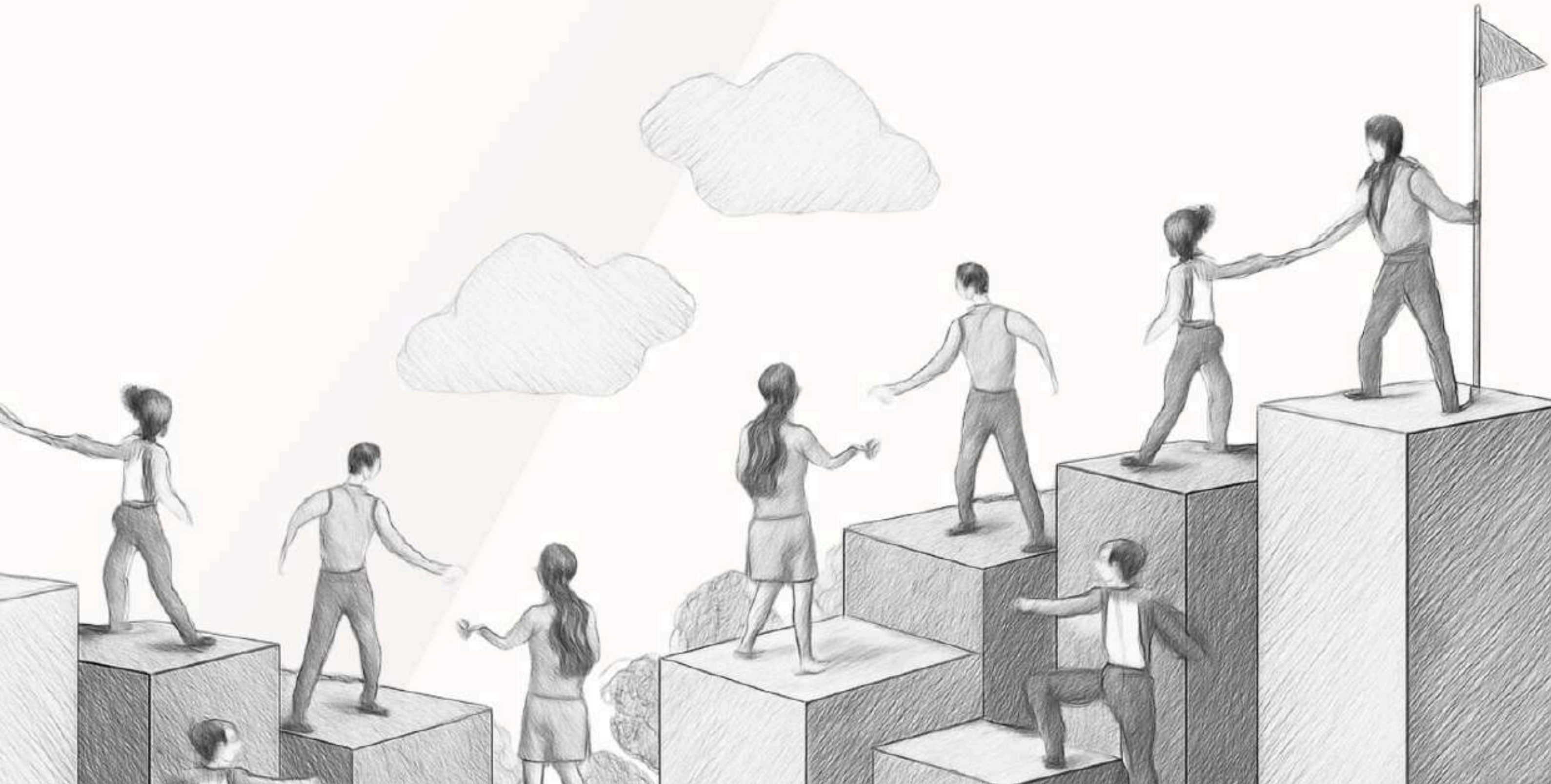
Capacity Development Roadmap for UP CSIRT

Prepared by the UP Office of the Vice President for Digital Transformation

This is an open document and maintained at links.up.edu.ph/csirtroadmap.
Feedback is most welcome.



Capacity Development Roadmap for UP CSIRT

Prepared by the UP Office of the Vice President for Digital Transformation

Version:
[OVPDxRoadmaps001] Capacity Development Roadmap for UP CSIRT_v01_11282025

As of 28 November 2025

Preface

Cybersecurity threatens institutional survival.

In 2024, cyberattacks hit 80% of Philippine organizations. Universities accounted for 13% of incidents (DICT, 2024a). When systems crashed, the recovery cost for Philippine organizations reached hundreds of millions.

This **Capacity Development Roadmap for UP CSIRT** (University of the Philippines Computer Security Incident Response Team) costs a fraction of what incident recovery demands.

Better still, it works—modular steps you implement in any order your budget allows. No fantasy scenarios. No assumptions of unlimited money or staff.

How This Works

Eight independent steps:

Basics → Practice → Tools → Certifications → Governance → Specializations → Infrastructure → Community

Weak governance but strong technically? Start with Step 5. Strong policies but unprepared for actual incidents? Jump to Step 2.

Your organization. Your priorities. Your pace.

Timeline

Year 1: Achieve operational capability.

Year 2: Master detection.

Year 3: Set the benchmark.

This builds infrastructure, not a project.

Without incident response capability, universities lose research data, leak student records, crash during enrollment, and forfeit international partnerships.

For HR and CSIRT People

HR challenge: Private sector pays ₱60K-150K monthly for experienced cybersecurity staff. While we cannot match that, we can offer: clear career paths, real training budgets, and reasonable on-call schedules (Cabato, 2024).

CSIRT professionals: Your roadmap runs pages 7-44. Four competency levels (L1-L4). Five specialization tracks.

Living Document

Threats evolve. Technology shifts. This roadmap demands periodic revision—annually at minimum, or immediately when major threats emerge or capabilities change. Let's build *review* into our governance cycle.

What worked in 2025 may fail in 2027. Plan to update and improve it continuously..

This roadmap is more than a guide. It is an investment in the continued trust, stability, and mission-critical functionality of the entire University system. Its successful implementation is paramount to securing and fortifying the future of the University in the digital era.

Peter Sy

PETER A. SY

Vice President for Digital Transformation
University of the Philippines

Contents

2 *Preface*

5 *Understanding This Roadmap: Modularity and Flexibility*

6 *The Philippine Context Demands Urgency*

7 *Overview: Steps 1-8*

- ➢ Step 1: Master Cybersecurity Basics—Building Organizational Foundation
- ➢ Step 2: Hands-On Practice—Progressive Exercise
- ➢ Step 3: Learn Security Tools—Integrated Architecture
- ➢ Step 4: Get Entry-Level Certifications—Portfolio
- ➢ Step 5: Learn GRC (Governance, Risk & Compliance)—Philippine Context
- ➢ Step 6: Dive Into Specialized Areas—Building T-Shaped
- ➢ Step 7: Build Infrastructure—Modular Deployment
- ➢ Step 8: Join Communities and Stay Updated—Structured

37 *Complete Three-Year Budget Summary*

39 *Three-Year Implementation Timeline: Modular Progression*

42 *Competency Matrix: Team Skill Progression*

43 *Conclusion: Modular, Scalable, Achievable*

44 *References*

Understanding This Roadmap: Modularity and Flexibility

🔧 **MODULAR DESIGN:** ***Each step functions independently.*** Start wherever your team's current capabilities suggest. A team with strong technical skills but weak governance might prioritize Step 5 (GRC) before Step 3 (Tools). Another team with excellent policies but limited hands-on experience should emphasize Step 2 (Practice) immediately.

📊 **LEARNING MODES:**

- 👤 **Self-Learning:** Individual study, certification preparation, personal skill development
- 👥 **Team-Learning:** Collaborative exercises, group training, coordinated capability building

💰 **COST INDICATORS (Philippine Peso basis, ₱58.92 = $1 USD):**

- 🆓 **FREE:** No cost resources (may require registration)
- 🌐 **OPEN SOURCE:** Free software requiring technical deployment/maintenance
- 💵 **LOW COST:** ₱56-28,000 per person annually
- 💰 **MODERATE COST:** ₱28,001-112,000 per person annually
- 💳 **PREMIUM COST:** ₱112,001+ per person annually

🎯 **SKILL LEVELS:** Each competency progresses through four levels:

- **L1 - Foundation:** Awareness and basic understanding
- **L2 - Practitioner:** Hands-on capability with guidance
- **L3 - Advanced:** Independent complex work
- **L4 - Expert:** Leads others, innovates, teaches

The Philippine Context Demands Urgency

The threat landscape confronting UP is both severe and accelerating. Philippine organizations experienced a dramatic surge in cyberattacks during 2024, with 80% suffering an average of three breaches (Cyberint, 2024). **The academic sector accounts for 13% of all incidents reported to the National Computer Emergency Response Team (NCERT)**, second only to emergency response agencies (Department of Information and Communications Technology [DICT], 2024a). Malware dominates at 48.9% of incidents—particularly infostealers harvesting credentials from personal devices used for work—followed by sophisticated smishing campaigns employing IMSI-catchers during holidays, DDoS attacks during enrollment periods, and persistent phishing targeting university credentials (Cyberint, 2024).

The regulatory environment has matured substantially. President Marcos Jr. adopted the National Cybersecurity Plan (NCSP) 2023-2028 via Executive Order 58, mandating that universities establish organizational CERTs, participate in the national CERT network, and implement structured incident response capabilities (Presidential Communications Office, 2024). Compliance with the Data Privacy Act of 2012 (Republic Act 10173) requires 72-hour breach notification to the National Privacy Commission and comprehensive security incident management (National Privacy Commission, 2012). These are not optional initiatives—they represent legal obligations carrying substantial penalties.

