recommendations (CARR Conclusion)

MONDAY SESSION

Calculating the CARR Score & Building the Report

Teach students how to consolidate their assessment findings into the CARR risk rating. Discuss whatever scoring methodology is used (for instance, assigning weights to domains and calculating a score out of 800 or 1000, etc.). Emphasize the need for evidence-backed scoring to keep it objective. Then focus on how to write the CARR Report: it typically includes an executive summary with the overall score and what it means (e.g., compared to industry average), a breakdown of findings by category, and a prioritized remediation roadmap. Show an example outline of a CARR report. Also cover how to formulate actionable recommendations (SMART: Specific, Measurable, Achievable, Relevant, Time-bound) – for each gap identified, there should be a suggested improvement (e.g., "Implement multi-factor authentication for remote access within 3 months").

Learning Objectives: Learn to translate qualitative and quantitative assessment data into a clear, business-friendly report that justifies the risk rating and persuades stakeholders to take action. Students should be able to articulate both the current state and the target state (what needs to be improved) in plain language.

STUDY SESSION

Drafting the CARR Assessment Report

Students compile all their findings from Weeks 17–18 into a coherent CARR report for the case organization. They determine an overall score or grade (with instructor guidance on scoring model). They write an Executive Summary that might say, for example: "Organization X scored 550 out of 1000 in the CARR assessment, indicating a below-average cybersecurity posture relative to peers. Key risk areas include outdated software and lack of formal security governance, which increase likelihood of a serious incident." Then, in the main report, they list findings by category with their recommendations.

Practical Application: This task mirrors the deliverable they will produce during their real internship assessments. It forces them to prioritize issues (not every minor issue can appear in an exec summary) and to phrase technical problems in terms executives care about (risk and business impact). They also practice the quantitative aspect – turning their judgment into a score requires calibration and justification, an important consultancy skill.

MENTOR MEETING

The mentor reviews report drafts and gives feedback on clarity and impact. They ensure the recommendations are actionable and aligned with best practices (for instance, if a team suggests "get ISO 27001 certified" as a recommendation, mentor might refine it to "implement an ISMS for systematic security management"). The mentor also checks that the tone is constructive – a CARR report should spur improvement, not just criticize. **Key Takeaway**: Students learn how to communicate a comprehensive risk assessment effectively. By justifying their CARR score and recommendations, they reinforce their understanding of why those security controls matter. This also enhances their presentation skills, as they will present these findings next week.

DELIVERABLES

Draft CARR Assessment Report for the case study, including an overall risk rating score and a list of prioritized recommendations.

Preparation: Finalize the report and prepare a brief presentation of findings as if to the company's executives. Also, ensure all team members understand every part of the assessment, anticipating questions that might be asked.

Week 20

CARR Presentation, Certification, and Phase Wrap-Up

MONDAY SESSION

Presentation of CARR Findings

Each student team delivers a presentation as if they were consultants presenting the CARR assessment results to the client's senior management. They cover the overall score, the top 3-5 findings, and recommended next steps. This serves as both an assessment of their work and a practice of client communication. Instructors and mentors (acting as the "executives") ask questions during the presentation, such as clarifications or "what-if" scenarios ("What would you suggest we tackle first and why?"). After presentations, the instructor debriefs and ensures key points are driven home. The session ends with a formal completion of the CARR training – if there is a certification exam or evaluation for CARR, it may be conducted (for example, a quiz on the CARR methodology or an evaluation of their report). Successful students are awarded a **CARR program certification** acknowledging their ability to perform cybersecurity risk reviews

STUDY SESSION

Transition to Internship Planning

With the formal CARR module done, this session prepares students for the upcoming real internships. They discuss logistics and expectations: which companies they'll be placed in, what kinds of systems or policies those might have, and how to prepare. Students may do research on their assigned internship company's industry and any known cyber regulations or threats in that sector. Additionally, they reflect on the entire program so far, perhaps writing in a journal about how they will apply what they've learned when they step into a real office next week.

Practical Application: This is a crucial professional development moment – students shift from classroom mode to practitioner mode. Researching their internship organization helps them hit the ground running.

