Funded
by the European Union
and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Implemented
by the Council of Europe

INTERPOL

GUIDE FOR DEVELOPING

LAW ENFORCEMENT TRAINING STRATEGIES

ON CYBERCRIME AND ELECTRONIC EVIDENCE

March 2022

Prepared by
Cybercrime Programme Office
of the Council of Europe (C-PROC)
and
INTERPOL Cybercrime Directorate

Acknowledgement

The present *Guide for Developing Law Enforcement Training Strategies on Cybercrime and Electronic Evidence* was prepared under the Global Action on Cybercrime Extended (GLACY+) and the CyberSouth joint projects of the European Union and the Council of Europe. The work on this document was coordinated by the Cybercrime Programme Office of the Council of Europe (C-PROC) and the INTERPOL Cybercrime Directorate, and contributions were received from the following experts: Lim May-Ann (Singapore), Terry Baker (United Kingdom) and Victor Völzow (Germany). A total of 59 INTERPOL members responded to the survey on cybercrime training strategies (Appendix I).

Contact

Cybercrime Division
Council of Europe Directorate General Human Rights and Rule of Law
F-67075 Strasbourg Cedex (France)
E-mail: cybercrime@coe.int

INTERPOL Cybercrime Directorate
INTERPOL Global Complex for Innovation
18 Napier Road
Singapore 258510
E-mail: EDPS-CD@interpol.int
Twitter: @INTERPOL_Cyber

Disclaimer

The views expressed in this technical report do not necessarily reflect official positions of the Council of Europe, of the European Commission, of INTERPOL or of the Parties to the treaties referred to.

Table of Contents

ACRONYMS

CEPOL	European Union Agency for Law Enforcement Training
CERT	Computer Emergency Response Team
CoE	Council of Europe
CSIRT	Cyber Security Incident Response Team
DFIR	Digital Forensics, Incident Response
ECOWAS	Economic Community of West African States
ECTEG	European Cybercrime Training and Education Group
EJTN	European Judicial Training Network
Eurojust	European Judicial Cooperation Unit
Europol	European Law Enforcement Organization
G2B	Government to Business
G2G	Government to Government
GLACY+	Global Action on Cybercrime Extended
INTERPOL	International Criminal Police Organization
IP	Internet Protocol
KMS	Knowledge Management System
KPI	Key Performance Indicator
KSA	Knowledge, Skills, and Attitudes
LEA	Law Enforcement Agency
LMS	Learning Management System
M&E	Monitoring and Evaluation
MLA(T)	Mutual Legal Assistance (Treaty)
OSINT	Open-Source Intelligence
R&D	Research and Development
ROI	Return on Investment
SMART	Specific, Measurable, Achievable, Relevant, Time-Bound
SOP	Standard Operating Procedure
SWOT	Strengths, Weaknesses, Opportunities, Threats
TCF	Training Competency Framework
TNA	Training Needs Assessment
UNODC	United Nations Office on Drugs and Crime

EXECUTIVE SUMMARY

Criminal use of technology is constantly evolving, with offenses committed at ever greater volume, speed and reach. Therefore, law enforcement agencies (LEAs) are under constant pressure to keep abreast and renew their knowledge and skills on cybercrime and electronic evidence. As the challenges are multifaceted, LEAs must take numerous actions simultaneously: training, recruiting, researching, investing in tools and equipment, and others.

A strategy to efficiently obtain and maintain multi-layered knowledge and skills on cybercrime and electronic evidence is a crucial part of a holistic response to cybercrime and the challenges of electronic evidence. A 'roadmap' plan that sets such goals and ways to achieve them can help direct actions and maximize impact. The plan must ensure flexibility as technology evolves: organizations must adopt an open, continuous process to detect and accommodate such changes.

INTERPOL and the Council of Europe present this Guide for Developing Law Enforcement Training Strategies on Cybercrime and Electronic Evidence to help LEAs coordinate their efforts for capability development. The guide proposes a systematic, step-by-step approach to creating, implementing and managing a training strategy, including: setting up the strategy team, assessing the current conditions, building a strategic framework, devising actions, implementing actions, measuring the outcomes, and monitoring the strategy. This structured approach helps to avoid a fragmentation of efforts, confusion and waste of limited resources.