Yet opportunity accompanies obligation. The DICT offers free training partnerships with CISCO, Oracle, and Microsoft for certifications, including CISSP, CEH, and CISA (Philippine News Agency, 2022). The UP-CIFAL Philippines Professional Course on Digital Governance and Cybersecurity, established through a partnership with DICT's Cybersecurity Investigation and Coordinating Center in 2020, demonstrates UP's existing leadership position (University of the Philippines-CIFAL Philippines, 2021). We must now operationalize this expertise into a formal CSIRT serving our entire university system.

Overview: Steps 1-8

This modular roadmap provides a flexible, three-year framework for building world-class cybersecurity incident response capability at the University of the Philippines.

Step 1 - Master Cybersecurity Basics: Establishes foundational knowledge through free online courses (CISA, SANS, Google) and essential reading of NIST guidelines and Philippine regulations. Includes team workshops for mandate development, stakeholder mapping, and baseline maturity assessment.

Step 2 - Hands-On Practice: Develops practical skills through progressive tabletop exercises using free CISA scenarios and cyber range training on platforms like TryHackMe. Builds internal facilitation capability (EXCON) to reduce dependence on expensive external consultants.

Step 3 - Learn Security Tools: Deploys integrated security architecture starting with free Splunk Enterprise SIEM through Academic Alliance, plus open-source tools for network monitoring (Suricata, Zeek), endpoint detection (Wazuh), and digital forensics. Creates comprehensive detection and response capability using primarily free or low-cost solutions.

Step 4 - Get Entry-Level Certifications: Implements role-based certification tracks from entry-level (ISC2 CC, CompTIA Security+) to practitioner (CySA+, ECIH) to advanced (GIAC, CISSP) levels. Provides cost optimization strategies and three-year deployment timeline with budgets ranging from ₱97K-1M per approach.

Step 5 - Learn GRC (Governance, Risk & Compliance): Ensures deep understanding of Philippine legal requirements (Data Privacy Act, Cybercrime Prevention Act, NCSP 2023-2028) through free training resources. Integrates international frameworks (ISO 27035, NIST CSF 2.0, FIRST) and establishes quarterly risk assessment processes.

Step 6 - Dive Into Specialized Areas: Builds T-shaped teams where all members have baseline competency across domains but develop expert-level skills in one of five tracks: SOC Analysis, Incident Response, Digital Forensics, Vulnerability Management, or Threat Intelligence. Includes UP-specific research security specialization addressing unique academic requirements.

Step 7 - Build Infrastructure: Deploys security infrastructure in four modular phases from minimal viable operations (SIEM, ticketing, forensics workstations) to advanced capabilities (SOAR automation, malware sandboxes, threat intelligence platforms). Offers three cost approaches from all-open-source (₱1.5-2.2M) to comprehensive premium (₱5.6-9M) over three years.

Step 8 - Join Communities and Stay Updated: Establishes mandatory NCERT registration and engagement with Philippine national cybersecurity ecosystem, plus optional regional ASEAN partnerships and international FIRST membership. Creates structured, continuous learning infrastructure through conferences, peer exchanges, and knowledge management practices.

Step 1: Master Cybersecurity Basics—Building Organizational Foundation

Module 1A: Foundational Knowledge (Self-Learning + Team-Learning)

Target Competency: Cybersecurity Fundamentals → L1-L2

Self-Learning Resources

🆓 **FREE Courses:**

- **Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Essentials** (8 hours) - Basic security concepts, threat landscape (CISA, 2025a)
- **SANS SEC275** - Core knowledge and practical skills in computers, technology, and security foundations with hands-on labs (SANS Institute, n.d.-a)
- **Cybrary Introduction to IT and Cybersecurity** (8 hours) - Foundational concepts (Cybrary, n.d.)
- **Google Cybersecurity Professional Certificate** (Coursera) - Comprehensive beginner program (💵 ₱2,744/month or 🆓 with financial aid) (Google, n.d.)

🌐 **OPEN SOURCE Learning:**

- **OWASP Training Materials** - Web application security fundamentals (OWASP Foundation, n.d.)
- **ENISA Training Resources** - 50+ courses on incident response, risk management, CSIRT operations (European Union Agency for Cybersecurity [ENISA], 2020)

📚 **Essential Reading (Self-Study):**

- **NIST SP 800-61r3: Computer Security Incident Handling Guide** (🆓) - The incident response bible (National Institute of Standards and Technology [NIST], 2025)
- **Philippine NCSP 2023-2028** (🆓) - National cybersecurity strategy and requirements (DICT, 2024a)
- **Data Privacy Act of 2012 Implementing Rules** (🆓) - Legal obligations (National Privacy Commission, 2016)

Skill Progression:

Competency Area	L1 Foundation	L2 Practitioner
Threat Landscape	Identify common attack vectors	Explain attacker motivations and TTPs
Defense Strategies	Understand defense-in-depth	Apply layered security controls
Incident Response	Describe IR lifecycle	Follow IR playbooks with guidance
Philippine Context	Know major laws (DPA, Cybercrime Act)	Apply compliance requirements to scenarios

Time Investment: 40-60 hours self-study over 8-12 weeks

Cost per Team Member: ₱0-2,800 (materials, documentation)

Team-Learning Activities

👥 **Facilitated Workshops (Monthly):**

- **Month 1:** Philippine Threat Landscape - DICT threat reports, NCERT advisories, local incident case studies
- **Month 2:** Attack Kill Chain Analysis - Map real breaches to Lockheed Martin kill chain model (Hutchins et al., 2011)
- **Month 3:** Incident Response Fundamentals - NCSP six-stage model walkthrough with Philippine examples (DICT, 2024a)

🆓 **FREE Team Resources:**

- **CISA Incident Response Training Materials** - Facilitator guides, participant handbooks (CISA, 2025a)

- **Forum of Incident Response and Security Teams (FIRST) Technical Colloquia Recordings** - Past presentations on emerging threats and techniques (FIRST, n.d.-a)

Module 1B: Governance Foundation (Team-Learning)

Target Competency: CSIRT Governance → L1-L2

Prerequisites: Executive sponsorship secured, preliminary budget allocated

👥 **Team Activities (Non-Technical):**

1. **Mandate Development Workshop** (8 hours)
    - Define constituency (UP System scope)
    - Establish service catalog (initial)
    - Document authority and escalation paths
    - Reference: Carnegie Mellon SEI CSIRT Handbook (West-Brown et al., 2003)

2. **Stakeholder Mapping Exercise** (4 hours)
    - Identify key stakeholders: Legal, Audit, Compliance, Research, Academic Computing
    - Define communication protocols
    - Establish Cybersecurity Advisory Council

3. **Baseline Maturity Assessment** (8-12 hours)
    - Use Security Incident Management Maturity Model (SIM3) v2 online tool (🆓) at https://sim3-check.opencsirt.org/
    - Document current state across 45 parameters (Open CSIRT Foundation, 2023)
    - Identify priority capability gaps

🆓 **FREE Resources:**

- **ENISA "How to Set-up CSIRT and SOC" Guide** - Comprehensive organizational playbook (ENISA, 2020)
- **FIRST Services Framework** - Standard service definitions (FIRST, 2023)
- **CMU SEI CSIRT Handbook** - Governance best practices (West-Brown et al., 2003)

Deliverable: CSIRT Charter Document, Baseline SIM3 Assessment Report

Cost: ₱0 (internal labor only)

Step 2: Hands-On Practice—Progressive Exercise Program

Module 2A: Tabletop Exercises (Team-Learning)

🆓 **FREE TTX Packages:**

- CISA Tabletop Exercise Packages (100+ scenarios)
- MS-ISAC Tabletop Exercise Package
- SANS Internet Storm Center Cyber Scenarios

Progressive Difficulty:

Month	Scenario Type	Complexity
1	Phishing Campaign	Basic
2	Malware Outbreak	Basic
3	Ransomware Attack	Intermediate
4	Data Breach	Intermediate
5	DDoS Attack	Intermediate
6	Insider Threat	Advanced

Cost Year 1: ₱112,000-224,000 (external facilitation) → ₱0 (internal capability)

Module 2B: Cyber Range Technical Exercises (Team-Learning)

💵 **LOW COST - Academic Pricing:**

- TryHackMe Business - ₱588/user/month
- U.S. Cyber Range - ₱504/user/month

🆓 **FREE Alternatives:**

- PicoCTF
- OverTheWire Wargames
- SANS Holiday Hack Challenge

Cost per Team Member: ₱5,600-16,800/year

Module 2C: EXCON Capability Development

Target: 2-3 certified internal facilitators by Year 2 **Cost:** ₱56,000-140,000

Step 3: Learn Security Tools—Integrated Architecture

Module 3A: SIEM Platform

🆓 **FREE Enterprise SIEM:**

- Splunk Enterprise via Academic Alliance (Value: ₱560,000-1,120,000)
- 10GB/day ingestion, Enterprise Security, SOAR included

🌐 **OPEN SOURCE Alternative:**

- ELK Stack (Elasticsearch, Logstash, Kibana)

Cost: ₱0 (software) + Infrastructure: ₱112,000-280,000

Module 3B: Essential Security Tool Portfolio

Network Monitoring (🌐 OPEN SOURCE):

- Suricata - Network IDS/IPS
- Zeek - Network security monitor
- Wireshark - Packet analysis

Endpoint Detection & Response:

- Wazuh (🌐 Free) or Commercial EDR (💳 ₱280,000-1,120,000/year)

Vulnerability Management:

- Nessus Essentials (🆓) or Professional (₱167,440/year)
- OpenVAS (🌐 Free)

Digital Forensics (🌐 All Free):

