CYBER READY CLINIC®
ASSESS.PRACTICE.APPLY

★ PRACTITIONER PROGRAM

CYBER READY CLINIC

Practitioner Program Course Outline

A 10-week, intern-staffed clinical experience — built on the law-school and medical-school clinic model. Structured weekly instruction paired with live client engagements under expert supervision, designed for direct adaptation into a **16-week undergraduate semester**.

BUILT AROUND CRC'S ASSESSMENT FRAMEWORKS

Discover5	Ready5	Digital Wellness	Ready10 Preview
NIST CSF	NICE Framework	DoD 8140	CIS 18

PREPARED BY
John Bruns, CEO — Cyber Ready Clinic

PROGRAM TRACK
10-Week Cohort · 16-Week Semester Mapping

HOW THE PROGRAM WORKS

A clinic model for cybersecurity practice.

The CRC Practitioner Program is a **10-week, intern-staffed clinical experience** modeled on the law- and medical-school clinic concept: structured weekly instruction paired with live client engagements under expert supervision. Interns deliver free cybersecurity assessments to small-to-medium nonprofits while building the practical, framework-aligned skills employers expect of entry-level cyber talent.

01

Learn

Two hours of synchronous instruction each week building cumulatively from foundations to frameworks to enterprise context.

02

Practice

Three live client engagements — Discover5, Ready5, and Digital Wellness close-out — alongside expert practitioners under NDA.

03

Apply

Capstone project, proficiency exam, and digital badge issuance — portable, verifiable proof of clinical work performed.

WHAT EVERY COHORT DELIVERS

Program format at a glance

Duration

10 instructional weeks (intern program); 16 weeks (proposed academic semester).

Contact Time

2 hours per week of synchronous instruction; client meetings scheduled outside the block.

Cohort Size

Typically 15–20 interns per cohort; mentor pairing at intake.

Delivery

Hybrid: virtual lecture and discussion plus in-person or virtual client engagements.

Assessment Frameworks

CRC Discover5 (business risk) and CRC Ready5 (cyber capabilities) drive the curriculum.

Standards Mapped

NIST CSF, NIST 800-53, CIS 18, NICE Workforce Framework, and DoD 8140.

Confidentiality

All client work is performed under a mutual NDA executed at intake; client-identifying material never leaves NDA-controlled channels.

Real clients, mentored practice, portable evidence

Every cohort delivers free assessments to small-to-medium nonprofits — interns leave with documented work, a verifiable digital badge, and a portfolio that respects client confidentiality.

WHAT EVERY STUDENT LEAVES WITH

Program learning outcomes.

On successful completion, students will be able to perform the full assessment arc — from business-risk discovery through capability evaluation to customer-facing close-out — mapped to recognized cybersecurity workforce standards.

ASSESSMENT & REPORTING

- Conduct a structured business-risk assessment using the CRC **Discover5** framework across personnel, finances, operations, IT support, and risk management.
- Evaluate cybersecurity capabilities using the CRC **Ready5** framework across endpoint, identity, email, edge, and response, mapping findings to NIST CSF.
- Produce a customer-ready **Digital Wellness Report** that synthesizes findings into prioritized, criticality-scored recommendations.
- Communicate technical findings to non-technical stakeholders in writing and in live customer meetings.

INDUSTRY & WORKFORCE CONTEXT

- Interpret threat-intelligence and claims data (Verizon DBIR, NetDiligence) to justify control selection for SME-sized organizations.
- Distinguish workforce roles and certification pathways using the **NICE Framework** and **DoD 8140** mappings.
- Articulate enterprise cybersecurity program components — tools, processes, structure, budgets, metrics — and how they differ by organization size.
- Evaluate cybersecurity products and vendors critically: product-market fit, consolidation, procurement, and how to see through marketing claims.
- Demonstrate professional conduct under NDA, including handling of customer data and incident-response escalation protocols.

RECOMMENDED WEIGHTING

Graded components

COMPONENT	DESCRIPTION	WEIGHT
Weekly Reflections	Up to 10 written reflections submitted to the course portal after each instructional session.	**15%**
Client Meeting Participation	Attendance and role in three live client meetings: Discover5, Ready5, and Digital Wellness close-out.	**20%**
Capstone Project	Student-selected applied project benefiting a CRC client, the clinic, or the broader cyber workforce.	**30%**
Proficiency Exam	Written plus practical exam covering Discover5, Ready5, threat data, workforce framework, and enterprise concepts.	**20%**
Participation & Professionalism	Cameras-on, on-time attendance, NDA adherence, and substantive mentor engagement.	**15%**

TEN WEEKS. ONE ARC.