MENTOR MEETING

In this final weekly mentor meeting before the internship, the mentor provides individualized advice for each student's placement. For example, "You're going to a financial services company – remember the importance of compliance (ASIC APRA guidelines) in your assessment. Review encryption controls, as those are often scrutinized." They also cover etiquette and mindset: being proactive, asking questions, and observing experienced professionals.

Key Takeaway: Students finish Phase 3 with a validated skillset in performing cyber risk reviews and are mentally prepared to apply these skills in a real-world setting. They have effectively earned a certification in the CARR methodology, demonstrating their capability to provide a "360-degree cybersecurity review". Now they are ready to transition into the workplace and gain on-the-job experience.

DELIVERABLES

Final CARR Assessment Report and Presentation slides (submitted for evaluation). Possibly a CARR knowledge test or quiz (depending on certification process) – completion will yield the CARR program certificate.

Preparation: Rest and get ready for the internship; coordinate with host company for any onboarding requirements (NDAs, accounts setup, etc.). Optionally, review notes on audit and CARR to be sharp for real assessments.

WEEK 21-28:
MCP TRAINING – MICROSOFT SECURITY TECHNOLOGIES AND CERTIFICATION

OVERVIEW

Weeks 21–28 shift focus to technical cybersecurity skills, specifically through MCP (Microsoft Certified Professional) training in security, compliance, and identity. In this phase, students learn to implement and manage security controls using Microsoft technologies, reflecting the fact that many organizations rely on Microsoft's ecosystem (Azure, M365, Windows) for their infrastructure. Monday sessions cover key topics aligned with a Microsoft certification exam syllabus (for example, **Security, Compliance & Identity Fundamentals SC-900**, or a similar certification) – identity and access management, platform protection, security operations, and compliance solutions.

The second study day involves practical labs in a Microsoft 365/Azure demo environment: configuring policies, analysing security alerts, and protecting data. By the end of Week 28, students will be prepared to take a Microsoft certification exam and will have hands-on experience with enterprise security tools. This practical knowledge complements their governance/risk skills with operational security know-how. (Note: MCP generally denotes Microsoft Certified Professional, validating technical expertise across Microsoft products

Week 21

Security in the Microsoft Ecosystem – Overview and Azure AD Basics

MONDAY SESSION

Microsoft Security Fundamentals & Azure AD

Provide a broad overview of Microsoft's security, compliance, and identity landscape. Introduce Azure Active Directory (now part of Microsoft Entra) as the heart of identity and access in Microsoft environments. Cover basic concepts of authentication, authorization, and identity management in Azure AD – tenants, users, groups, roles, and applications. Discuss how Azure AD implements Zero Trust principles (verify explicitly, least privilege, assume breach) – for instance, through Conditional Access policies.

Learning Objectives: Understand the fundamental role of identity in cloud security and get familiar with Azure AD's interface and core features. Students should see how Microsoft's cloud services require a strong identity foundation and how this ties back to controlling access (which they saw in ISO 27001 Annex A controls).

STUDY SESSION

Lab – Azure AD Setup

Students log into a provided Microsoft 365/Azure trial environment (or use a simulation) to perform basic Azure AD tasks. They create a few user accounts and groups, assign licenses or roles, and configure a basic Conditional Access Policy (e.g., require MFA for an admin account). If a live environment is available, they test the policy by attempting a login under conditions that trigger MFA.

Practical Application: This hands-on lab solidifies their understanding of identity management. It shows how policies are implemented in a real tool, connecting concept to execution. It also prepares them for exam objectives related to identity and access (which are significant in Microsoft certifications)

MENTOR MEETING

The mentor discusses real-world identity management challenges in companies (like managing thousands of users, integrating with on-prem AD, etc.). They ensure students understand Zero Trust in practice – e.g., share that "Zero Trust model assumes breach and verifies each request as if it originated from an uncontrolled network," which is exactly what Conditional Access achieves by checking each login.

