# Program on Cyber Security Studies (PCSS)

## Resident Course and Outreach Activities

Provide an overview of cyber security key themes within the construct of strategy development, policy, legal frameworks, international cooperation, development and management of cyber defense. Priority themes include:

- Capacity Building
- Citizen Awareness
- Combating Cyber Crime
- Critical Infrastructure Protection
- Cyber Risk Management
- Understanding Cyber Threats
- Cyber Security Workforce Development
- Incident Response
- Information Sharing
- International Laws and Norms
- Internet Freedom
- Internet Governance
- Military Characteristics
- Privacy and Security
- Public-Private Partnerships
- Standards and Development Management
- Strategy and Policy Development / Implementation
- Training and Exercises

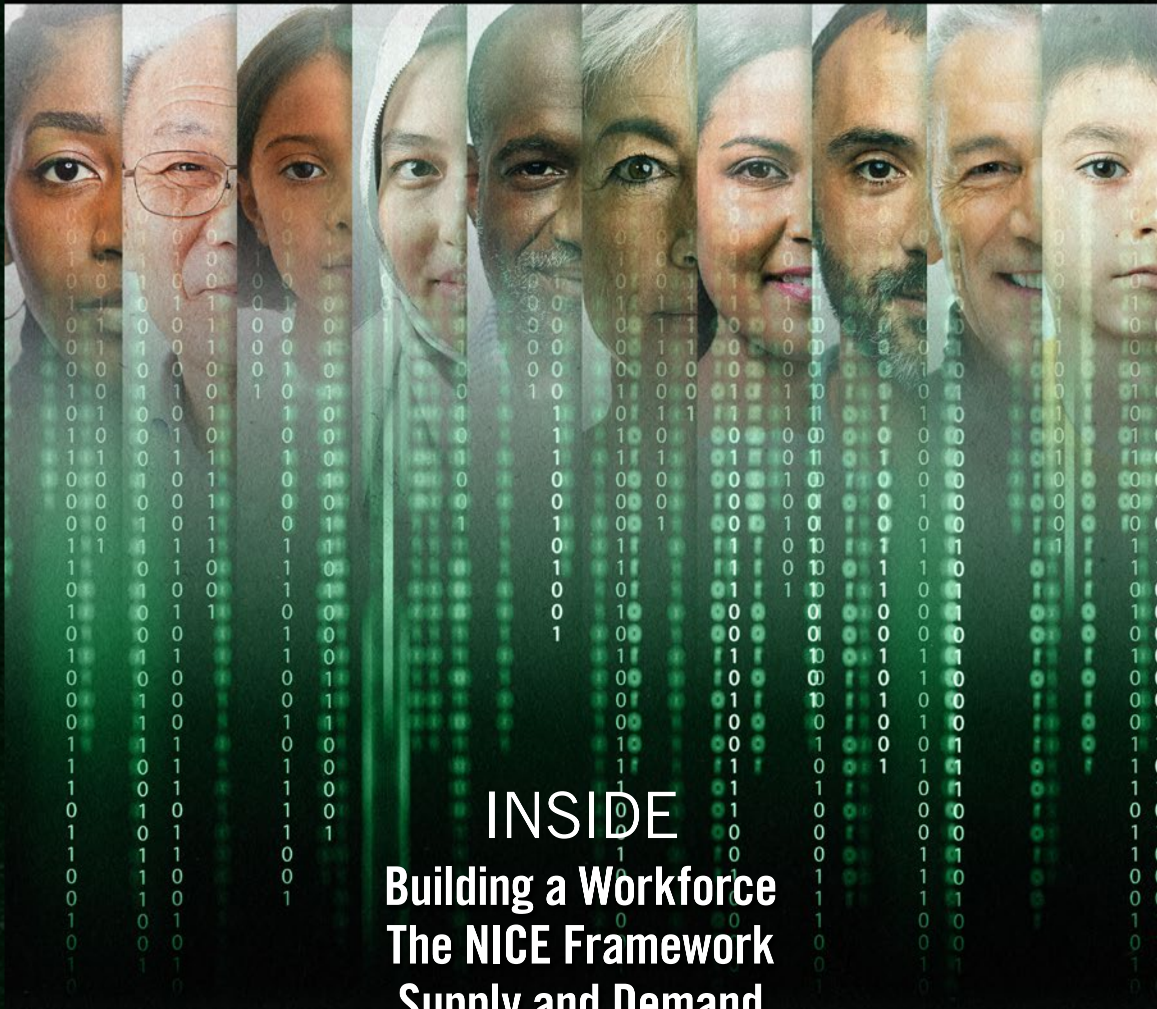
## Participant Objectives

- Increase capacity to address transnational cyber security challenges.
- Understand cyber threats and collective approaches.
- Enhance regional and global information sharing to include sharing of best practices.
- Evaluate and incorporate improved whole-of-government approaches for developing cyber strategies and policies, along with implementation action plans.
- Ensure inclusion of private industry in governmental activities and dialogue.
- Share Euro-Atlantic and public-private partnership proposals for addressing asymmetric threats from nonstate actors.
- Understand threats, collective approaches and principles to evaluate key considerations when developing a national cyber strategy.
- Foster an environment of cyber due diligence.
- Facilitate a global network of senior-level cyber security professionals.
- Increase awareness and implementation of cyber security norms development and confidence- and security-building measures.

