# Full Course Outline and Syllabus Model Set

**Undergraduate, graduate, professional | Reference**

These outlines show how outcomes, activities, evidence, and updateable modules can fit together. They are deliberately product-neutral. Named tools should be selected only after the learning outcome, safety boundary, accessibility requirement, and operational support are known.

## E.1 Undergraduate Course Outline: Foundations of Cybersecurity Practice

Length: Fifteen weeks Recommended prerequisites: Basic computing and networking literacy Course purpose: Develop durable cybersecurity concepts, safe practical habits, analytical reasoning, and professional communication.

Course Outcomes

By the end of the course, learners will be able to:

1. Explain core security objectives, risk relationships, identity concepts, and defensive principles.
2. Analyze common attack paths and recommend proportionate safeguards.
3. Perform approved configuration, log-analysis, and incident-response tasks in a controlled environment.
4. Distinguish facts, assumptions, evidence, and uncertainty.
5. Communicate findings to technical and nontechnical audiences.
6. Apply legal, ethical, privacy, and authorization boundaries to coursework.

Weekly Sequence

| Week | Theme | Guided practice | Evidence |
|---|---|---|---|
| 1 | Mission, ethics, authorization, and learning environment | Scenario sorting and lab orientation | Learning agreement and diagnostic |
| 2 | Confidentiality, integrity, availability, assets, threats, and risk | Risk relationship map | Short analysis |
| 3 | Identity, authentication, authorization, and account lifecycle | Identity-lifecycle activity | Access-control explanation |
| 4 | Networks and trust boundaries | Packet-flow or architecture mapping using approved data | Annotated diagram |
| 5 | Systems, configuration, updates, and secure defaults | Configuration review | Findings and remediation plan |
| 6 | Social engineering and verification | Message-evidence lab | Reporting decision |
| 7 | Cryptography and data protection | Safe encryption demonstration and key-management discussion | Concept application |
| 8 | Mid-course integration | Scenario assessment and learner conference | Revised learning plan |
| 9 | Logging, monitoring, and detection | Log triage | Event timeline |

| Week | Theme | Guided practice | Evidence |
|---|---|---|---|
| 10 | Incident response and recovery | Tabletop exercise | Response brief |
| 11 | Cloud and shared responsibility | Responsibility and configuration analysis | Control map |
| 12 | Secure software and dependency risk | Threat model or secure-design review | Design decision record |
| 13 | Governance, policy, and professional judgment | Policy critique | Governance memo |
| 14 | Career evidence and capstone workshop | Peer review | Portfolio draft |
| 15 | Integrated demonstration and reflection | Presentation and debrief | Final project and reflection |

Assessment Model

- Diagnostic and participation evidence: 5%
- Low-stakes knowledge checks: 15%
- Practical exercises and documentation: 30%
- Scenario analyses and communication: 20%
- Integrated final project: 25%
- Professional reflection and portfolio organization: 5%

No single timed exam should be the sole evidence of course mastery.

## E.2 Graduate Course Outline: Security Architecture, Evidence, and Research

Length: Twelve to fifteen weeks Recommended prerequisites: Prior coursework or professional experience in cybersecurity and systems Course purpose: Evaluate security architectures and claims through rigorous evidence, research, design, and stakeholder analysis.

Course Outcomes

Learners will be able to:

1. Evaluate architectures, trust assumptions, identity models, dependencies, and resilience strategies.
2. Formulate researchable or designable security problems.
3. Assess source quality, methods, limitations, and reproducibility.
4. Develop and defend an architecture, experiment, policy, or applied solution.
5. Communicate uncertainty and tradeoffs to expert and executive audiences.
6. Maintain ethical, privacy, legal, and safety controls throughout the work.