- Autopsy, SANS SIFT Workstation, Volatility, Wireshark, FTK Imager

Threat Intelligence:

- MISP (🌐 Free) + FIRST membership (💰 ₱56,000-280,000/year)

Module 3C: Integration & Automation

🆓 **FREE SOAR:**

- Splunk SOAR Community Edition
- Shuffle (open source)

TOTAL STEP 3 COSTS:

- Minimal: ₱112,000-280,000
- Moderate: ₱560,000-1,120,000
- Comprehensive: ₱1,680,000-2,800,000

Step 4: Get Entry-Level Certifications—Portfolio Strategy

Module 4A: Role-Based Certification Tracks

Track 1: Entry-Level Analyst (All Team Members)

Foundation Certification (Choose One):

💵 **CompTIA Security+**

- Cost: ₱21,952 exam
- Level: L1-L2 validation
- Self-Study: 60-80 hours
- Renewal: 3 years, 50 CEUs

🆓 **ISC2 Certified in Cybersecurity (CC)**

- Cost: 🆓 exam, ₱2,800/year AMF
- Level: L1 validation
- Self-Study: 40-60 hours (training included free)
- Renewal: 3 years, 45 CPEs

💵 **Google Cybersecurity Professional Certificate**

- Cost: ₱2,744/month (6 months = ₱16,464) or 🆓 with aid
- Level: L1 validation
- Format: Coursera online with labs

Recommendation: CC (free) for budget-constrained teams, Security+ for industry recognition

Track 2: Incident Responder (Core Team)

💰 **MODERATE COST:**

CompTIA CySA+ (Cybersecurity Analyst)

- Cost: ₱27,720 exam
- Level: L2-L3 validation
- Self-Study: 80-120 hours
- Focus: Blue team operations, SIEM, incident response

EC-Council ECIH (Certified Incident Handler)

- Cost: ₱47,600 exam only, or ₱89,544 with training
- Level: L2-L3 validation
- Self-Study: 100-150 hours
- Practical: Labs included with training

Deployment: Year 2: 2-3 team members; Year 3: 50% of core team

Track 3: Advanced Specialist (Senior Team)

💳 **PREMIUM COST:**

GIAC Certified Incident Handler (GCIH)

- Cost: ₱53,144-55,944 exam only, or ₱139,944 with SANS training
- Level: L3-L4 validation
- Study: 200+ hours or 5-day bootcamp + 80 hours
- Gold Standard: Highly respected globally

GIAC Certified Forensic Analyst (GCFA)

- Cost: Similar to GCIH
- Level: L3-L4 validation
- Focus: Advanced digital forensics

Certified Ethical Hacker (CEH)

- Cost: ₱67,144 exam, or ₱195,944 with training
- Level: L2-L3 validation
- Focus: Offensive security

🆓 **SUBSIDIZED Options:**

- DICT Training Partnerships (check availability)
- NSA Centers of Academic Excellence scholarships

Deployment: Year 3: 1-2 specialists

Track 4: Leadership (Management)

💳 **PREMIUM COST:**

CISSP (Certified Information Systems Security Professional)

- Cost: ₱41,944 exam, ₱7,560/year AMF
- Level: L3-L4 management focus
- Prerequisites: 5 years security experience
- Self-Study: 150-250 hours
- Recognition: Industry gold standard

CISM (Certified Information Security Manager)

- Cost: ₱32,200-42,560 exam, ₱7,840/year AMF
- Level: L3-L4 management
- Prerequisites: 5 years including 3 years management
- Focus: Governance, risk, incident programs

Deployment: Year 2-3: Director/Deputy achieves CISSP or CISM

Module 4B: Specialized Certifications

SOC Analyst:

- GIAC GCDA - ₱53,144-139,944
- GIAC GMON - ₱53,144-139,944
- Security Blue Team Level 1 - ₱22,344

Forensics:

- GIAC GCFE - ₱53,144-139,944
- CHFI - ₱30,800-106,344

Malware Analysis:

- GIAC GREM - ₱139,944+

Cloud Security:

- AWS Certified Security - ₱16,800
- Azure Security Engineer - ₱9,240
- CCSK - ₱22,120

Module 4C: Certification Cost Optimization

🆓 **FREE Preparation:**

- Professor Messer (Security+, Network+)
- ISC2 Official CC Training
- Cybrary free tier
- SANS Reading Room

💵 **LOW COST:**

- Udemy courses - ₱560-1,680 during sales
- LinkedIn Learning - ₱1,680/month
- Practice exams - ₱1,120-2,800

Study Groups: Form internal groups (🆓)

Certification Portfolio Timeline & Budget

Year 1: ₱0-87,808 (3-4 members, entry certifications)
Year 2: ₱55,440-266,896 (practitioner + remaining entry)
Year 3: ₱181,888-322,448 (advanced + leadership)

Three-Year Total:

- Minimal: ₱97,384-309,904
- Balanced: ₱280,000-560,000
- Comprehensive: ₱672,000-1,008,000

Step 5: Learn GRC (Governance, Risk & Compliance)—Philippine Context

Module 5A: Philippine Legal & Regulatory Framework

🆓 **FREE Essential Training:**

👤 **Self-Learning (Required for All):**

1. **Data Privacy Act of 2012 Training (8-12 hours)**

    - NPC online resources
    - Breach notification (72-hour rule)
    - Penalties: up to ₱5M, 6 years imprisonment

2. **Cybercrime Prevention Act Training (4-6 hours)**

    - Official Gazette full text
    - Cybercrimes definitions and penalties
    - Evidence handling for prosecution

3. **National Cybersecurity Plan 2023-2028 (4-6 hours)**

    - DICT official documentation
    - Organizational CERT requirements
    - NCERT incident reporting obligations
    - Six-stage IR model

👥 Team-Learning Workshops:

Workshop 1: Data Privacy & Breach Response (8 hours)

- Facilitator: Legal counsel + DPO + CSIRT lead
- Personal data categories in university context
- Breach notification requirements
- Coordination: CSIRT → DPO → NPC → Affected individuals

Workshop 2: Law Enforcement Coordination (4 hours)

- Facilitator: NCERT/NBI Cybercrime liaison
- When to involve law enforcement
- Evidence preservation and chain of custody
- Coordination with NBI, PNP, DICT Cybercrime Unit

Skill Progression - Compliance:

Level	Data Privacy	Cybercrime	NCSP Requirements
L1	**Identify personal data types**	**List major cybercrimes**	**Describe six IR stages**
L2	**Apply notification requirements**	**Preserve evidence appropriately**	**Execute NCSP workflow**

L3	**Lead breach response**	**Coordinate law enforcement**	**Produce NCERT reports**
L4	**Design privacy-by-design programs**	**Expert witness preparation**	**National CERT policy contribution**

Cost: ₱0 (all free resources)

Module 5B: International Frameworks

🆓 **FREE Framework Resources:**

ISO/IEC 27001 & 27035 Family:

- ISO 27035-1:2023 Principles (Official: 💳 ₱5,600-11,200; 🆓 Alternative: ENISA guides)
- ISO 27035-2 Planning & Preparation (free summaries)
- ISO 27035-3 ICT Incident Response Operations

NIST Cybersecurity Framework 2.0:

- Complete Framework (🆓) - Published February 2024
- Six core functions: Govern, Identify, Protect, Detect, Respond, Recover
- Self-Learning: NIST online courses (🆓, 10-15 hours)
- Team Workshop: Map UP CSIRT to CSF categories (8 hours)

NIST SP 800-61r3 (April 2025):

- Complete Guide (🆓) - Incident Handling aligned with CSF 2.0
- Self-Study: 20-30 hours
- Primary tactical reference for IR procedures

FIRST CSIRT Services Framework v2.1:

- Complete Framework (🆓)
- Five service areas: Event Management, Incident Management, Vulnerability Management, Situational Awareness, Knowledge Transfer
- Self-Study: 8-12 hours
- Team Exercise: Design UP service catalog (12 hours)

Skill Progression - Frameworks:

Level	ISO 27035	NIST CSF	FIRST Framework
L1	Describe incident phases	List six functions	Identify five service areas
L2	Apply processes	Map activities to CSF	Deliver defined services
L3	Customize for organization	Conduct CSF assessments	Design service portfolio
L4	Lead ISO implementation	Integrate CSF org-wide	Contribute to FIRST community

Cost: ₱0-28,000 (reference materials)

Module 5C: Risk Management Integration

👥 **Quarterly Risk Workshops (4 hours each):**

Workshop 1: Cyber Risk Scenario Development Develop university-specific scenarios:

1. Ransomware disrupting research data
2. Research IP theft by nation-state actors
3. Student data breach (PII exposure)
4. DDoS during enrollment period
5. Insider threat (credential misuse)
6. Supply chain compromise
7. Cloud service provider breach

Workshop 2: Risk Assessment Methodology

- Adopt risk matrix (🆓 NIST or ISO templates)
- Quantitative vs qualitative approaches
- Integration with university ERM

Workshop 3: Executive Risk Communication

- Briefings to the President, Board of Regents
- Risk dashboards and visualizations
- Translating technical risks to business impact

Deliverable: Annual Cybersecurity Risk Assessment Report

Skill Progression - Risk Management:

- L1: Identify cyber risks
- L2: Assess risks using standard methodology
- L3: Develop risk treatment plans, communicate to leadership
- L4: Design organizational cyber risk management program

Cost: ₱0-56,000 (risk assessment tools)

TOTAL STEP 5 COSTS:

- Year 1: ₱0-28,000
- Year 2: ₱28,000-84,000
- Year 3: ₱56,000-112,000

Step 6: Dive Into Specialized Areas—Building T-Shaped Teams

Specialization Strategy: T-Shaped Skill Model

Concept: Every team member develops:

- **Horizontal Bar:** Baseline competency (L1-L2) across all domains
- **Vertical Bar:** Expert competency (L3-L4) in 1-2 specializations

Five Specialization Tracks:

1. Security Monitoring & Detection (SOC Analysis)
2. Incident Response & Coordination
3. Digital Forensics & Malware Analysis
4. Vulnerability Management
5. Threat Intelligence & Situational Awareness

Cross-Training Protocol:

- Months 1-12: Rotate through all specializations (quarterly)
- Months 13-18: Self-select primary + secondary specialization
- Months 19+: Deep skill development while maintaining broad knowledge

Track 1: Security Monitoring & Detection (SOC Analysis)

Core Competencies:

Skill Area	L1	L2	L3	L4
SIEM Operations	Navigate dashboards	Tune rules	Custom correlation	Architecture design
Log Analysis	Identify anomalies	Investigate alerts	Hunt threats	Develop hunting program
Behavioral Analytics	Understand baselines	Apply UEBA tools	Build ML models	Research novel detection
Alert Triage	Follow runbooks	Prioritize independently	Optimize workflow	Mentor analysts

👤 **Self-Learning Resources:**

🆓 **FREE:**

- TryHackMe SOC Level 1 Path (40+ hours)
- TryHackMe SOC Level 2 Path (60+ hours)
- SANS Blue Team Village Talks (YouTube)
- Active Countermeasures Applied Network Defense

💵 **LOW COST:**

- Security Blue Team Junior Analyst - ₱22,344
- Blue Team Labs Online - ₱840/month

💳 **PREMIUM:**

- SANS SEC555 (SIEM with Tactical Analytics) - ₱403,200-504,000
- SANS SEC450 (Blue Team Fundamentals) - Similar pricing
- GIAC GCDA or GMON - ₱53,144-139,944

Recommended Allocation: 40% of CSIRT (3-4 members in 8-10 person team) **Cost per Specialist:** ₱22,400-504,000

Core Competencies:

Skill Area	L1	L2	L3	L4
Incident Handling	Follow playbooks	Adapt to novel situations	Lead complex incidents	Design IR program
Crisis Management	Execute tasks	Coordinate small team	Manage major incident	Design crisis protocols
Stakeholder Comm	Status updates	IT briefings	Executive communication	Media relations
Documentation	Incident notes	Comprehensive reports	Root cause analysis	Process improvement

👤 **Self-Learning:**

🆓 **FREE:**

- CISA Incident Response Training
- HTB Academy Incident Handling Path
- SANS Reading Room (IR papers)

💰 **MODERATE:**

- EC-Council ECIH - ₱47,600-89,544
- CompTIA CySA+ - ₱27,720

💳 **PREMIUM:**

- SANS SEC504 (Hacker Tools, Techniques, IR) - ₱403,200-504,000
- GIAC GCIH - ₱53,144-139,944

Recommended Allocation: 30% of CSIRT (2-3 members) **Cost per Specialist:** ₱28,000-504,000

Core Competencies:

Skill Area	L1	L2	L3	L4
Disk Forensics	Create images	File system analysis	Deleted file recovery	Expert witness testimony
Memory Forensics	Acquire dumps	Basic volatility analysis	Advanced memory analysis	Rootkit detection
Malware Analysis	Static basics	Dynamic sandbox	Reverse engineering	APT analysis
Evidence Handling	Chain of custody	Legal requirements	Court documentation	Expert consultation

👤 **Self-Learning:**

🆓 **FREE:**

- 13 Cubed YouTube Channel
- SANS DFIR Blog & Posters
- Volatility Documentation
- Autopsy Tutorials
- Practical Malware Analysis Book (~₱1,120-2,240 used)

💵 **LOW COST:**

- EC-Council CHFI - ₱30,800-106,344
- X-Ways Forensics Training - ₱28,000-56,000

💳 **PREMIUM:**

- SANS FOR500 (Windows Forensics) - ₱403,200-504,000
- SANS FOR508 (Advanced IR & Forensics) - Similar
- SANS FOR610 (Reverse-Engineering Malware) - Similar
- GIAC GCFA/GCFE/GREM - ₱53,144-139,944 each

🌐 **OPEN SOURCE Tools:** Autopsy, SIFT, Volatility, REMnux, Cuckoo Sandbox - All free

Recommended Allocation: 20% of CSIRT (1-2 members) **Cost per Specialist:** ₱0-504,000

Track 4: Vulnerability Management

Core Competencies:

Skill Area	L1	L2	L3	L4
Vuln Scanning	Run scans	Configure policies	Optimize coverage	Program design
Risk Prioritization	Read reports	CVSS scoring	Contextual analysis	Strategic reduction
Remediation	Track patches	Coordinate patching	Validate fixes	Develop strategy
Disclosure	Understand process	Internal coordination	External coordination	Disclosure program

👤 **Self-Learning:**

🆓 **FREE:**

- Tenable University (Nessus training)
- OWASP Testing Guide
- OpenVAS Documentation

💵 **LOW COST:**

- INE eLearnSecurity Junior Penetration Tester - ₱13,944

💰 **MODERATE:**

- Offensive Security OSCP - ₱83,944

Recommended Allocation: 10-15% of CSIRT (1 member) **Cost per Specialist:** ₱0-84,000

Track 5: Threat Intelligence & Situational Awareness

Core Competencies:

Skill Area	L1	L2	L3	L4
Intelligence Collection	Subscribe to feeds	Curate sources	OSINT techniques	Collection management
Analysis	Understand IOCs	Tactical analysis	Campaign tracking	Strategic intelligence
Dissemination	Share reports	Actionable alerts	Tailored products	Executive briefings
Platform Management	Use TI platform	Configure integrations	Optimize workflows	Design TI architecture

👤 **Self-Learning:**

🆓 **FREE:**

- FIRST Threat Intelligence Presentations
- MISP Training Materials
- SANS ISC InfoSec Handlers Diary
- Open Threat Exchange (OTX)

💰 **MODERATE:**

- SANS FOR578 (Cyber Threat Intelligence) - ₱403,200-504,000
- GIAC GCTI - ₱53,144-139,944

🌐 **OPEN SOURCE:** MISP - Free threat intelligence platform

Recommended Allocation: 10-15% of CSIRT (1-2 members) **Cost per Specialist:** ₱0-504,000

Module 6B: Research Security Specialization (UP-Specific)

Unique Requirements:

- High-performance computing (HPC) security
- Research data classification & handling
- International collaboration security
- Export control compliance
- Research integrity vs security incidents

👤 **Self-Learning:**

- NSA Centers of Academic Excellence Resources (🆓)
- EDUCAUSE Research Security Resources (🆓)
- Research security case studies (🆓)

👥 **Team Activities:**

- Partnership with UP Research Administration (🆓)
- Develop research security consulting service (🆓)
- Quarterly researcher training workshops (🆓)

Cost: ₱0-28,000

TOTAL STEP 6 COSTS (Team of 8-10):

- Minimal: ₱56,000-168,000
- Balanced: ₱448,000-840,000
- Comprehensive: ₱1,400,000-2,240,000

Step 7: Build Infrastructure—Modular Deployment

Infrastructure Modularity Approach

- **Module 7A:** Minimal Viable Operations (Months 1-6)
- **Module 7B:** Enhanced Detection (Months 7-12)
- **Module 7C:** Advanced Capabilities (Months 13-24)
- **Module 7D:** Optimization & Expansion (Months 25-36)

Module 7A: Minimal Viable Operations (Priority 1)

Target: Basic incident response operations

Component 1: SIEM Deployment

🆓 **FREE: Splunk Enterprise (Academic Alliance)**

- 10GB/day SIEM + Enterprise Security + SOAR
- Infrastructure: On-premise server (₱168,000-280,000) or Cloud (₱0-5,600/month)
- Deployment: 20-40 hours, 2-3 people over 2-4 weeks

🌐 **OPEN SOURCE: ELK Stack**

- Similar infrastructure
- More complex configuration
- Deployment: 40-60 hours

Cost: ₱0-280,000

Component 2: Ticketing System

🌐 **OPEN SOURCE:**

- TheHive - CSIRT-specific case management
- Deployment: 8-16 hours

💵 **LOW COST:**

- Jira or ServiceNow (if institutional license exists)

Cost: ₱0

Component 3: Forensics Workstations

Hardware (2-3 workstations):

- CPU: Intel i7/i9 or AMD Ryzen 7/9
- RAM: 64GB minimum
- Storage: 500GB SSD + 2TB HDD
- Cost per workstation: ₱84,000-140,000

🌐 **OPEN SOURCE Software (All Free):**

- SANS SIFT Workstation, Autopsy, Volatility, Wireshark, FTK Imager

Cost: ₱168,000-420,000 (hardware only)

Component 4: Secure Communications

🆓 **FREE:**

- Signal, PGP/GPG, Jitsi Meet

💵 **LOW COST:**

- Zoom or Microsoft Teams (if institutional license)

Cost: ₱0

Component 5: Documentation Repository

🌐 **OPEN SOURCE:**

- MediaWiki, BookStack, GitBook

💵 **LOW COST:**

- Confluence (if institutional license)

Cost: ₱0

MODULE 7A TOTAL:

- Minimal: ₱168,000-280,000
- Balanced: ₱448,000-672,000
- Time: 60-90 team hours over 4-8 weeks

Module 7B: Enhanced Detection (Priority 2)

Target: Proactive threat detection

Component 6: Network Sensors

🌐 **OPEN SOURCE:**

- Suricata or Zeek
- Hardware per sensor: ₱112,000-168,000
- Initial deployment: 3-5 sensors
- Cost: ₱336,000-840,000