Key Takeaway: Students appreciate that identity is the new perimeter in cloud security. By successfully configuring Azure AD policies, they've taken the first step toward being a Microsoft Certified Professional in security. They also see alignment: the exam they're targeting will test knowledge on Azure AD and identity concepts, which they are now getting hands-on with

DELIVERABLES

Azure AD lab report (screenshots or descriptions of created users/groups and the MFA policy test results).

Preparation: Read about Microsoft's threat protection solutions (Defender suite) for next week, and complete a Microsoft Learn module on security fundamentals if assigned.

Week 22

Microsoft 365 Security – Threat Protection and Device Security

MONDAY SESSION

Defender Suite and Endpoint Security

Focus on Microsoft's threat protection services in Microsoft 365 and Azure. Introduce Microsoft Defender for Endpoint (endpoint detection & response), Defender for Office 365 (email & collaboration protection), and Defender for Identity/Cloud Apps briefly. Explain how these tools work together to prevent, detect, and respond to threats (malware, phishing, etc.) in a modern workplace. Also cover Windows security features (BitLocker encryption, Windows Defender AV, Windows Hello, etc.) as part of endpoint security baseline.

Learning Objectives: Know the capabilities of Microsoft's security solutions to protect devices and data. Understand key concepts like EDR (Endpoint Detection and Response), anti-phishing policies, and secure configuration baselines. Relate this to incident management: these tools generate alerts that analysts must handle.

STUDY SESSION

Lab – Defender in Action

Students perform a lab in which they explore the Microsoft 365 Defender portal (or a simulation). They might be given a scenario: e.g., a phishing email was sent to a user. In the lab, they navigate to Defender for Office 365 and locate the alert or email trace (in a demo dataset). They also check Defender for Endpoint's dashboard for any active alerts (perhaps a simulated malware detection on a machine). If possible, they configure a simple anti-phishing rule or Safe Links policy.

Practical Application: By interacting with these security tools, students gain practical insight into day-to-day security operations. This experience supports exam topics around describing Microsoft security solutions and more importantly, gives them real skills to respond to threats using widely adopted tools.

MENTOR MEETING

The mentor shares how threat protection is implemented in their experience – possibly discussing how E5 Security features are used in enterprises or how effective these tools are against current threats. They answer questions from students who might have seen various alerts in the lab and clarify how to prioritize and respond.

Key Takeaway: Students learn that **enterprise threat protection** involves an ecosystem of tools that work together. They see that Microsoft's security stack is quite comprehensive (covering email, endpoints, cloud apps) and that mastering it can make them valuable in security operations roles. This knowledge is directly linked to the **MCP certification objectives** around understanding Microsoft security services.

DELIVERABLES

Lab worksheet documenting at least one security alert investigated and one policy configured (e.g., anti-phishing rule).

Preparation: Review notes on Azure network security and cloud security concepts, as next week extends into Azure platform security and compliance.

Week 23

Azure Security and Compliance Management

MONDAY SESSION

Azure Infrastructure Security & Compliance Tools

Expand into Azure (cloud platform) security. Cover fundamental Azure security services: **Network Security Groups (NSGs)** and Azure Firewall for network filtering, **Azure Security Center/Defender for Cloud** for cloud posture management, and **Azure Sentinel** (cloud-native SIEM) for security monitoring. Also introduce Microsoft's compliance management tools like **Microsoft Purview Compliance Manager** and **Information Protection** (sensitivity labels, DLP – Data Loss Prevention) which ensure data is properly handled.

Learning Objectives: Understand how core cloud resources are secured (network segmentation, VM hardening, etc.) and how Azure provides unified recommendations via Defender for Cloud. Also, grasp how compliance requirements (like GDPR or data classification) can be addressed with Microsoft tools (Compliance Manager provides a score against regulations, DLP prevents data leaks). These align with exam topics on describing Azure security and compliance capabilities

STUDY SESSION

Azure Security Center and Compliance

In a controlled lab environment, students use Azure Security Center (Defender for Cloud) on a sample Azure subscription. They review the Secure Score and list of recommendations (e.g., enable MFA, close port 3389 on a VM, etc.) and note how improving these reduces risk. They then pivot to compliance: using Compliance Manager in Microsoft 365, they look at an example assessment (perhaps for ISO 27001 or GDPR) and see control status. If possible, they also create a simple sensitivity label and apply it to a document, observing how it can encrypt or mark data.