Building and managing a strategy does not necessarily mean that all actions, programmes and projects need to be mapped out completely. Rather, a strategy provides a framework under which specific actions and sub-programmes can be developed. Those implementing the strategy, participating units and other stakeholders can contribute with confidence when this framework is rooted in evidence and efficiently communicated as a shared process. Both the framework and actions under it must stay open for revision.

The steps for developing a training strategy presented in this guide must be adapted to the specific circumstances and needs of each organization to ensure a robust, agile and realistic strategy. We encourage readers of this guide to take leadership in building and managing self-driven strategies within their organizations. We hope it will help law enforcement officials in strategic planning departments, police training institutions, cybercrime units, digital forensics units, and other relevant departments in their continuous effort to improve capabilities on cybercrime and electronic evidence.

1 INTRODUCTION

A well-developed strategic plan can play a pivotal role in responding to multi-layered, complicated problems such as cybercrime and electronic evidence. However, the mere existence of a strategic document is not enough: strategies are only useful when they become the part of organization's culture through continuous communication among its members and stakeholders. To be effective, strategies must also be rooted in – and respond to – the needs of the organization, which should be identified on the basis of broad-based consultations with relevant stakeholders. See **Appendix A** for a brief questionnaire for assessing existing strategic plans.

1.1 Capacity building on cybercrime and electronic evidence

Before discussing how to build a training strategy, it is useful to introduce some key terms and concepts.

Capacity building is a multi-layered and gradual process enabling individuals and institutions to improve their performance through enhanced skills and knowledge, tools, equipment, connections, processes, and other resources needed to do their jobs competently. Capacity building implies a gradual process of change towards a desired performance in areas such as the following:

- **Planning and policy capacity** is how organizations choose a course of action with limited resources and conditions. Robust planning with a strong strategic attitude is a good example.

- **Legal capabilities** protect human rights while giving LEA the legal tools necessary for crime deterrence and investigation. National legislation compatible with the Budapest Convention on Cybercrime provides substantive and procedural grounds for criminal investigations.

- **Institutional competencies** cover the capabilities of specialised units in cybercrime and electronic evidence: structural setup and responsibilities, staffing and training, analysis tools, Standard Operating Procedures (SOPs) and cooperation mechanism including crime reporting and statistics, etc.

- **Knowledge and skills** of the LEA professionals is central to all other competencies and are obtained through training, job experience, self-study, recruitment, organizational knowledge management, etc. Knowledge and skills are the core components of learning objectives: training often wanders without direction without them clearly itemized.

- **Cooperation capacity** implies organizational ability to work with other entities such as (1) ability to collect and share data securely, (2) organization's trust profile and practices upon which others grant to each other, (3) capability of the entire cooperative group or network itself, (4) ability to apply oversight through communication with the judicial authorities.

- **International cooperation** implies the ability to work and collaborate internationally such as (1) participation in bilateral/multilateral legal framework or partnership such as Budapest Convention, (2) participation in operational platforms such as INTERPOL or 24/7 networks, (3) participation in policy initiatives, dialogues, and activities led by international organizations such as the Council of Europe, European Union, United Nations Office on Drugs and Crime (UNODC), INTERPOL, etc.

Knowledge and skills can be developed partly through training. In this sense, **training** is a sub-component of capacity building and includes planning, organization, and delivery of training sessions

intended to enhance the knowledge and skill of individuals or organizations. Training is an ever-evolving process where specific development and delivery method applies.

Training strategies are structured plans to acquire desired knowledge and skills through training and other related activities as part of an organizational capacity building effort. It has a multi-layered scope linked to various non-training areas such as cybercrime policy, legislation, human resources management, or international cooperation.

Training is an ever-evolving process, including the planning, organizing, and delivering training sessions. For practitioners engaged in standalone training courses, we recommend another guide for in-depth knowledge on instructional design: INTERPOL's Guide on Effective Training (2018).