Alternative: Virtual sensors on existing infrastructure (₱0)

Component 7: Endpoint Detection & Response

🌐 **OPEN SOURCE:**

- Wazuh - Host-based intrusion detection
- Infrastructure: ₱168,000-280,000 (server)
- Initial: 100-200 endpoints

💳 **PREMIUM Alternative:**

- Commercial EDR (CrowdStrike, SentinelOne, Microsoft Defender)
- Cost: ₱280-840/endpoint/month
- 100 endpoints: ₱336,000-1,008,000/year

Cost: ₱168,000-1,120,000 (first year)

Component 8: Vulnerability Scanner

🆓 **FREE:**

- Nessus Essentials (up to 16 IPs)

💰 **MODERATE:**

- Nessus Professional - ₱112,000-168,000/year

🌐 **OPEN SOURCE:**

- OpenVAS (₱0 software, ₱56,000-112,000 hardware)

Cost: ₱0-168,000/year

MODULE 7B TOTAL:

- Open Source: ₱560,000-1,120,000
- Hybrid: ₱840,000-1,680,000
- Time: 120-200 team hours over 2-3 months

Module 7C: Advanced Capabilities (Priority 3)

Target: Sophisticated threat detection, automation

Component 9: SOAR Platform

🆓 **FREE:**

- Splunk SOAR Community (included with Academic Alliance)
- Shuffle (open source)

Automation Use Cases:

1. Alert enrichment
2. User notifications
3. Host isolation
4. Automated evidence collection

Implementation: 60-100 hours over 2-3 months **Cost:** ₱0

Component 10: Malware Analysis Sandbox

🌐 **OPEN SOURCE:**

- Cuckoo Sandbox
- Infrastructure: ₱112,000-224,000
- Setup: 40-60 hours

💰 **MODERATE Commercial:**

- ANY.RUN - ₱22,400-44,800/month
- Joe Sandbox Cloud - Pay-per-analysis

Cost: ₱0-280,000

Component 11: Threat Intelligence Platform

🌐 **OPEN SOURCE:**

- MISP
- Infrastructure: ₱28,000-56,000
- Setup: 20-40 hours

Cost: ₱28,000-56,000

Component 12: Deception Technology

🌐 **OPEN SOURCE Honeypots:**

- T-Pot, Cowrie, Dionaea
- Infrastructure: ₱56,000-168,000

Cost: ₱56,000-168,000

MODULE 7C TOTAL:

- Open Source: ₱168,000-560,000
- Time: 150-250 team hours over 3-6 months

Module 7D: Optimization & Expansion (Ongoing)

Activities:

- Sensor optimization
- SIEM tuning
- Automation expansion
- Coverage expansion
- Backup and disaster recovery
- Redundancy implementation

Ongoing Costs:

- Maintenance/replacement: ₱280,000-560,000/year
- License renewals: ₱280,000-1,120,000/year
- Capacity expansion: ₱168,000-560,000/year

Infrastructure Summary: Cost Comparison

Approach	Year 1	Year 2	Year 3	3-Yr Total
Minimal (All Open Source)	₱560-840K	₱448-672K	₱448-672K	**₱1.456-2.184M**
Balanced (Hybrid)	₱1.12-1.68M	₱840-1.4M	₱840-1.4M	**₱2.8-4.48M**
Comprehensive (Premium)	₱2.24-3.36M	₱1.68-2.8M	₱1.68-2.8M	**₱5.6-8.96M**

Recommendation: Start with Balanced approach

Step 8: Join Communities and Stay Updated—Structured Engagement

Module 8A: Philippine National Partnerships

🆓 **FREE Mandatory Engagement:**

National CERT (NCERT) Registration

Actions Required (Month 1):

- Submit organizational CERT information
- Designate focal person
- Establish secure communication channels
- Time: 4-8 hours

Services to Leverage (Ongoing, 🆓):

- Incident response assistance
- Vulnerability assessment and penetration testing
- Threat monitoring and advisories
- Capacity building training
- Monthly coordination calls

Obligations:

- Report critical/severe incidents
- Participate in national exercises (annual)
- Share anonymized threat intelligence
- Attend quarterly meetings

DICT Cybersecurity Programs

🆓 **FREE Opportunities:**

- Training partnerships (CISCO, Oracle, Microsoft certifications)
- ICT Academy programs
- Cybersecurity Awareness Month (October)
- Policy consultation opportunities

Cost: ₱0-112,000/year (travel for meetings)

Module 8B: Regional ASEAN Engagement

🆓-💰 **MODERATE COST:**

ASEAN Cyber Capacity Programme (ACCP)

- Workshops for senior officials (🆓, regional travel ₱28,000-84,000)
- Technical training for CERT personnel (🆓, regional travel)
- Virtual exercises (🆓)

ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE)

- Cyber law and policy research (🆓)
- CERT technical training (🆓-💵 ₱11,200-28,000)
- Virtual cyber defense exercises (🆓)

Bilateral Partnerships

Peer CSIRT Relationships (🆓):

- ThaiCERT (Thailand)
- SingCERT (Singapore)
- JPCERT/CC (Japan)
- Academic CSIRTs: NUS, Universiti Malaya, Chulalongkorn

Activities:

- Quarterly virtual calls (🆓)
- Annual staff exchanges (💰 ₱56,000-168,000)
- Joint exercises (🆓)
- Threat intelligence sharing (🆓)

Cost Year 1-3: ₱56,000-280,000/year

Module 8C: International FIRST Membership

💰 **MODERATE COST Investment**

Membership Timeline

Year 1: Build Foundation

- Establish operational CSIRT
- Document services following FIRST framework (🆓)
- Conduct SIM3 assessment (🆓)
- Identify potential sponsors (🆓)

Year 2: Formal Documentation

- Draft RFC 2350 CSIRT description (🆓, 20-40 hours)
- Achieve baseline SIM3 maturity
- Engage sponsors (REN-ISAC, regional academic CSIRT)

Year 3: Application & Membership

- Submit application (💰 ₱56,000)
- Site visit (💰 ₱28,000-112,000 hosting)
- Annual dues: ₱112,000-280,000

Membership Benefits

🆓 **Included:**

- Private threat intelligence platform
- Member-only training resources
- Technical colloquium presentations
- Global CSIRT coordination
- Best practice documentation

💰 **MODERATE Optional:**

- FIRST Conference (Annual)
    - Registration: ₱22,400-44,800
    - Travel: ₱112,000-280,000/person
    - Send 1-2 members annually

Three-Year Investment:

- Year 1: ₱0
- Year 2: ₱0-28,000

- Year 3: ₱196,000-392,000
- Ongoing: ₱280,000-560,000/year

Module 8D: Academic Sector Networks

REN-ISAC Membership

💵 **LOW-**💰 **MODERATE COST**

Services:

- 24/7 watch desk support
- Sector-specific threat intelligence
- Security contact database
- Vulnerability scanning
- Web seminars and training
- Annual Summit conference

Action: Contact REN-ISAC about partnership for Southeast Asian university **Estimated Cost:** ₱0-280,000/year

EDUCAUSE Cybersecurity Program

💵 **LOW COST**

🆓 **FREE Resources:**

- Cybersecurity resource library
- Benchmarking surveys
- Working group publications

💵 **LOW COST Paid:**

- Security Professionals Conference
    - Virtual: ₱11,200-22,400
    - In-person: ₱44,800-84,000 + travel
- EDUCAUSE Institutional Membership: Variable

Year 1-3 Budget: ₱11,200-112,000/year

TF-CSIRT & SIM3 Certification

💰 **MODERATE COST (Optional Year 3+)**

SIM3-based CSIRT Certification:

- Objective validation of maturity
- TF-CSIRT certification process

- Cost: €2,000-5,000 (~₱123,200-308,000)

Recommendation: Consider Year 3-4 after achieving strong SIM3 scores

Module 8E: Continuous Learning Infrastructure

👤 **Self-Learning (Individual):**

🆓 **FREE Daily/Weekly:** Subscribe to:

- SANS Internet Storm Center
- FIRST Technical Lists
- US-CERT Bulletins
- Krebs on Security
- r/netsec Reddit

💵 **LOW COST Monthly:**

- Security podcasts (🆓)
- Online courses (₱560-2,800/month)

👥 **Team-Learning (Structured):**

Weekly Team Meeting (1 hour, 🆓):

- Threat intelligence briefing
- Tool demonstrations
- Incident review
- Knowledge sharing

Monthly Technical Deep-Dive (2-4 hours, 🆓): Rotating specializations:

- Month 1: SOC Operations
- Month 2: Incident Response
- Month 3: Forensics
- Month 4: Vulnerability Management
- Month 5: Threat Intelligence
- Repeat cycle

Quarterly External Expert Sessions (🆓-💰):

- NCERT representatives (🆓)
- Peer CSIRT practitioners (🆓)
- Commercial vendors (🆓)
- Regional researchers (🆓-💵 ₱28,000-56,000)

Annual Conference Attendance (💰):

Conference Selection:

Type	Frequency	Cost Range	Team Members
National (Philippines)	2-3x/year	🆓-💵 ₱5,600-28,000	4-6 members
Regional (ASEAN)	1x/year	💵-💰 ₱28,000-112,000	2-3 members
International Premium	1x/2 years	💰-💳 ₱168,000-336,000	1-2 senior

Knowledge Management:

1. Incident Reports: Within 48 hours of closure
2. Lessons Learned: Quarterly compilation
3. Playbook Updates: Continuous improvement
4. Tool Procedures: Updated with changes
5. Annual Report: Comprehensive year review

Community Contribution (Optional):

- Blog posts on UP CSIRT activities
- Presentations at local security meetups (🆓)
- White papers on Philippine threat landscape
- Contribution to open source tools