For more information contact the Marshall Center Registrar at:
registrar@marshallcenter.org

per Concordiam
Journal of European Security and Defense Issues

# SPECIAL CYBER SUPPLEMENT



INSIDE

**Building a Workforce**
**The NICE Framework**
**Supply and Demand**

# Cybersecurity Month

## European Cybersecurity Month

Enhancing citizen awareness in cyber security

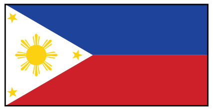
### The objectives of the European Cybersecurity Month are to:

- Generate general awareness about cyber security, which is one of the priorities identified in the EU Cybersecurity Strategy.
- Generate specific awareness on Network and Information Security (NIS), which is addressed in the proposed NIS Directive.
- Promote safer use of the internet for all users.
- Build a strong track record to raise awareness through the ECSM.
- Involve relevant stakeholders.
- Increase national media interest through the European and global dimension of the project.
- Enhance attention and interest with regard to information security through political and media coordination.

**As a direct target of cyber security attacks during the COVID-19 pandemic, the health care sector needs to be vigilant.** #StayAtHome #Covid19 For advice see our infographic at enisa.europa.eu/WFH-COVID19

**Businesses face significant financial loss when a cyber attack occurs.** Cyber criminals often rely on human error — employees failing to install software patches or clicking on malicious links — to gain access to systems. From senior leadership to the newest employee, cyber security requires the vigilance of everyone to keep data, customers, and capital safe and secure. #BeCyberSmart to connect with confidence and support a culture of cyber security at your organization.

## The Philippines National Cybersecurity Month:



The 2019 national cybersecurity month's awareness campaign was built around the theme: **I Am Secure 2019: Industry 4.0, with a notable tagline of "Information Security Professionals in the Midst of the Digital Tsunami."** Our country is on the brink of a global phenomena, facing grand-scale changes that influence everyday lives, communication, and consumption of goods — technology-wise. The Information Security Officers Group (ISOG) believes that updating fellow security officers about innovative models, frameworks and alternative sources in response to the Fourth Industrial Revolution is a pressing concern. The conference presented a collaboration of great minds and ideas to prepare the Philippines for the changing times.