Practical Application: This gives students practice in assessing and improving a cloud environment's security posture – a likely job task for cloud security engineers. It also shows how technical measures tie into compliance obligations (which resonates with their ISO 27001 knowledge). For the exam, it reinforces understanding of Microsoft compliance solutions

MENTOR MEETING

The mentor asks students to describe how they would approach securing a new Azure deployment, listening for points covered (network controls, monitoring, secure score). They provide insight into how organizations use these Azure tools for governance (e.g., weekly review of Secure Score as a KPI). They also discuss any challenges in the lab, like understanding certain recommendations.

Key Takeaway: Students realize that **cloud security posture management** is an ongoing process – tools like Defender for Cloud make it easier by giving a score and guidance. They also appreciate that compliance is not separate from security; with tools like Purview, technical enforcement of policies (like DLP) can ensure compliance requirements are met. This integrated view is something the MCP training emphasizes (security, compliance, and identity are interconnected)

DELIVERABLES

Azure Secure Score report excerpt (what is the score, top 3 recommendations to improve) and notes from Compliance Manager (e.g., what percentage of controls were compliant in a sample standard).

Preparation: Study identity protection and access governance (topics like conditional access, Privileged Identity Management) for the next session, which will focus on advanced identity security.

Week 24

Azure Security and Compliance Management

MONDAY SESSION

Identity Security & Zero Trust Implementation

Build on earlier identity basics with advanced topics: Multi-Factor Authentication (MFA) (if not already enforced, reiterate its importance), Conditional Access policies in depth (targeting specific apps or risk conditions), Azure AD Identity Protection (Microsoft's tool for detecting compromised accounts and risky sign-ins), and Privileged Identity Management (PIM) for just-in-time admin access. Tie these into the Zero Trust model concretely: never trust, always verify means continuous assessment of session risk. Also mention passwordless authentication options (Windows Hello, FIDO2 keys) as emerging best practices.

Learning Objectives: Be able to describe and recommend measures to secure identities in Microsoft environments, which is a key aspect of Microsoft's security exam and real implementations. Understand how Azure AD Identity Protection can automatically respond to leaked credentials or atypical behaviour (e.g., disable account or force password reset), and how PIM reduces standing admin privileges.

STUDY SESSION

Lab – Conditional Access and Identity Protection

Students configure a Conditional Access policy in Azure AD (in a lab tenant) to enforce MFA or block login under certain conditions (for example, block access from foreign countries or old protocols). They simulate a sign-in that would be blocked (if possible) to see the effect. Then, in Azure AD Identity Protection (or using provided screenshots if live data is not available), they examine how risky sign-in alerts are presented. They also explore Privileged Identity Management by activating an admin role in the lab (if enabled) or reviewing how PIM requests work.

Practical Application: This lab deepens hands-on skills with identity-centric security – arguably the most critical defence in cloud services. Students gain confidence in setting policies that reflect security requirements (just as they would in a real job securing O365/Azure for a company). This directly supports exam preparation on identity and access management topics and gives them experience that many entry-level practitioners lack.

MENTOR MEETING

The mentor checks understanding by asking, for instance, how students would protect an admin account from being compromised (expecting answers like "use MFA, use PIM so it's not permanently global admin, monitor sign-in risk"). They share real incidents of identity breaches (like password spray attacks) and how Conditional Access/MFA foiled or could have foiled them.

Key Takeaway: Students reinforce that identity is a primary attack vector and Microsoft provides robust tools to mitigate this (which they now know how to use). This furthers their readiness for MCP certification, as identity and access features are a significant portion of Microsoft's Security, Compliance, and Identity content. They also feel more prepared to help manage such technologies during their internships if needed.