Budget for Continuous Learning

Item	Year 1	Year 2	Year 3	Ongoing
Conferences & Events	₱112-224K	₱224-336K	₱280-448K	₱280-560K/yr
Subscriptions	₱0-56K	₱56-112K	₱56-112K	₱56-112K/yr
Guest Speakers	₱0-56K	₱56-112K	₱56-112K	₱56-112K/yr
TOTAL STEP 8	**₱112-336K**	**₱336-560K**	**₱392-672K**	**₱392-784K/yr**

Complete Three-Year Budget Summary

Cost by Implementation Approach

Currency Note: All costs in Philippine Pesos (₱), ₱56 = $1 USD

Approach 1: Minimal Budget (Maximum Open Source)

Step	Year 1	Year 2	Year 3	3-Year Total
1. Basics	₱0-56K	₱0	₱0	**₱0-56K**
2. Practice	₱112-224K	₱112-168K	₱56-112K	**₱280-504K**
3. Tools	₱280-448K	₱168-280K	₱112-224K	**₱560-952K**
4. Certifications	₱0-112K	₱112-224K	₱168-280K	**₱280-616K**
5. GRC	₱0-28K	₱28-56K	₱56-112K	**₱84-196K**
6. Specializations	₱56-168K	₱168-280K	₱280-448K	**₱504-896K**
7. Infrastructure	₱560-840K	₱448-672K	₱448-672K	**₱1.456-2.184M**
8. Communities	₱112-224K	₱224-336K	₱336-560K	**₱672-1.12M**
Personnel (5-8 FTE)	₱5.6-8.4M	₱8.4-11.2M	₱10.08-14M	**₱24.08-33.6M**
GRAND TOTAL	**₱6.72-10.472M**	**₱9.632-13.216M**	**₱11.536-16.408M**	**₱27.888-40.096M**

Approach 2: Balanced Budget (Hybrid FOSS + Commercial)

Step	Year 1	Year 2	Year 3	3-Year Total
1. Basics	₱112-168K	₱0-56K	₱0-56K	**₱112-280K**
2. Practice	₱168-280K	₱168-224K	₱112-168K	**₱448-672K**
3. Tools	₱840-1.4M	₱560-1.008M	₱560-1.008M	**₱1.96-3.416M**
4. Certifications	₱112-224K	₱224-392K	₱336-560K	**₱672-1.176M**
5. GRC	₱28-56K	₱56-112K	₱56-112K	**₱140-280K**

Step	Year 1	Year 2	Year 3	3-Year Total
6. Specializations	₱168-448K	₱448-840K	₱560-1.12M	**₱1.176-2.408M**
7. Infrastructure	₱1.12-1.68M	₱840-1.4M	₱840-1.4M	**₱2.8-4.48M**
8. Communities	₱168-336K	₱336-560K	₱448-672K	**₱952-1.568M**
Personnel (8-12 FTE)	₱8.4-11.2M	₱10.08-14M	₱11.2-15.68M	**₱29.68-40.88M**
GRAND TOTAL	**₱11.144-15.792M**	**₱12.712-18.592M**	**₱14.112-20.776M**	**₱37.968-55.16M**

Approach 3: Comprehensive Budget (Premium Tools + Training)

Step	Year 1	Year 2	Year 3	3-Year Total
1. Basics	₱168-280K	₱56-112K	₱56-112K	**₱280-504K**
2. Practice	₱280-448K	₱224-336K	₱168-280K	**₱672-1.064M**
3. Tools	₱1.96-2.8M	₱1.4-2.24M	₱1.4-2.24M	**₱4.76-7.28M**
4. Certifications	₱280-448K	₱448-672K	₱560-840K	**₱1.288-1.96M**
5. GRC	₱56-112K	₱112-168K	₱112-168K	**₱280-448K**
6. Specializations	₱560-1.12M	₱1.12-1.96M	₱1.4-2.24M	**₱3.08-5.32M**
7. Infrastructure	₱2.24-3.36M	₱1.68-2.8M	₱1.68-2.8M	**₱5.6-8.96M**
8. Communities	₱280-448K	₱448-672K	₱560-840K	**₱1.288-1.96M**
Personnel (10-15 FTE)	₱10.08-14M	₱11.2-15.68M	₱14-19.6M	**₱35.28-49.28M**
GRAND TOTAL	**₱15.904-23.016M**	**₱16.688-24.64M**	**₱19.936-29.12M**	**₱52.528-76.776M**

Three-Year Implementation Timeline: Modular Progression

Year 1: Foundation & Initial Operations (Months 1-12)

Q1 (Months 1-3): Budget ₱1.4-2.8M

- Module 1A: Foundational knowledge
- Module 1B: Governance foundation
- Module 2A: Begin monthly TTX
- Module 8A: NCERT registration

Q2 (Months 4-6): Budget ₱1.68-2.8M

- Module 3A: Deploy SIEM
- Module 7A: Minimal viable infrastructure
- Module 4A Track 1: First certifications
- Module 5A: Philippine legal training

Q3 (Months 7-9): Budget ₱1.68-2.8M

- Module 3B: Deploy network monitoring
- Module 2B: First cyber range exercise
- Module 8E: Establish continuous learning
- Module 5B: Begin NIST/ISO framework study

Q4 (Months 10-12): Budget ₱1.96-3.36M

- Module 7B: Enhanced detection infrastructure
- Module 3B: Deploy EDR pilot
- Module 5C: First risk assessment
- Module 6: Cross-training rotation begins

Year 1 Deliverables:

- Operational CSIRT with 24/7 contact capability
- Basic SIEM and detection infrastructure
- 12 tabletop exercises completed
- 3-4 team members with entry certification
- NCERT coordination established
- Baseline SIM3 assessment
- Initial incident response playbooks

Year 1 Total: ₱6.72-11.76M

Year 2: Capability Enhancement (Months 13-24)

Q5 (Months 13-15): Budget ₱1.96-3.36M

- Module 6: Specialization tracks assigned
- Module 4A Track 2: Practitioner certifications
- Module 7C: SOAR platform deployment
- Module 8B: First regional ASEAN engagement

Q6 (Months 16-18): Budget ₱2.24-3.92M

- Module 3B: Full EDR rollout to priority systems
- Module 2C: EXCON capability development
- Module 3C: Integration & automation
- Module 8C: FIRST membership preparation

Q7 (Months 19-21): Budget ₱2.52-4.2M

- Module 7C: Threat intelligence platform (MISP)
- Module 6: Specialized training (3-5 members)
- Module 5C: Quarterly risk assessments routine
- Module 2B: Quarterly cyber range exercises

Q8 (Months 22-24): Budget ₱2.8-4.76M

- Module 7C: Malware analysis sandbox
- Module 4A Track 3: First advanced certification
- Module 8C: RFC 2350 documentation complete
- Module 8D: First peer CSIRT partnership

Year 2 Deliverables:

- 24/7 on-call capability
- SOAR automation operational
- Comprehensive tool integration
- 50% team with practitioner certifications
- Specialized capabilities operational
- FIRST membership application ready
- SIM3 Level 2-3 maturity
- 15-20 defined services

Year 2 Total: ₱9.52-15.96M

Year 3: Maturation & Leadership (Months 25-36)

Q9 (Months 25-27): Budget ₱3.08-5.04M

- Module 8C: FIRST membership achieved
- Module 4A Track 4: Leadership certifications
- Module 7D: Infrastructure optimization
- Module 6B: Research security program

Q10 (Months 28-30): Budget ₱3.36-5.32M

- Module 3C: Advanced automation
- Module 6: Advanced specialized training
- Module 8E: First FIRST Conference
- Module 5C: Annual risk assessment to leadership

Q11 (Months 31-33): Budget ₱3.64-5.6M

- Module 8B: Regional CSIRT partnership exchanges
- Module 2B: Full-scale multi-day incident simulation
- Module 7D: Redundancy & disaster recovery
- Consider TF-CSIRT SIM3 certification

Q12 (Months 34-36): Budget ₱3.92-6.16M

- Module 1B: Final SIM3 assessment (Level 3-4)
- Module 8E: Annual report publication
- Module 8A: Mentor peer Philippine universities
- Planning for Year 4-5 continuous improvement

Year 3 Deliverables:

- FIRST full membership active
- SIM3 Level 3-4 maturity demonstrated
- 24/7 SOC operations or equivalent
- Published annual report
- Regional leadership in academic CSIRT
- All team certified, multiple advanced
- Comprehensive 20-25 service portfolio
- Mentoring peer institutions
- Measurable risk reduction metrics

Year 3 Total: ₱14-22.12M

Competency Matrix: Team Skill Progression

Comprehensive Skill Tracking (Self-Assessment Tool)

Instructions: Each team member self-assesses quarterly. Manager validates annually.