Module Sequence

| Module | Focus | Core product |
|---|---|---|
| 1 | Architecture as a set of trust and risk decisions | Architecture critique |
| 2 | Threat modeling and misuse cases | Threat model with assumptions |
| 3 | Identity-centered and zero-trust design | Identity and policy decision record |
| 4 | Cloud, platform, and supply-chain dependencies | Dependency and responsibility analysis |

| Module | Focus | Core product |
|---|---|---|
| 5 | Resilience, incident response, and recovery architecture | Resilience design and test plan |
| 6 | Research design, evidence, and reproducibility | Proposal and source review |
| 7 | Privacy, governance, and stakeholder conflict | Structured dilemma or impact analysis |
| 8 | Emerging topic evaluation | Evidence maturity and adoption recommendation |
| 9 | Project execution and peer review | Draft artifact and review response |
| 10 | Defense, transfer, and maintenance | Final artifact, briefing, and continuation package |

Graduate Assessment Model

- Architecture and source critiques: 20%
- Research or design proposal: 15%
- Technical or policy artifact: 30%
- Oral defense and stakeholder briefing: 15%
- Peer-review quality and revision record: 10%
- Reproducibility, transfer, and maintenance package: 10%

## E.3 Professional Short-Course Outline: Cyber Risk Decisions for Busy Professionals

Length: Eight sessions of sixty to ninety minutes Audience: Managers, project leaders, auditors, educators, and professionals who influence security decisions but do not require deep tool training Course purpose: Improve risk, governance, communication, and response decisions using realistic scenarios.

| Session | Focus | Practical product |
|---|---|---|
| 1 | What cybersecurity risk means to the mission | Asset and dependency map |
| 2 | Identity, access, and account lifecycle | Access-review questions |
| 3 | Social engineering, verification, and reporting | Communication and escalation plan |
| 4 | Cloud, vendors, software, and shared responsibility | Supplier-risk checklist |
| 5 | Incident priorities and executive decisions | Tabletop decision log |
| 6 | Privacy, legal obligations, and ethical tradeoffs | Stakeholder impact map |
| 7 | Metrics, evidence, and misleading certainty | Executive dashboard critique |
| 8 | Improvement plan and continuing governance | Ninety-day action plan |

Short-Course Assessment

Use completion evidence, scenario decisions, briefing quality, and the final action plan. Avoid high-stakes testing that rewards terminology recall without improving workplace decisions.

## E.4 Syllabus Checklist

Identity and Purpose

- [ ] Course title, audience, prerequisites, and delivery mode are accurate.
- [ ] The course purpose describes capability rather than broad topic exposure.
- [ ] Learning outcomes are measurable and limited to what the course can reasonably achieve.

Learning and Assessment

- [ ] Each major outcome has planned evidence.
- [ ] Grading weights match the importance of outcomes.
- [ ] Practical activities include documentation and debriefing.
- [ ] Late, revision, collaboration, and academic-integrity expectations are explicit.
- [ ] AI-use expectations distinguish permitted assistance, required disclosure, prohibited substitution, and verification duties.

Safety, Privacy, and Access

- [ ] Authorization and prohibited activities are stated.
- [ ] Learners know how to report mistakes, unsafe conditions, or suspected incidents.
- [ ] Required accounts, software, hardware, bandwidth, and costs are disclosed.
- [ ] Accessibility and accommodation processes are stated.
- [ ] Data handling, screenshots, recordings, and use of employer or personal information are controlled.

Course Operation

- [ ] Schedule includes preparation, practice, feedback, and recovery time.
- [ ] Contact methods, response expectations, office hours, and support paths are clear.
- [ ] Volatile modules and named tools can be replaced without rewriting the entire course.
- [ ] Version, release date, source date, and next review are recorded.

## E.5 Modular Schedule Template

| Module ID | |
|---|---|
| Outcome | _____ |
| Enduring concept | _____ |
| Replaceable example or tool | _____ |
| Practice | _____ |
| Assessment | _____ |
| Accessibility alternative | _____ |
| Source/review date | _____ |

Vertical planning form

### Source and use

The Complete Cybersecurity Educator, Dr. Jason Edwards. Online public appendices - Appendix E.

Sharing and reuse: Please do not resell this resource. You may repost or share it with other educators. Please leave the Bare Metal Cyber Educators Hub URL below intact. Use fictional or appropriately authorized data where applicable.

Read online: https://educate.baremetalcyber.com/resources/course-models/