From foundations to capstone.

Modules build cumulatively: foundations and frameworks first, then enterprise program and product context, then live client engagement, and finally synthesis and career preparation. Three required client meetings span Weeks 3–10.

FOUNDATION

Wk 1 · Clinic Foundations

Wk 2 · Discover5: Business Risk

CAPABILITY FRAMEWORKS

Wk 3 · Ready5 I: Endpoint & Identity

Wk 4 · Ready5 II: Email, Edge & Response

INDUSTRY & ENGAGEMENT

Wk 5 · The Cyber Workforce

Wk 6 · Applied Client Practice

PROGRAM & PRODUCT CONTEXT

Wk 7 · Enterprise Cyber Programs

Wk 8 · Cyber Products & SaaS

SYNTHESIS & CAPSTONE

Wk 9 · Capstone & Exam Prep + Ready10 Preview
Career narrative, advanced concepts

PROGRAM CLOSE

Wk 10 · Capstone Presentations & Close
Practical proficiency exam, badge issuance

WEEK	MODULE	CORE THEME	MAPS TO
1	**Clinic Foundations**	The clinic model, mission, ecosystem, and program mechanics.	NIST CSF · NICE
2	**Discover5: Business Risk**	Understand the organization before assessing the technology.	NIST CSF · CIS 18
3	**Ready5 I: Endpoint & Identity**	Lock down the workforce — devices and credentials.	NIST CSF Protect
4	**Ready5 II: Email, Edge & Response**	Stop the inbound, control the outbound, recover what gets through.	Detect/Respond/Recover
5	**The Cyber Workforce**	Locate yourself on a 160+ role map; choose a credible next step.	NICE · DoD 8140
6	**Applied Client Practice**	Run the full Discover5 → Ready5 → Digital Wellness arc.	NIST CSF · NICE
7	**Enterprise Cyber Programs**	From individual controls to a coherent, fundable program.	NIST CSF · 800-53
8	**Cyber Products & SaaS**	How the industry builds and sells — and how to buy without getting burned.	Procurement · TCO
9	**Capstone Prep + Ready10**	Convert clinical experience into a portfolio and credible job search.	NICE · Career
10	**Capstone & Close**	Capstone presentations, practical exam, transition to alumni.	Practical Exam

WEEK 1 · FOUNDATION

Clinic Foundations

01

Orient students to the clinic model, the CRC mission, and the program mechanics.

KEY TOPICS

- CRC origin, mission, vision, and 501(c)(3) structure
- The three challenges CRC addresses: workforce shortage, awareness gaps, defensive capability gaps
- Customer Process: Discover5 → Ready5 → Digital Wellness → Practice → CISO Advisory
- The CRC ecosystem: client, education, employment, funding, and service partners
- Cohort introductions, mentor pairing, and confidentiality expectations under the NDA

LEARNING OBJECTIVES

- Describe the clinic model and articulate why localized trust matters in cyber service delivery
- Identify the five stages of the CRC Customer Process and what each delivers to the client
- Demonstrate understanding of the NDA, communications expectations, and reflection requirements

ACTIVITIES & ASSIGNMENTS

- In-session: Cohort introductions and mentor matching
- Out-of-session: Sign program NDA; sign up for first client meeting; submit Week 1 reflection

SOURCE FRAMEWORKS

CRC Customer Process

MAPS TO OUTCOMES

Professional Conduct & NDA

WEEK 2 · FOUNDATION

Discover5: Business Risk Assessment

02

Understand the organization before assessing the technology.

KEY TOPICS

- The Discover5 framework: Personnel, Finances, Operations, IT Support, Risk Management
- Financial risk: revenue, IT spend benchmarks (3–4% of revenue, lower for nonprofits), MSP spend, planned investments
- Operational risk: critical business systems, data storage, website attack surface
- Service models & standards: MSP vs. MSSP vs. SOC; audits vs. assessments vs. compliance; voluntary frameworks vs. regulatory mandates
- Cyber insurance fundamentals and the business-level incident response process

LEARNING OBJECTIVES

- Identify the five Discover5 domains and the sub-elements within each
- Differentiate an MSP from an MSSP and explain why this matters for SMEs
- Distinguish audits, assessments, and compliance; select the right framework for a context
- Explain how cyber insurance fits into incident response beyond loss reimbursement

ACTIVITIES & ASSIGNMENTS

- In-session: Case discussion — serving a 10-employee local business with no IT-savvy staff
- Out-of-session: Submit Week 2 reflection; review Ready5 pre-read; confirm client meeting attendance

SOURCE FRAMEWORK

CRC Discover5

MAPS TO OUTCOMES

Business Risk Assessment

WEEK 3 · CAPABILITY FRAMEWORKS

Ready5 I: Endpoint & Identity

03

Lock down the workforce — the devices people use and the credentials they use to log in.