Competency Domain	**L1 Foundation**	**L2 Practitioner**	**L3 Advanced**	**L4 Expert**	**Current**	**Target (6mo)**	**Target (1yr)**
1. Incident Response	Understand IR lifecycle	Execute playbooks	Lead incidents	Design IR program			
2. SIEM Operations	Navigate interface	Tune rules	Custom correlations	Architecture design			
3. Network Analysis	Capture packets	Filter & extract	Reconstruct attacks	Hunt advanced threats			
4. Endpoint Forensics	Image systems	File system analysis	Memory forensics	Expert testimony			
5. Malware Analysis	Static basics	Dynamic sandbox	Reverse engineering	APT analysis			
6. Threat Intelligence	Consume feeds	Tactical analysis	Campaign tracking	Strategic intelligence			
7. Vulnerability Mgmt	Run scans	Prioritize remediation	Validate fixes	Program design			

Competency Domain	L1 Foundation	L2 Practitioner	L3 Advanced	L4 Expert	Current	Target (6mo)	Target (1yr)
8. Compliance	Know laws	Apply requirements	Lead audits	Policy development			
9. Crisis Communication	Status updates	IT briefings	Executive comms	Media relations			
10. Automation/ Scripting	Read code	Modify scripts	Write custom tools	Design architectures			

Scoring Guide:

- **L1:** 0-6 months experience, requires supervision
- **L2:** 6-18 months experience, works independently with guidance
- **L3:** 18-36 months experience, handles complex work independently
- **L4:** 3+ years experience, mentors others, innovates

Team Composition Target (Year 3, 10-person team):

- **L4 Expert:** 2 people (Director + Senior Specialist)
- **L3 Advanced:** 4 people (Deputies, Lead Responders)
- **L2 Practitioner:** 3 people (Analysts, Responders)
- **L1 Foundation:** 1 person (New hire, rotating junior)

Conclusion: Modular, Scalable, Achievable

This roadmap provides a **flexible, modular framework** adaptable to the University of the Philippines' unique constraints and opportunities. Key success principles:

🔧 **Modularity:** Implement components in any sequence based on priorities, budget, and existing capabilities. Start where you are, use what you have, do what you can.

📊 **Transparency:** Clear cost indicators (🆓🌐💵💰💳) enable informed budgeting. Three implementation approaches (Minimal/Balanced/Comprehensive) offer choices ranging from ₱27.9M to ₱76.8M over three years.

👤👥 **Dual Learning Modes:** Self-learning empowers individuals; team-learning builds cohesion. Both essential for CSIRT success.

🎯 **Skill Progression:** Four-level competency model (L1-L4) provides clear development paths. Track quarterly, celebrate growth.

💰 **Budget Realism:** Three-year investment of ₱27.9M-76.8M (70-80% personnel, 15-25% technology, 5-10% community/training) is substantial but proportional to risk. For perspective, a single major data breach under the Data Privacy Act could result in fines up to ₱5M plus reputational damage worth multiples of the entire CSIRT budget.

🇵🇭 **Philippine Context:** Deep integration with NCERT, compliance with NCSP 2023-2028, alignment with Data Privacy Act obligations, ensure national ecosystem contribution beyond institutional benefit.

The University of the Philippines, as our nation's premier academic institution, must lead by example. This roadmap provides the path—modular, practical, and achievable. The question isn't whether UP can afford to build this capacity—**the question is whether UP can afford not to**.

Let's begin.

References

Active Countermeasures. (n.d.). *Applied network defense.* https://www.activecountermeasures.com/

Amazon Web Services. (n.d.). *AWS Certified Security – Specialty.* https://aws.amazon.com/certification/certified-security-specialty/

ANY.RUN. (n.d.). *Interactive malware analysis service.* https://any.run/

Association of Southeast Asian Nations. (2022). *ASEAN cybersecurity cooperation strategy 2021-2025.* https://asean.org/

ASEAN-Singapore Cybersecurity Centre of Excellence. (n.d.). *Training programmes.* https://www.ascce.org/

AT&T Cybersecurity. (n.d.). *Open Threat Exchange (OTX).* https://cybersecurity.att.com/open-threat-exchange

Atlassian. (n.d.). *Jira software.* https://www.atlassian.com/software/jira

Basis Technology. (n.d.). *Autopsy: Digital forensics platform.* https://www.autopsy.com/

Blue Team Labs Online. (n.d.). *Practice platform.* https://blueteamlabs.online/

BookStack. (n.d.). *Simple & free wiki software.* https://www.bookstackapp.com/

Cabato, L. (2024). DICT: *Low salary discourages cybersecurity experts from joining gov't.* INQUIRER.net. https://newsinfo.inquirer.net/2013929/dict-low-salary-discourages-cybersecurity-experts-from-joining-govt

CIRT. (n.d.). *Nikto web scanner.* https://cirt.net/Nikto2

Cloud Range. (2025). *Cyber attack simulations for SOC & incident response teams.* https://www.cloudrangecyber.com/

Cloud Security Alliance. (n.d.). *Certificate of Cloud Security Knowledge* (CCSK). https://cloudsecurityalliance.org/education/ccsk/

CompTIA. (n.d.-a). *CompTIA Security+ certification.* https://www.comptia.org/certifications/security

CompTIA. (n.d.-b). *CompTIA CySA+ certification.* https://www.comptia.org/certifications/cybersecurity-analyst

Cowrie. (n.d.). SSH/*Telnet honeypot.* https://github.com/cowrie/cowrie

CrowdStrike. (n.d.). *CrowdStrike Falcon platform.* https://www.crowdstrike.com/

Cuckoo Foundation. (n.d.). *Cuckoo Sandbox.* https://cuckoosandbox.org/

Cyberint. (2024). *Philippine threat landscape report* 2024-2025. https://e.cyberint.com/hubfs/Philippine%20Threat%20Landscape%20Report%202024.pdf

Cybersecurity and Infrastructure Security Agency. (n.d.). US-CERT *bulletins.* https://www.cisa.gov/

Cybersecurity and Infrastructure Security Agency. (2025a). *Incident response training.* https://www.cisa.gov/resources-tools/programs/Incident-Response-Training

Cybersecurity and Infrastructure Security Agency. (2025b). CISA *tabletop exercise packages.* https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages

Cybersecurity and Infrastructure Security Agency. (2025c). *Exercise design and development.* https://www.cisa.gov/exercise

Cybrary. (n.d.). *Cybersecurity training platform.* https://www.cybrary.it/

Department of Information and Communications Technology. (2024a). *National Cybersecurity Plan* 2023-2028. Republic of the Philippines. https://cms-cdn.e.gov.ph/DICT/pdf/NCSP-2023-2028-FINAL-DICT.pdf

Department of Information and Communications Technology. (2024b). *National Computer Emergency Response Team* (NCERT). Republic of the Philippines. https://dict.gov.ph/cybersecurity/

Deutsche Telekom Security. (n.d.). T-Pot: *The all in one honeypot platform.* https://github.com/telekom-security/tpotce

DFIR.training. (n.d.). *Digital forensics and incident response training resources.* https://www.dfir.training/

Dionaea. (n.d.). *Malware capture honeypot.* https://github.com/DinoTools/dionaea

EC-Council. (n.d.). *EC-Council certifications.* https://www.eccouncil.org/

EDUCAUSE. (n.d.). *Cybersecurity and privacy program.* https://www.educause.edu/

Elastic. (n.d.). *Elastic Stack: Elasticsearch, Logstash, Kibana.* https://www.elastic.co/

European Union Agency for Cybersecurity. (2020). *How to setup CSIRT and SOC: Good practice guide.* https://www.enisa.europa.eu/

Exterro. (n.d.). *FTK Imager.* https://www.exterro.com/ftk-imager

Federal Emergency Management Agency. (n.d.). *Emergency Management Institute.* https://training.fema.gov/

Forum of Incident Response and Security Teams. (n.d.-a). *About FIRST.* https://www.first.org/about/

Forum of Incident Response and Security Teams. (n.d.-b). *Threat intelligence.* https://www.first.org/global/sigs/cti/

Forum of Incident Response and Security Teams. (2023). *CSIRT services framework* (Version 2.1). https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2-1

Forum of Incident Response and Security Teams. (2024). *Membership process.* https://www.first.org/membership/process

GIAC. (n.d.-a). *GIAC Certified Incident Handler* (GCIH). https://www.giac.org/certifications/certified-incident-handler-gcih/

GIAC. (n.d.-b). *GIAC Certified Forensic Analyst* (GCFA). https://www.giac.org/certifications/certified-forensic-analyst-gcfa/

GIAC. (n.d.-c). *GIAC Certified Detection Analyst* (GCDA). https://www.giac.org/certifications/certified-detection-analyst-gcda/

GIAC. (n.d.-d). *GIAC Continuous Monitoring* (GMON). https://www.giac.org/certifications/continuous-monitoring-certification-gmon/

GIAC. (n.d.-e). *GIAC Certified Forensic Examiner* (GCFE). https://www.giac.org/certifications/certified-forensic-examiner-gcfe/

GIAC. (n.d.-f). *GIAC Reverse Engineering Malware* (GREM). https://www.giac.org/certifications/reverse-engineering-malware-grem/

GIAC. (n.d.-g). *GIAC Cyber Threat Intelligence* (GCTI). https://www.giac.org/certifications/cyber-threat-intelligence-gcti/

Gibb, R. (n.d.). *13 Cubed* [YouTube channel]. https://www.youtube.com/@13Cubed

GitBook. (n.d.). *Documentation platform.* https://www.gitbook.com/

GNU Privacy Guard. (n.d.). *The GNU Privacy Guard.* https://gnupg.org/

Google. (n.d.). *Google Cybersecurity Professional Certificate.* https://grow.google/certificates/cybersecurity/

Greenbone. (n.d.). *OpenVAS: Open Vulnerability Assessment System.* https://www.openvas.org/

Hack The Box. (n.d.). *Cybersecurity training platform.* https://www.hackthebox.com/

Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Leading Issues in Information Warfare & Security Research*, 1(1), 80-106.