DELIVERABLES

Conditional Access Policy configuration summary (what conditions and access controls were set) and notes on any Identity Protection findings or PIM usage.
Preparation: Review Microsoft's information protection and data governance features for next week, possibly via a Microsoft Learn module on compliance or a case study of data loss prevention.

Week 25

Data Protection and Information Governance

MONDAY SESSION

Protecting Data – Classification, DLP, and Encryption

Focus on how Microsoft technologies help protect sensitive information. Cover Microsoft Purview Information Protection (sensitivity labels that classify and encrypt documents/emails), Data Loss Prevention (DLP) policies in Microsoft 365 (to prevent sensitive data from leaving via email or Teams), and Azure Information Protection if applicable. Discuss setting up labels for categories like “Confidential” or “Public” and enforcing rules (e.g., credit card numbers cannot be emailed unencrypted). Mention integration with Office apps (users can be prompted to label docs) and scanning of data at rest (using content scans in SharePoint/OneDrive). Also address encryption of data in transit and at rest by default in cloud services.

Learning Objectives: Learn how to implement a data classification scheme and technical controls to prevent data leakage. Understand that technology can assist users in handling data properly, but policies (from ISO 27001) need to underpin them – this ties back to their earlier work on classification policies. They should also grasp how these tools fulfill compliance requirements (HIPAA, GDPR require controlling sensitive data, etc.).

STUDY SESSION

Lab – DLP and Labelling

In the lab environment, students create a simple DLP policy (for example, configure a rule that if an email contains a 9-digit number resembling a SSN or a credit card pattern, it blocks or warns). They test this by attempting to send a dummy sensitive info in an email and observing if it gets blocked or a policy tip appears. Additionally, they create a Sensitivity Label (e.g., “Confidential – Finance”) in the Compliance Center, apply encryption to it (so only certain users can open), then apply that label to a document or email and attempt access as an unauthorized user (if feasible).

Practical Application: This lab demonstrates how organizations enforce data protection in practice. Students see immediate effects of their configurations (blocked communications, encryption preventing access), which underscores the power of well-implemented security policies. It also gives them concrete experience to talk about in interviews or to use in their internships (data protection is a big focus in many companies).

MENTOR MEETING

The mentor asks students to reflect on how the lab aligns with real business needs. They might pose a scenario: “If a company wants to prevent any employee from accidentally sharing client personal data externally, how would you achieve that with Microsoft tools?” Students should now be able to answer: “Use DLP policies with rules for personal data identifiers, and possibly sensitivity labels for confidential data, ensuring external sharing is restricted.”

Key Takeaway: Students learn that data protection is proactive and automated in modern platforms; it’s not just trusting employees to follow policy but also using tools to enforce policy. This resonates with their understanding from ISO 27001 about needing both administrative and technical controls. It also completes the coverage of Microsoft’s core security and compliance capabilities, rounding out what the MCP certification expects them to know

DELIVERABLES

Results from DLP test (e.g., screenshot of blocked email or policy tip) and a brief description of a sensitivity label created and its effect.

Preparation: Begin formal exam preparation: review all topics covered (identity, threat protection, compliance, Azure security) and use Microsoft’s official learning paths or practice tests. Also, mentors may assign practice exam questions to attempt before next session.

Week 26

Security Operations and Monitoring with Azure Sentinel

MONDAY SESSION

SIEM and Security Monitoring (Azure Sentinel)

Introduce the concept of a Security Information and Event Management (SIEM) system and how Azure Sentinel (now Microsoft Sentinel) serves as a cloud-native SIEM+SOAR (Security Orchestration Automated Response) solution. Cover how Sentinel aggregates logs from various sources (Azure, Microsoft 365, on-prem appliances via connectors) and uses analytics rules to detect threats. Show examples of incidents in Sentinel (correlated alerts) and discuss automated response playbooks (integrations with Logic Apps). Also touch on Azure Monitor and Log Analytics as underlying components.

Learning Objectives: Understand the importance of centralized logging and automated analysis in detecting advanced threats. Recognize how Microsoft Sentinel can be used to investigate an incident (similar to what they did manually in incident management, but now with tooling). This topic may be a bit beyond the fundamentals exam (SC-900) level, but it provides valuable context for real-world security operations. It reinforces incident response knowledge with tooling.