KEY TOPICS

- The full Ready5 framework introduction and the SME attack chain across all five domains
- Endpoint deep-dive: legacy AV vs. next-gen AV vs. EDR vs. XDR; 24/7 MDR and SOC monitoring (in-house vs. MSSP vs. MDR-as-a-service)
- Identity deep-dive: identity providers (Entra, Google Workspace, Okta, Duo) as the new perimeter
- MFA strength tiers: SMS vs. TOTP vs. push vs. FIDO2/passkeys; bypass and fatigue attacks
- Conditional access and privileged access management fundamentals
- Threat-data grounding: 2025 Verizon DBIR — ransomware in 44% of breaches, 88% of SMB breaches

LEARNING OBJECTIVES

- Distinguish AV, EDR, MDR, and XDR — and explain the right combinations by org scale
- Map endpoint and identity controls to specific steps in a ransomware or credential-abuse attack chain
- Justify FIDO2/passkey-based MFA over SMS using DBIR data on credential abuse
- Explain why the IdP has replaced the network perimeter as the primary SME control plane

ACTIVITIES & ASSIGNMENTS

- In-session: School-system ransomware story — propose which control would have changed the outcome
- In-session: IdP comparison — Entra vs. Google Workspace vs. Okta for a 25-person nonprofit
- Out-of-session: Submit Week 3 reflection; sign up for Discover5 meeting if not yet attended

SOURCE FRAMEWORK
CRC Ready5 (Endpoint, Identity)

THREAT GROUNDING
Verizon DBIR 2025

WEEK 4 · CAPABILITY FRAMEWORKS

Ready5 II: Email, Edge & Response

04

Stop the inbound, control the outbound, and recover when something gets through.

KEY TOPICS

- Email capabilities: secure email gateways, native M365/Workspace protections, safe links and attachments
- Email authentication: SPF, DKIM, DMARC — what each does and why “p=none” is not protection
- Business email compromise and payment fraud: why BEC produces higher claims frequency than ransomware
- Edge capabilities & segmentation: web protection, DNS filtering, SWG; guest Wi-Fi, IoT separation, VPN vs. ZTNA
- Response: server, endpoint, SaaS, and website backup; immutable/offline copies; restore-tested vs. backup-tested
- Threat-data grounding: NetDiligence 2025 — avg SME incident $264K, with business interruption $1.8M

LEARNING OBJECTIVES

- Explain DMARC alignment and why “p=none” is not protection
- Differentiate ransomware-driven loss from BEC-driven loss using NetDiligence claims data
- Justify why SaaS backup (M365/Workspace) is a separate purchase from server/endpoint backup
- Articulate the full Ready5 capability picture in a single narrative covering an end-to-end SME attack

ACTIVITIES & ASSIGNMENTS

- In-session: BEC scenario walkthrough — vendor invoice swap; identify email, identity, and process controls
- In-session: Backup posture exercise — design backup for a 30-seat nonprofit on M365 with one on-prem server
- Out-of-session: Submit Week 4 reflection; review the sample Digital Wellness Report

SOURCE FRAMEWORK
CRC Ready5 (Email, Edge, Response)

THREAT GROUNDING
NetDiligence 2025

WEEK 5 · INDUSTRY & ENGAGEMENT

The Cybersecurity Workforce

05

Locate yourself on a 160+ role map and choose a credible next step.