1.2 Benefits of being strategic

Being strategic means that an organization's actions are constantly reviewed against its mission and current conditions. Activities and sub-programmes are devised based on clear objectives and the operational environment. The process is cyclical and iterative, incorporating new issues to ensure continuous development.

A strategic approach has several benefits:

- An organization can draw the roadmap to attain its goals, maximize resources, minimize conflict, prepare for contingencies, and be resilient to change through environmental scanning.
- Cyclical review ensures continuous, agile, and adaptive development - one which is customized for the organization's own needs.
- Encouraging broader participation in planning brings about a results-sharing system among individuals. A centralized decision-making system has a shallow impact on individuals.
- Multi-stakeholder engagement prevents a siloed approach towards cybercrime training. It promotes a coherent approach, rather than a piecemeal, individual-agency approach.
- Self-development of plans removes dependence on external assistance. Externally assisted activities will be planned within the framework of their own training strategies.
- Finally, it invites others to participate and cooperate more openly. Other LEAs and international organizations can easily understand the strategies and identify synergies by mapping and cross-fertilization of programmes.

1.3 Costs of not acting strategically

The lack of a strategic approach may lead to (1) duplication of work or inefficient allocation of resources, (2) uneven, inconsistent, or siloed training, (3) impossibility to assess the impact of actions, (4) lost opportunities to produce synergies or learn from interactions.
The following scenarios capture some of the consequences of not planning and acting strategically:

- A police organization opens a new digital forensics lab (DFL) in the absence of a first-responder's programme that allows electronic evidence to be collected at crime scenes. As

there was insufficient field staff with evidence collection skills and knowledge, the lab experts had to be called up to attend crime scenes.

- A fraud investigation agency is looking for e-evidence training for its staff. It does not have a training institution and searches for other government training institutions. It learns that there is a cybercrime course offered at the central police school. When asked, the school replied it is a 5-day course on cybercrime, but no further details. The school actually does not know what is taught in the class because they were fully dependent on the instructors to formulate and deliver the course.

- A manager of a cybercrime unit thinks every staff member must be trained in cybercrime and electronic evidence. To provide equal opportunity for his staff, he takes a round-robin approach for each training invitation, which usually comes from external partners. After five years, all his 30 staff were trained in cybercrime training of various topics overseas. He is not sure if these numbers actually mean capabilities were improved, and he finds it is difficult to elaborate on the contents of the improvement.

- An organization invests in data visualization systems because many experts say data analysis is the key to next-generation law enforcement. The manager finds out that all her staff is using spreadsheet tools and not the new data analysis system. It was because the amount of data flowing into her team was too small and so the system had little value. The legal department says her team is not allowed to receive and share such data according to the law on data protection.

Cybercrime and electronic evidence pose multifaceted legislative, institutional, and operational challenges. Adopting existing best practices can be helpful in general, but blindly importing them into an organization may not reflect reality. For an LEA to be truly strategic, it must constantly be aware of its own environment while examining past experiences.

2 FINDINGS OF THE SURVEY

In August 2021, a Survey on Training Strategies was sent to the INTERPOL National Central Bureaus of member countries. 321 LEA officers responded, and 246 responses from 59 countries that had country affiliation were used for analysis (**Appendix I**).

Below are some findings, expressed on a scale from 1 (strongly disagree) to 7 (strongly agree).

- While officials were more aware that the strategic plans existed (3.64), they perceived that those plans were less/not effectively communicated throughout the organization (3.04) and that the methods for measuring the impact were insufficient (2.94).

- Officials agreed more on that the strategic plans exist (3.64), but less on that the strategies are well communicated throughout the organization (3.04), and that the methods are established for measuring the impact (2.94).

- Similarly, officials think that training and education plans are ‘documented’ (3.29) but are less implemented in practice (2.98).

- Officials feel the organization is putting more emphasis on generating strategic options (3.38) and less on developing long-term objectives (2.96) or gaining employee commitment (3.01).

The respondents agreed that strategic planning is produced in many countries, while the impact of its implementation is somewhat limited. A good strategic plan should have a good balance between proclaiming its plans and producing actual outcomes.