STUDY SESSION

Lab – Sentinel Investigation

In a provided Sentinel workspace (or using a simulation), students walk through a sample incident. For example, see an alert that indicates multiple failed login attempts followed by a successful login (possible brute-force). They practice using Sentinel's investigation graph, check the logs related (like sign-in logs), and maybe run a KQL (Kusto Query Language) query to dig deeper (e.g., list all logins by that account). If time, they also explore creating a simple analytic rule or see an existing one's logic.

Practical Application: This gives a taste of working in a Security Operations Center (SOC). Even if not deeply covered in the exam, it consolidates their learning: identity events, device logs, etc., all come together in Sentinel. It's a culminating technical exercise that shows how everything from Weeks 21–25 can feed into detecting and responding to incidents with automation.

MENTOR MEETING

The mentor talks about careers in security operations and how the skills learned translate into those roles. They highlight that having both management (governance) knowledge and technical ability to investigate threats is a strong combination. Any questions from the Sentinel lab or general monitoring are addressed.

Key Takeaway: Students see the bigger security picture – while they set up individual security measures earlier (MFA, DLP, etc.), a SIEM like Sentinel ties it all together to manage and respond to threats enterprise-wide. This finalizes their technical training by showing the operational side of security. They are now well-prepared to take the Microsoft Security Fundamentals (or relevant) exam, having touched on all key domains: identity, threat protection, information protection, and security management

DELIVERABLES

A brief incident investigation report from Sentinel lab (what was the alert, what did they find, was it a false positive or real issue, and what response would be triggered).

Preparation: Complete any remaining official practice exams or review materials. Ensure registration for the Microsoft certification exam (likely scheduled in Week 28). Also prepare to summarize these technical skills in their resume or discussions, as the mentor might suggest.

Week 27

Microsoft Certification Exam Preparation and Mock Test

MONDAY SESSION

Comprehensive Review of Microsoft Security & Compliance (Exam Cram)

The instructor reviews all major topics from the MCP training module, possibly in a quiz game or flashcard style to keep it engaging. They revisit each skill area: Identity (Azure AD, Conditional Access), Security Solutions (Defender suite), Compliance (DLP, labels, Compliance Manager), and Azure security basics. Any known exam tips or common tricky questions are highlighted. Students are encouraged to ask final clarifying questions.

Learning Objectives: Reinforce retention of key concepts and ensure understanding of Microsoft's terminology and services, which is important for the exam. Also, build test-taking confidence by demonstrating how to parse exam questions for keywords.

STUDY SESSION

Full-Length Practice Exam

Students take a full-length mock exam under exam-like conditions, covering the breadth of content. This could be an official practice test or a compiled set of questions. After completion, they review answers (with explanations) in a group discussion led by the instructor or mentor. This helps clear any last confusion. The instructor provides individual guidance on any weak spots revealed by the practice test results.

Practical Application: This not only prepares them for the certification exam format but also consolidates their knowledge as they discuss why certain answers are correct. It mimics the scenario of sitting for the real exam, reducing anxiety and identifying if any topic needs one more look.

MENTOR MEETING

The mentor uses this meeting as a final prep talk and Q&A for the exam. They might share their own experience achieving Microsoft certifications – focusing on the value it brought to their career. They also remind students how the technical skills gained will be used in real-world tasks (potentially even during the upcoming internship if the host company uses Microsoft products).

Key Takeaway: Students feel exam-ready and see the certification as an achievable goal that validates their new technical expertise. They also recognize that beyond the exam, they have practical skills in managing Microsoft security tools that will make them effective team members in any IT security department.

DELIVERABLES

Completed practice exam answer sheet and self-assessment notes on any remaining areas to study.

Preparation: Rest well, do a light review of notes, and be prepared to take the official Microsoft certification exam during Week 28.