KEY TOPICS

- Enterprise cyber program structure: Engineering, Cyber Services, GRC, IR, Operations, Resilience
- SecOps budget allocation: how a $50–100M program differs from a $1–5M mid-market program
- The Datacare Workforce map: 160+ cyber roles across leadership, engineering, GRC, IR, ops, offensive, DevOps, data, identity
- Cyber roles needed during a ransomware response, from identification through after-action; Forensic Analyst deep-dive (ELK, Axiom, EnCase, FTK)
- DoD 8140 mapping to NIST work roles and required industry certifications; HR-construct vs. genuine prerequisite
- Certification roadmap: A+/ITF+ → Network+/Security+ → CySA+/CISA → CISSP/CISM

LEARNING OBJECTIVES

- Identify at least three cyber roles aligned with the student's interests and skill profile
- Read a job posting and distinguish HR-construct requirements from substantive prerequisites
- Select a defensible certification pathway for the student's current career stage

ACTIVITIES & ASSIGNMENTS

- In-session: Each student presents one role from the Datacare Workforce map they want to learn more about
- Out-of-session: Submit top three target cyber jobs to mentor by end of Week 7; schedule 15-min mentor 1:1

SOURCE FRAMEWORKS

NICE · DoD 8140 · Datacare Workforce Map

MAPS TO OUTCOMES

Workforce & Career Pathways

WEEK 6 · INDUSTRY & ENGAGEMENT

Applied Client Practice

06

Run the full Discover5 → Ready5 → Digital Wellness arc in live engagements with real clients.

KEY TOPICS

- Capstone scoping & mind-mapping kickoff: client-, clinic-, and workforce-benefiting projects
- Conducting a Discover5 interview: open questions, follow-ups, capturing details accurately
- Conducting a Ready5 interview: calibrating technical depth, distinguishing in-place from configured-well
- Delivering the Digital Wellness close-out: leading with strengths, framing risks, handling pushback
- Connecting findings to next-step services: remediation, framework alignment, Ready10/Ready15 referrals
- Note-taking, evidence handling, and confidentiality during a live engagement; post-meeting report drafting

LEARNING OBJECTIVES

- Scope a capstone with a defined deliverable, audience, and success measure for mentor approval
- Conduct structured Discover5 and Ready5 interviews alongside a senior practitioner
- Score capability findings against the Ready5 rubric and justify the scores
- Deliver a portion of a Digital Wellness close-out to a real client under supervision

ACTIVITIES & ASSIGNMENTS

- Attend at least three live client meetings: one Discover5, one Ready5, one Digital Wellness close-out
- Submit meeting notes per the standard template within 48 hours of each engagement
- Submit capstone scope document for mentor approval by end of Week 9; submit Week 6 reflection

ENGAGEMENT TYPE

Live, NDA-controlled, mentor-supervised

MAPS TO OUTCOMES

Customer Engagement & Reporting

WEEK 7 · PROGRAM & PRODUCT CONTEXT

Building an Enterprise Cyber Program

07

From individual controls to a coherent program your organization can fund, staff, and operate.

KEY TOPICS

- What a cyber "program" actually is: people, processes, and technology aligned to risk — not a collection of tools
- Program structure across SME, mid-market, and enterprise: Engineering, Cyber Ops (SOC/IR), GRC, IAM, Resilience, Offensive Security
- Governance, reporting lines, and Board oversight; budget benchmarks (cyber as 8–15% of IT spend); build vs. buy vs. outsource
- The stack: SIEM/SOAR/XDR, EDR, IAM/PAM, exposure mgmt, GRC, DLP, CASB, email, NDR — what's required vs. nice-to-have at each scale
- NIST CSF as operating backbone; policy → standard → procedure architecture; 0-12-36 month roadmaps tied to risk reduction
- Metrics that matter (MTTD, MTTR, patch latency, control coverage) and how to present cyber risk to executives and the Board

LEARNING OBJECTIVES

- Describe how a cybersecurity program scales at SME, mid-market, and enterprise levels
- Construct a defensible line-item cybersecurity budget using IT-spend and revenue benchmarks
- Distinguish vanity from decision-quality metrics; propose a four-metric Board dashboard
- Explain how NIST CSF can serve as a program's operating backbone, not just an audit framework

ACTIVITIES & ASSIGNMENTS

- In-session: Program-design exercise — org, budget, and 12-month roadmap for a 200-person org
- In-session: Board-deck dry-run — 2-minute cyber-risk update to a mock audit committee
- Out-of-session: Submit Week 7 reflection; bring one published board-level cyber report for Week 8

SOURCE FRAMEWORKS

NIST CSF · NIST 800-53 · CIS 18

MAPS TO OUTCOMES

Enterprise Program Design

WEEK 8 · PROGRAM & PRODUCT CONTEXT

Cyber Product Development & the SaaS Marketplace

08

How the cybersecurity industry actually builds and sells — and how to buy without getting burned.