INE. (n.d.). *eLearnSecurity certifications.* https://ine.com/

International Organization for Standardization. (2023a). ISO/IEC 27035-1:2023 *Information security incident management—Part 1: Principles and process.* https://www.iso.org/standard/78973.html

International Organization for Standardization. (2023b). ISO/IEC 27035-2:2023 *Information security incident management—Part 2: Guidelines to plan and prepare for incident response.* https://www.iso.org/standard/78974.html

International Organization for Standardization. (2023c). ISO/IEC 27035-3:2020 *Information technology—Security techniques—Information security incident management—Part 3: Guidelines for ICT incident response operations.* https://www.iso.org/standard/77404.html

ISACA. (n.d.). *Certified Information Security Manager* (CISM). https://www.isaca.org/credentialing/cism

ISC2. (n.d.-a). *ISC2 Certified in Cybersecurity* (CC). https://www.isc2.org/Certifications/CC

ISC2. (n.d.-b). *Certified Information Systems Security Professional* (CISSP). https://www.isc2.org/Certifications/CISSP

Jitsi. (n.d.). *Jitsi Meet: Free video conferencing.* https://jitsi.org/

Joe Security. (n.d.). *Joe Sandbox Cloud.* https://www.joesecurity.org/

JPCERT/CC. (n.d.). *JPCERT Coordination Center.* https://www.jpcert.or.jp/english/

Krebs, B. (n.d.). *Krebs on Security.* https://krebsonsecurity.com/

LinkedIn. (n.d.). *LinkedIn Learning.* https://www.linkedin.com/learning/

Messer, J. (n.d.). *Professor Messer* [YouTube channel]. https://www.professormesser.com/

Microsoft. (n.d.). *Microsoft security certifications.* https://learn.microsoft.com/en-us/certifications/

MISP Project. (n.d.). *MISP: Open source threat intelligence platform.* https://www.misp-project.org/

MITRE. (2023). ATT&CK *framework.* https://attack.mitre.org/

Multi-State Information Sharing and Analysis Center. (n.d.). *Cybersecurity resources.* https://www.cisecurity.org/ms-isac

National Institute of Standards and Technology. (2024). *Cybersecurity Framework* (Version 2.0). https://www.nist.gov/cyberframework

National Institute of Standards and Technology. (2025). *Computer security incident handling guide* (NIST Special Publication 800-61 Revision 3). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf

National Privacy Commission. (2012). *Republic Act 10173: Data Privacy Act of 2012*. Republic of the Philippines. https://privacy.gov.ph/data-privacy-act/

National Privacy Commission. (2016). *Implementing rules and regulations of the Data Privacy Act of 2012*. Republic of the Philippines. https://privacy.gov.ph/

National Security Agency. (n.d.). *Centers of Academic Excellence in Cybersecurity*. https://www.nsa.gov/Academics/Centers-of-Academic-Excellence/

Offensive Security. (n.d.). *Offensive Security Certified Professional* (OSCP). https://www.offensive-security.com/pwk-oscp/

Official Gazette of the Republic of the Philippines. (2012). *Republic Act No. 10175: Cybercrime Prevention Act of 2012*. https://www.officialgazette.gov.ph/2012/09/12/republic-act-no-10175/

Open CSIRT Foundation. (2023). *SIM3 v2 interim standard: Security Incident Management Maturity Model*. https://opencsirt.org/

Open Information Security Foundation. (n.d.). *Suricata IDS/IPS*. https://suricata.io/

OpenText. (n.d.). *EnCase forensic*. https://www.opentext.com/products/encase-forensic

OverTheWire. (n.d.). *Wargames*. https://overthewire.org/wargames/

OWASP Foundation. (n.d.). *Open Web Application Security Project*. https://owasp.org/

Palo Alto Networks. (n.d.). *Cortex XSOAR*. https://www.paloaltonetworks.com/cortex/cortex-xsoar

Philippine News Agency. (2022, December 13). *DICT to launch courses on cybersecurity to build PH capacity*. https://www.pna.gov.ph/articles/1191181

PicoCTF. (n.d.). *Free computer security education*. https://picoctf.org/

Presidential Communications Office. (2024). *PBBM adopts DICT's National Cybersecurity Plan 2023-2028*. https://pco.gov.ph/

Reddit. (n.d.). *r/netsec: Network security*. https://www.reddit.com/r/netsec/

REN-ISAC. (2025). *CSIRT services*. https://www.ren-isac.net/

SANS Institute. (n.d.-a). SEC275: Foundations - Computers, Technology, & Security
. https://www.sans.org/cyberaces

SANS Institute. (n.d.-b). *Internet Storm Center*. https://isc.sans.edu/

SANS Institute. (n.d.-c). *SANS Holiday Hack Challenge*. https://www.sans.org/mlp/holiday-hack-challenge/

SANS Institute. (n.d.-d). *Cyber range facilitator resources*. https://www.sans.org/cyber-ranges/

SANS Institute. (n.d.-e). *SIFT Workstation*. https://www.sans.org/tools/sift-workstation/

SANS Institute. (n.d.-f). *Reading room*. https://www.sans.org/white-papers/

SANS Institute. (n.d.-g). *Blue Team Village*. https://www.blueteamvillage.org/

SANS Institute. (n.d.-h). *SEC555: SIEM with tactical analytics*. https://www.sans.org/cyber-security-courses/siem-with-tactical-analytics/

SANS Institute. (n.d.-i). *SEC450: Blue Team fundamentals*. https://www.sans.org/cyber-security-courses/blue-team-fundamentals-security-operations-analysis/

SANS Institute. (n.d.-j). *SEC504: Hacker tools, techniques, and incident handling*. https://www.sans.org/cyber-security-courses/hacker-techniques-exploits-incident-handling/

SANS Institute. (n.d.-k). *DFIR blog*. https://www.sans.org/blog/?focus-area=digital-forensics

SANS Institute. (n.d.-l). *FOR500: Windows forensic analysis*. https://www.sans.org/cyber-security-courses/windows-forensic-analysis/

SANS Institute. (n.d.-m). *FOR508: Advanced incident response, threat hunting, and digital forensics*. https://www.sans.org/cyber-security-courses/advanced-incident-response-threat-hunting-training/

SANS Institute. (n.d.-n). *FOR610: Reverse-engineering malware*. https://www.sans.org/cyber-security-courses/reverse-engineering-malware-malware-analysis-tools-techniques/

SANS Institute. (n.d.-o). *InfoSec handlers diary*. https://isc.sans.edu/diary.html

SANS Institute. (n.d.-p). *FOR578: Cyber threat intelligence*. https://www.sans.org/cyber-security-courses/cyber-threat-intelligence/

Security Blue Team. (n.d.). *Security Blue Team certifications*. https://www.securityblue.team/

Security Onion Solutions. (n.d.). *Security Onion*. https://securityonionsolutions.com/

SentinelOne. (n.d.). *Singularity platform*. https://www.sentinelone.com/

ServiceNow. (n.d.). *Security operations*. https://www.servicenow.com/

Shuffle. (n.d.). *Open source security automation*. https://shuffler.io/

Signal Foundation. (n.d.). *Signal: Private messenger*. https://signal.org/

Sikorski, M., & Honig, A. (2012). *Practical malware analysis: The hands-on guide to dissecting malicious software*. No Starch Press.

SingCERT. (n.d.). *Singapore Computer Emergency Response Team*. https://www.csa.gov.sg/singcert

Splunk. (n.d.). *Splunk Academic Alliance Program*. https://www.splunk.com/

Swimlane. (n.d.). *Security automation and orchestration*. https://swimlane.com/

Tenable. (n.d.-a). *Nessus Essentials*. https://www.tenable.com/products/nessus/nessus-essentials

Tenable. (n.d.-b). *Nessus Professional*. https://www.tenable.com/products/nessus/nessus-professional

Tenable. (n.d.-c). *Tenable University*. https://www.tenable.com/education

ThaiCERT. (n.d.). *Thailand Computer Emergency Response Team*. https://www.thaicert.or.th/

TheHive Project. (n.d.). *TheHive: Security incident response platform*. https://thehive-project.org/

Trusted Introducer. (n.d.). *TF-CSIRT certification*. https://www.trusted-introducer.org/

TryHackMe. (n.d.). *Cyber security training*. https://tryhackme.com/

U.S. Cyber Range. (2025). *Educational cyber range*. https://www.uscyberrange.org/

Udemy. (n.d.). *Online courses*. https://www.udemy.com/

University of the Philippines-CIFAL Philippines. (2021). *Digital governance and cybersecurity*. https://cifal.up.edu.ph/

Volatility Foundation. (n.d.). *Volatility: Advanced memory forensics framework*. https://www.volatilityfoundation.org/

Wazuh. (n.d.). *Open source security platform*. https://wazuh.com/

West-Brown, M. J., Stikvoort, D., Kossakowski, K. P., Killcrece, G., Ruefle, R., & Zajicek, M. (2003). *Handbook for computer security incident response teams (CSIRTs)* (CMU/SEI-2003-HB-002). Carnegie Mellon University Software Engineering Institute. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6305

Wikimedia Foundation. (n.d.). *MediaWiki*. https://www.mediawiki.org/

Wireshark Foundation. (n.d.). *Wireshark: Network protocol analyzer*. https://www.wireshark.org/

X-Ways Software Technology. (n.d.). *X-Ways Forensics*. https://www.x-ways.net/forensics/

Zeek. (n.d.). *Zeek network security monitor*. https://zeek.org/

Zoom Video Communications. (n.d.). *Zoom for education*. https://zoom.us/education

Audit trail

Details

FILE NAME	[OVPDxRoadmaps001] Capacity Development Roadmap for UP CSIRT_v01_11282025.pdf - 12/5/25, 12:07 PM
STATUS	● Signed
STATUS TIMESTAMP	2025/12/05 04:29:38 UTC

Activity

SENT	dxstaff@up.edu.ph **sent** a signature request to: • Peter Sy (pasy@up.edu.ph)	2025/12/05 04:07:33 UTC
SIGNED	**Signed** by Peter Sy (pasy@up.edu.ph)	2025/12/05 04:29:38 UTC
COMPLETED	This document has been signed by all signers and is **complete**	2025/12/05 04:29:38 UTC

The email address indicated above for each signer may be associated with a Google account, and may either be the primary email address or secondary email address associated with that account.