Week 28

Microsoft Certification Exam and Technical Skills Wrap-Up

MONDAY SESSION

Official Microsoft Certification Exam (MCP)

Students take the scheduled Microsoft certification exam (such as the SC-900 Security, Compliance, and Identity Fundamentals, or another relevant MCP exam) in a proctored environment. This exam will test their ability to describe and apply Microsoft security solutions across identity, security, and compliance. Upon completion, immediate results are given (for most Microsoft exams). The class congratulates those who pass – they now hold a Microsoft Certified Professional credential, as passing the exam qualifies one as an MCP. In case any student doesn't pass, instructors arrange a remediation plan (they can retake later, but for the program's purpose, the focus moves on). The remainder of the session is spent debriefing the exam (at a high level, no exact questions, but topics that felt hard or easy) and discussing how these technical skills integrate with everything else learned (ISO, incident, CARR).

STUDY SESSION

Technical Capstone and Next Steps

The final study session of the training program is used for a capstone discussion or project tying all threads together. For instance, students might discuss in groups a scenario like "Your company is going for ISO 27001 certification while migrating to Azure – how do you ensure cloud security (MCP knowledge) aligns with the ISMS requirements?" They outline a plan leveraging both management and technical controls. Alternatively, this time can be used to introduce any emerging topic or tool briefly (like a teaser on AI in security, or container security) to encourage continuous learning. The session ends with a briefing on the upcoming internship: expectations to behave professionally, learn actively, and accomplish the CARR reviews.

MENTOR MEETING

This is more of a closing meeting – mentors commend the students on completing all training modules and obtaining multiple certifications. They might give last-minute advice for the internship phase (like how to approach the first day, being observant and taking initiative). Mentors ensure students have contact info in case they need guidance during the internship.

Key Takeaway: Students leave the formal training portion with **multiple credentials (ISO 27001 LA, ISO 27035 Incident Manager, CARR program certificate, and a Microsoft certification) and a robust set of skills spanning governance, risk, compliance, and technical security operations**. They are ready to apply this knowledge in the real world and have learned how each component builds on the others to create a well-rounded cybersecurity professional. The mentor encourages them to view the internship as a chance to tie it all together and gain real experience that will kickstart their careers.

DELIVERABLES

Microsoft Certification exam completion (with certificate if passed). No new project deliverable, but students have compiled a personal portfolio throughout the program (policies, plans, reports, configs from labs) which they can reference in future.

Preparation: Gear up for the internship: finalize any required paperwork and mentally review the CARR assessment process, as they will be executing that in a real company context.

WEEK 29-30:
CARR PROGRAM INTERNSHIP – REAL-WORLD CYBERSECURITY ASSESSMENTS

OVERVIEW

The final two weeks are a part-time internship at partner companies where students put into practice everything they have learned by performing actual **Cyber Assurance Risk Review (CARR) assessments** in a real corporate environment. Each student (or team) is assigned to a company (or internal department) with the task of conducting a mini security review under supervision of company security staff and the program mentors. They will spend a few days each week on-site (or remote access as appropriate) gathering information, then analysing and reporting their findings.

Throughout the internship, mentors will hold check-ins to guide the students. The result is a real report delivered to the host company, giving students tangible experience and value to showcase on their resume. This internship solidifies their transition from theoretical knowledge to practical, professional competency.

Week 29

Microsoft Certification Exam and Technical Skills Wrap-Up

ACTIVITIES

Kick-off and Information Gathering

Students begin at their assigned companies with an orientation and scope discussion. They will typically start by meeting key personnel (IT manager, Security Officer, etc.) and understanding the organization's context (industry, size, critical assets). Using the CARR methodology, they outline an assessment plan for the week. Over the course of Week 29, students perform activities similar to their mock assessment but now with real data: reviewing actual security policies and procedures, interviewing staff about practices (password management, incident history, vendor management, etc.), and possibly inspecting configurations or vulnerability scan results the company provides. They keep detailed notes of all observations.

Learning Objectives: Apply the CARR assessment framework in a live environment – learn how to professionally interact with employees to gather necessary info and how to adapt when some information is unavailable or restricted. Time management is key, as they may have only a few days to assess a broad range of controls.