KEY TOPICS

- Anatomy of a cyber SaaS company: product, engineering, GTM, customer success, and the channel (MSP/MSSP/VAR)
- Product-market fit and ICP: how vendors define the Ideal Customer Profile; the cost of being outside it
- Categories & consolidation: endpoint, identity, network, email, cloud, GRC, exposure; XDR vs. SIEM+EDR+SOAR; platforms vs. best-of-breed
- Emerging tech: AI-SOC, CTEM, ITDR, ASPM/CNAPP, agentic and MCP-driven workflows — real innovation vs. rebrands
- Procurement & the sales motion: RFI/RFP vs. direct; PoCs with pass/fail criteria; TCO including operational overhead; BANT/MEDDIC from the buyer side
- Seeing through marketing: MITRE ATT&CK Evals, AV-Comparatives, SE Labs, analyst reports; vendor evaluation rubric (capability fit, lock-in, exit costs)

LEARNING OBJECTIVES

- Describe how a cyber SaaS company is organized and how each function influences the buyer experience
- Critically evaluate a vendor pitch — separate substantive capability claims from marketing language
- Design a structured PoC for a security tool: pass/fail criteria, scope, timeline, decision authority
- Articulate the platform-vs-best-of-breed tradeoff using two competing product categories

ACTIVITIES & ASSIGNMENTS

- In-session: Vendor pitch teardown — rewrite EDR/SIEM one-pager claims as testable PoC criteria
- In-session: Consolidation debate — platform vs. best-of-breed for a 500-person mid-market org
- Out-of-session: Submit Week 8 reflection; capstone proposal due to mentor

INDUSTRY LENSES

Gartner MQ · Forrester Wave · MITRE Evals

MAPS TO OUTCOMES

Vendor & Procurement Critique

WEEK 9 · SYNTHESIS

Capstone & Exam Prep + Ready10 Preview

09

Convert clinical experience into a portfolio and a credible job-search narrative.

KEY TOPICS

- Full proficiency exam review and live study session
- Review all client meetings to-date and discuss lessons learned
- Review capstone projects that create an output or artifact — publishable, demoable, or operationally useful
- Resume and LinkedIn translation of clinic work without breaching NDA
- Continuing involvement post-internship: employer engagement, certification roadmaps, alumni participation
- Ready10 preview: ITDR, CAASM, CI/CD pipeline security (SAST, DAST), Exposure Management, NDR, insider/APT detection

LEARNING OBJECTIVES

- Produce a portfolio-ready description of clinic work that respects confidentiality boundaries
- Articulate at least two success stories grounded in real client engagement
- Build a future roadmap to career success

ACTIVITIES & ASSIGNMENTS

- Capstone work session; resume and LinkedIn review with mentor
- Submit Week 9 reflection; sit for proficiency exam (written portion) at end of week

LOOKING AHEAD

Ready10 Advanced Concepts

MAPS TO OUTCOMES

Career Portfolio & Pathway

WEEK 10 · PROGRAM CLOSE

Capstone Presentations & Program Close

10

Present capstone work; complete the proficiency exam; transition to alumni status.

KEY TOPICS

- Capstone presentations to cohort, mentors, and (where appropriate) the client or stakeholder
- Proficiency exam practical portion: live walkthrough of a mock Discover5 or Ready5 scenario
- Program retrospective: what worked, what to change, recommendations to the next cohort
- Alumni pathway: continuing engagement, mentor reciprocity, employer introductions, badge issuance

LEARNING OBJECTIVES

- Present a capstone artifact to a mixed technical and non-technical audience
- Demonstrate end-to-end proficiency across Discover5, Ready5, Digital Wellness, and program/product concepts

ACTIVITIES & ASSIGNMENTS

- Deliver capstone presentation
- Complete proficiency exam (practical portion)
- Complete program retrospective during the session

OUTCOME

Verifiable Digital Badge Issued

MAPS TO OUTCOMES

End-to-End Practitioner Proficiency

REQUIRED FOR COMPLETION

Live work, real clients, real evidence.

Lecture explains the frameworks. The clinic experience is what makes graduates credible to employers. Four required components ensure every practitioner leaves with documented, supervised work product.

01

Client Meetings (×3)

One Discover5, one Ready5, one Digital Wellness close-out — live, NDA-controlled, mentor-supervised.

02

Capstone Project

One project benefiting a CRC client, the clinic, or the workforce — scoped by Week 9, presented in Week 10.