## Further information:

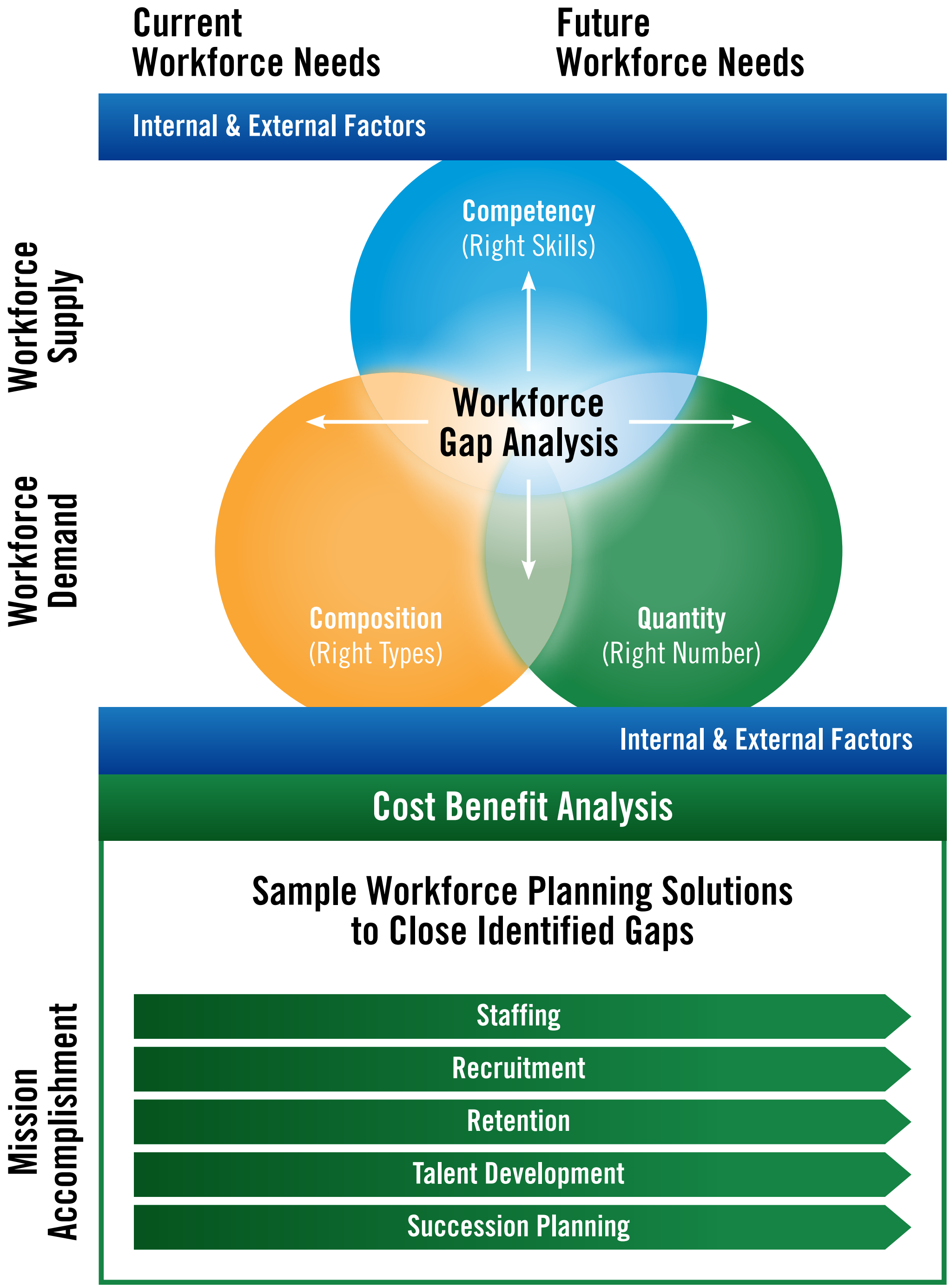
https://www.cisa.gov/national-cyber-security-awareness-month

https://www.getcybersafe.gc.ca/cnt/rsrcs/csam/thms-en.aspx

https://cybersecuritymonth.eu/

https://www.enisa.europa.eu/topics/cybersecurity-education/european-cyber-security-month

## Analyzing Requirements



Current Workforce Needs

Future Workforce Needs

Internal & External Factors

Workforce Supply

Workforce Demand

Competency (Right Skills)

Workforce Gap Analysis

Composition (Right Types)

Quantity (Right Number)