MENTOR CHECK-IN

Mid-week, mentors hold a virtual or in-person check-in meeting with the interns to discuss progress. Students share what they have done, any challenges (e.g., difficulty scheduling an interview or encountering unfamiliar technology), and preliminary findings. The mentor provides advice on how to overcome obstacles and ensure all assessment areas are covered. If a student is struggling with a particular technical detail, the mentor or company supervisor helps interpret it (for instance, explaining a firewall report).

Key Takeaway: Students learn to navigate real-world constraints – unlike classroom exercises, here they might deal with incomplete data or need to exercise discretion and confidentiality. Mentor feedback ensures they remain on track to complete the review in time and maintain assessment quality.

DELIVERABLES

By the end of Week 29, students produce a Draft CARR Findings Outline for their company. This is an internal working document listing the areas reviewed and notes on strengths and weaknesses identified so far. It might not have scores yet, but it frames what will go into the final report. They should also maintain a log of interviews conducted and documents reviewed (to provide transparency and traceability of their work).

Student Preparation: Before Week 30 begins, students refine any remaining questions or areas needing follow-up at the company. They may request additional evidence or clarification from staff so that Week 30 can be focused on analysis and reporting.

Week 30

Internship Week 2 – Analysis, Reporting, and Presentation

ACTIVITIES

Completion of CARR Report and Presentation to Stakeholders

In the second week, students shift from data collection to analysis and reporting. They finalize the CARR risk rating score for the organization by evaluating all gathered information against the CARR criteria. They then write the CARR Assessment Report for the company, similar to what they practiced but now with real findings. They ensure the report is professional, clear, and sensitive to the organization's context (no confidential details are mishandled). Once the report is reviewed by their mentor/supervisor for accuracy, students present the results to the company's management in a closing meeting. In the presentation, they explain the overall security posture, commend areas of good practice, and highlight top risks with recommended improvements – effectively delivering consulting advice.

Learning Objectives: Gain experience in delivering a professional security assessment from start to finish. This includes the soft skills of presenting potentially negative findings in a constructive manner and the professional responsibility of handling real organizational risk information. Students also see first-hand how their work can influence decision-makers (management may ask questions or plan to act on recommendations).

MENTOR DEBRIEF

At the end of Week 30 (and the program), mentors and instructors hold a debrief session with the students (outside the company setting). They discuss what each student learned from the internship: surprises, insights, and how it felt compared to classroom simulations. Mentors provide final feedback on the student's performance during the internship, both from their observation and any input from the host company. They also guide students on how to leverage this experience in their career – for example, updating their CV to include the tasks and skills demonstrated, and speaking about the experience in job interviews.

Key Takeaway: Students have now successfully applied their training in a real-world scenario, completing the loop from learning to doing. They have tangible outcomes – a real risk review report – that not only validates their skills but also often provides value to the host company (some may even implement the recommendations). This experiential learning significantly boosts their confidence and employability, as they can say they've done the job of an information security auditor/consultant in practice, not just in theory

DELIVERABLES

Final CARR Assessment Report and presentation delivered to the host company. A copy (sanitized if needed) may be provided to the training program as proof of completion and for the student's portfolio. Additionally, an Internship Completion Evaluation is filled out by the company supervisor, noting the student's performance (punctuality, professionalism, quality of analysis, etc.).

PROGRAM COMPLETION

With the internship done, students complete the 30-week program and receive any diplomas or certificates of program completion. They now possess **ISO 27001 Lead Auditor** and **ISO 27035 Incident Manager certifications**, **CARR program certification**, an **MCP certification**, and hands-on experience – ***a comprehensive foundation for a career in cybersecurity.***

ISO 27001 LEAD AUDITOR INFORMATION SECURITY MANAGEMENT

ISO 27035 Cybersecurity Incident Response

CARR CYBER ASSURANCE RISK RATING

Microsoft CERTIFIED Professional

Level 2, 1 Southbank Boulevard,
Melbourne, Victoria 3006
www.aphore.com
T: 1300 041 042 (Aust)
T: 1833 882 7467 (USA)