03

Proficiency Exam

Two-part: scenario-based written exam in Week 9, practical walkthrough of a mock Discover5/Ready5 in Week 10.

CLIENT MEETING	PURPOSE	TYPICAL WEEK
Discover5 Business Risk	Live intake interview covering Personnel, Finances, Operations, IT Support, and Risk Management.	Weeks 3–8
Ready5 Cyber Capabilities	Live capability interview with the client's IT team or MSP across Endpoint, Identity, Email, Edge, Response.	Weeks 5–10
Digital Wellness Close-Out	Live delivery of findings and prioritized recommendations to client leadership.	Weeks 7–10

CAPSTONE CATEGORIES

- **Client-benefiting** — a tailored remediation plan or tooling proof-of-concept for a CRC client.
- **Clinic-benefiting** — training assets, intake automations, or mentor resources.
- **Workforce-benefiting** — curriculum modules, outreach campaigns, or community partnerships.

WEEKLY REFLECTIONS

- Short written reflections after each session in Weeks 1–7, submitted to the program portal.
- Weeks 8–10 focus on capstone creation, presentation, and program close — no separate reflection required.
- Prompts connect content to prior coursework, current events, or target role — engagement and synthesis over correctness.

ADAPTING TO A 16-WEEK SEMESTER

From cohort to classroom.

The CRC curriculum occupies 10 of the 16 academic weeks. The remaining five weeks support onboarding, prerequisite refresh, employer engagement, and academic synthesis — preserving the clinical experience while satisfying standard undergraduate course-design requirements.

SEM WEEK	ACTIVITY	OWNER
1	Academic course onboarding: syllabus, learning outcomes, academic-integrity expectations, pre-assessment.	Faculty
2	Cyber fundamentals refresher and prerequisite check (networking, OS basics, productivity-suite literacy).	Faculty
3–12	CRC Practitioner Program Weeks 1–10 (this outline).	CRC
13	Capstone showcase open to faculty and CRC staff under NDA controls; proficiency-exam review; badge awarding.	CRC + Faculty
14–15	Employer panel and/or industry guest speakers from the local partner network; capstone polish and peer review.	Faculty
15–16	Academic synthesis: written paper connecting clinical experience to a chosen framework (NIST CSF, NICE, enterprise-program design, or DBIR analysis).	Faculty

RECOMMENDED PREREQUISITES

- Introductory networking or systems administration (CompTIA Network+ or equivalent comfort).
- Introductory security (CompTIA Security+ topics or equivalent) — strongly recommended, not strictly required.
- Professional comfort with Microsoft 365 and/or Google Workspace, plus basic data analysis.

STANDARDS & FRAMEWORK ALIGNMENT

- **NIST CSF** — Identify, Protect, Detect, Respond, Recover all addressed across Discover5, Ready5, and Week 7.
- **NICE Workforce Framework** — explicit instruction in Week 5; capstones can be scoped to specific work roles.
- **DoD 8140** — explicit instruction in Week 5 including industry-certification mappings.
- **CAE Knowledge Units** — risk management, policy, governance, IR, network defense, security program management.

Pilot first, then scale

CRC recommends piloting the course with a small cohort (10–15 students) in a single semester before scaling. The clinic supports faculty co-delivery scope, NDA alignment, and academic-record practices during program setup.

CYBER READY CLINIC®
ASSESS.PRACTICE.APPLY

★ BUILD THE PROGRAM WITH US

FOR FACULTY PARTNERS

A clinic experience, on your semester.

The Practitioner Program is delivered in partnership: CRC supplies the curriculum, the assessment frameworks, the real clients, and mentor-led supervision. The institution supplies academic structure, prerequisites, and credit-bearing assessment. The result is a clinical experience that maps cleanly to your program-level outcomes.

SUGGESTED NEXT STEPS

- ✓ Review this outline and identify modifications for institutional fit (course numbering, credit hours, prerequisites).
- ✓ Schedule a working session with CRC to walk through Weeks 1–10 in detail and confirm faculty co-delivery scope.
- ✓ Request reflection prompts and prior-cohort capstone brainstorms as supplementary appendices.
- ✓ Confirm institutional NDA and data-handling controls for student work involving real client engagements.

CRC

Cyber Ready Clinic — 501(c)(3) Nonprofit

Build the academic partnership with us

John Bruns
Chief Executive Officer
john@cyberreadyclinic.com

Tim Glinka
Director of Strategic Partnerships
tim@cyberreadyclinic.com

Web www.cyberreadyclinic.org