3 STEPS FOR DEVELOPING THE TRAINING STRATEGY

The focus of this guide is to introduce general steps for training strategy: a two-phase, 7-step cyclic approach towards building and implementing strategy. It is not to be interpreted as a 'one-size fits all' method: we encourage flexible and creative customization.

Figure 1: Steps for building a cybercrime training strategy

The developers of a strategy must consider implementation. A good strategy clearly communicates how each department will contribute by informing them how best to direct resources in output-oriented language. Details are not a focus of training strategy: as they are for the implementors to plan and execute. The implementor's engagement at the development phase is crucial for reality. It must be reasonably easy for the implementors to align the strategy with their short- and long-term plans.

3.1 Setting up the team (Step 1)

An organization needs a team that will develop and manage a strategy. Team set-up depends on the management style of an organization. We have outlined typical steps such as team initiation, identifying stakeholders and their roles, and creating a plan to start the process.

3.1.1 Strategy team

A strategy team is responsible for developing and managing the training strategy. It may have various forms and structures, depending on the decision-making practice of the organization. A strategy team must engage representatives from the organization's management and decision-makers, including training institutions, units specialized in cybercrime or digital forensics, and supporting units such as finance or budget. In some cases, these members may form a separate, ad-hoc, special committee that will guide the strategy team of practitioners and experts. External stakeholders may participate as part of the team, special committee, or separately in several stages of developing and implementing the strategy.

Before starting with the formal constitution of the team, there must be an agreement on its purpose and scope. It will include organizational commitments in terms of staff hours for exploring strategic choices and administrative resources for the team's operation, such as office space and equipment.

A leader is designated once organization sets the initial scope of the strategy team on a management / political level. That person will have the task of leading the strategic planning, coordinating the work of the team and representing the strategy externally and internally. The leader may be responsible for designating other members of the strategy team, taking into consideration existing hierarchies, responsibilities, and professional expertise.

The team needs to dedicate sufficient time for frequent meetings and workshops because it will be essential to communicate with stakeholders and partners. Frequent internal communication is needed to create a strategy tailored to the specificities of the law enforcement units, while external communication will help identify synergies and create partnerships.

3.1.2 Stakeholders

It is crucial to identify stakeholders who will support and benefit from the strategy from the inception. Stakeholders exist internally and externally. In general, anyone affected by the training strategy, potential supporters and implementors, should be considered: political and strategic decision-makers, officials in the police training institutions, units specialized in cybercrime and digital forensics, human resources and training, strategic planning department, and partners.

Staffs who are the potential trainee should also need to be invited. They include practitioners in the specialized units, first responders, crime investigators, and partner authorities. Furthermore, the general public may be considered an external stakeholder as potential victims of crime.

An example of a stakeholder analysis result can be found in the **Appendix B** to keep track of the progress made and information gathered from each stakeholder. The result of stakeholder analysis would include information on the stakeholder's point of contact, roles, associated profiles, priorities, and potential contributions to the strategy, and a plan for engaging them.

3.1.3 Working group

The strategy team may form a larger working group among the identified stakeholders, which will meet regularly and actively influence the work of the strategy team. While external partners may contribute with their advice, guidance, and suggestions, the strategy itself needs to focus on the needs of the internal stakeholders that will form the core of the working group.

3.1.4 Collaboration with partners

Collaboration is more than simply cooperating with other teams, departments, or organizations; it involves a shared vision, respect, and in-depth understanding of each other's role to achieve excellent business outcomes. It encourages sharing information, knowledge and skills for shared objectives, creating an environment for continuous learning and development.

Collaboration leverages strengths and supports success. Seamless and effective collaboration between departments and organizations requires effort and sometimes changes at the leadership and cultural level; however, the work involved in making those changes can produce transformative results.

Police-academia partnerships provide opportunities for greater specialized skills and sustainable knowledge transfer by bringing together a diverse group of academic researchers. The partnership can also provide opportunities for research and development (R&D) in forensic science. It also provides key resources toward professional accreditation of courses developed under the training strategy.