Internal & External Factors

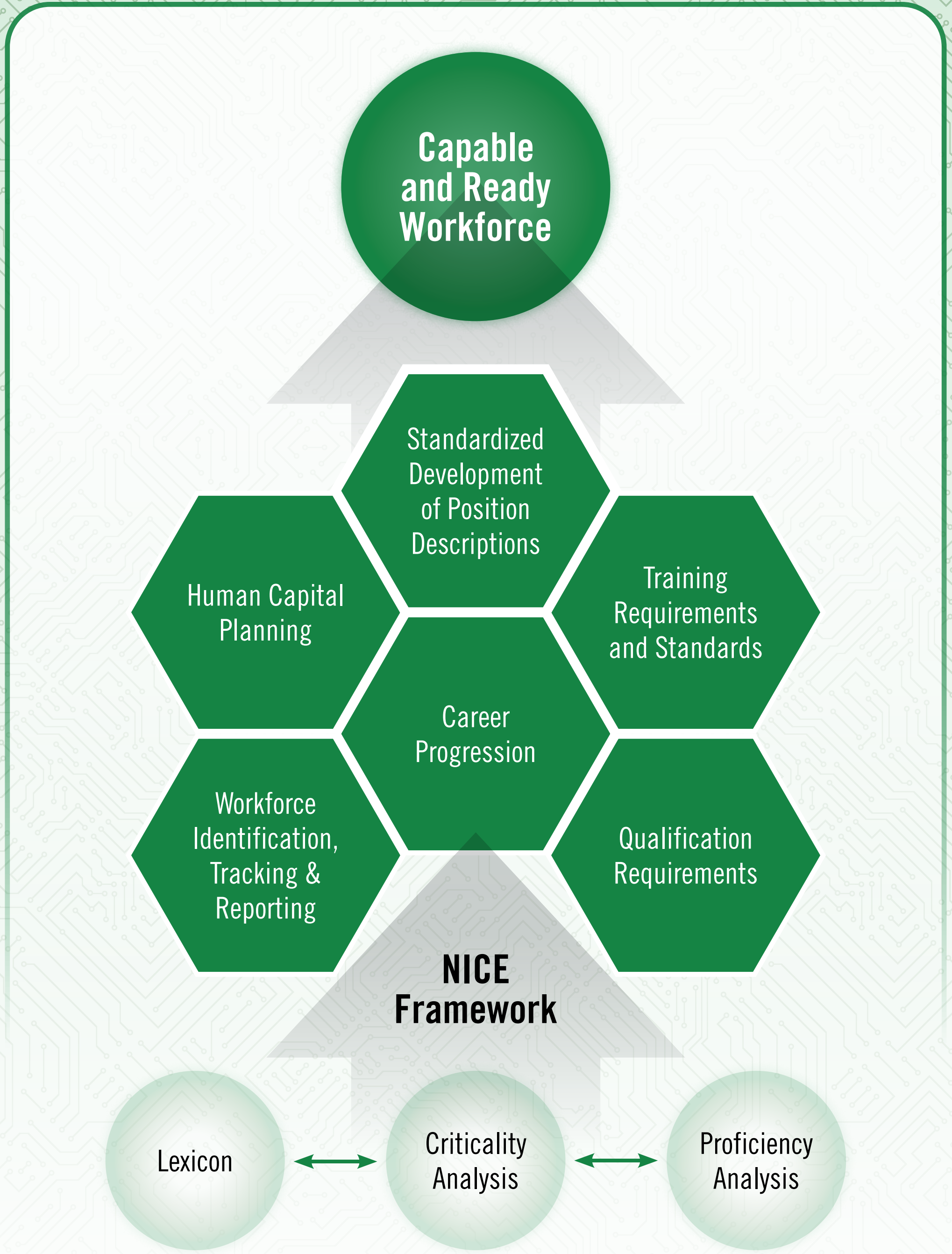
Cost Benefit Analysis

Mission Accomplishment

Sample Workforce Planning Solutions to Close Identified Gaps

- Staffing
- Recruitment
- Retention
- Talent Development
- Succession Planning

## Building Blocks for a Capable and Ready Cyber Security Workforce



Capable and Ready Workforce

Standardized Development of Position Descriptions

Human Capital Planning

Training Requirements and Standards

Career Progression

Workforce Identification, Tracking & Reporting

Qualification Requirements

NICE Framework

Lexicon ⟷ Criticality Analysis ⟷ Proficiency Analysis

# BSI – Federal Office for Information Security

Federal Office
for Information Security

**The BSI is a German federal agency.** It provides information on risks and threats relating to cyber security and develops preventive measures. This work includes IT security testing and assessment of IT systems, including their development, in cooperation with industry. (https://www.bsi.bund.de/EN/TheBSI/thebsi_node.html)

## Certification for Persons

- Primarily to support certifications/evaluations the BSI is conducting.
- Required for employees of a BSI-certified IT security contractor
- Categories: IT-GS-Berater/IT basic protection advisor, information security auditor and advisor, information security penetration tester and more.
- Evaluation phase + certification phase (3 years, control of competence, potential exchange of experiences).

### Allianz für Cybersicherheit

Alliance for Cyber Security

- BSI initiative
- Training, workshops, analysis and penetration tests. Further education in the Training Center Network Defense
- Exchange of experiences and expertise

### BSI ACS Übungszentrum Netzverteidigung

Training Center Network Defense

In the Training Center Network Defense, 24 participants complete modules regarding vulnerabilities of different IT components and applications over the course of five days.

# TeleTrusT – IT Security Association Germany

TeleTrusT
Pioneers in IT security.

**TeleTrusT** is a widespread competence network for IT security comprising members from industry, administration, consultancy and research as well as national and international partner organizations. TeleTrusT provides interdisciplinary fora for IT security experts and comments on technical, political and legal issues related to IT security, and is an organizer of events and conferences. TeleTrusT carries the “European Bridge CA” (EBCA; PKI network of trust) and provides the trust seal “IT Security made in Germany.” (https://www.teletrust.de/en/startseite/)

## Training and Certification

- **T.I.S.P TeleTrust Information Security Professional**
  Focuses on the international aspects, but also BSI Baseline Protection Catalog (IT-Grundschutz) and European and German law

- **T.P.S.S.E TeleTrusT Professional for Secure Software Engineering**
  Focuses on how to complement software development with security aspects.

### Cyber Security Challenge Germany

- Pupils and students age 14-25
- Identify and nurture “qualification potential” in IT security
- Facilitates contact to private industry

### Promotion of young talent

Education, startups, women in IT, hacking competitions, fair stands, events to connect young talents and industry