Police-private sector partnerships provide opportunities for collaboration that can lead to greater efficiency and an opportunity to draw from specialized skills, software, platforms, research, and training that support law enforcement. One example of such cooperation is the recent partnership of the UK police with the Cisco Networking Academy[1] to launch a nationwide initiative to provide access to cybercrime training for 120,000 officers, both in-person and online.

Collaboration with international organizations provides opportunities for collaboration in training. Regional and international organizations who provide support to law enforcement tackling cybercrime include: INTERPOL, Council of Europe, UNODC, European Cybercrime Training and Education Group (ECTEG), Organization of American States (OAS), African Union Convention (AUC), European Cybercrime Center Europol, NATO Cooperative Cyber Defence Centre, International Cyber Security Protection Alliance (ICSPA), International Association of Internet Hotlines (INHOPE) and Internet Crimes Against Children (ICAC) Task Force.

3.1.5 Initial Preparation

The strategy team's mission is to develop a training strategy that will address the needs of the stakeholders. The strategy must consider the existing boundaries of the national strategies and policies when defining its own strategic goals and objectives. The team needs to lay out the plan for drafting the strategy. If a plan is not in existence at this stage, the team's very first task is to identify existing policies and actions.

In the initial preparation meeting(s), the strategy team should lay out:

[1] https://cisomag.eccouncil.org/cisco-to-train-120000-uk-police-officers-on-cybersecurity/

- current strategies, policies, or regulations that directly affect the process (if any), including the external timeline, milestones for the entire process;

- the methodologies to identify stakeholders, partners, and the status quo in terms of training on cybercrime and electronic evidence;

- the methodologies to assess the vision and the strategic objectives of the strategy;

- an agenda of meetings for the strategy team, the working group and liaising with stakeholders and partners;

- the roles and responsibilities of the individual team members (including clear responsibilities for internal/external communication), as well as tasks for the team members connected with deadlines;

- the collaboration tools/platforms used to draft the strategy.

3.2 Assessing current conditions (Step 2)

Before any actions can be defined or solutions discussed, it is essential to understand the current technological and organizational environment. Visualizing this picture of the "status quo" will help identify weaknesses, gaps, and current limitations that need to be addressed.

3.2.1 External environment

External environmental factors strongly impact training strategy and the LEA's motivation behind it.

LEAs should carefully examine the environment in which it operates. Examples include:

- **Criminal phenomena** should be observed more closely. What are current and upcoming trends of technological developments and cybercrime modus operandi? Is there a drastic change in the landscape? Does the observer have sufficient visibility, or does it depend on others' observation? What do crime statistics indicate?

- **People** should be considered. Do people report perceived crimes? What stops them from reporting? What prevents the awareness of being victimized? Who will be impacted by the training strategy other than the learners?

- **Conditions surrounding the organization** limit strategic choices. What is the scope of the strategy? Can it be broader or narrower? Which channels of international cooperation are available? Are there potential partners or competitors? What is the current situation in the cyber security industry? Are there any expectations of others in terms of roles or performances?

- **Capabilities of external entities** provide insights on areas of potential cooperation. Some entities have capabilities to detect dormant or latent criminal activities, while some entities have capabilities to prevent or flag certain types of financial transactions. Other law enforcement and international organizations may have unique capabilities. Are there existing training courses offered by any entities? What are the existing public-private partnerships?

- **Existing laws and policies** should be carefully examined. Laws and policies will define the crime and empower the agency to investigate and cooperate. Some regulations may prevent collecting specific data or mandate certain processes before collection.

3.2.2 Internal environment

A good assessment of the external environment provides a reliable baseline for further analysis of the internal conditions. For internal environment scanning, the strategy team can use SWOT (Strength, Weakness, Opportunities, and Threats) analysis to understand the current approach better. What are the weaknesses and threats, and what strengths and opportunities are relevant to the weaknesses?

A mapping of the internal environmental must be an honest, objective, and thorough assessment of the organization, including the people, resources, culture, and practices. Any 'inconvenient truths' must be identified and communicated earlier for more realistic stages.

One methodology is to map out the organization's needs and take stock of the resources and opportunities available through SWOT analysis. A simplified example is depicted in the below diagram.

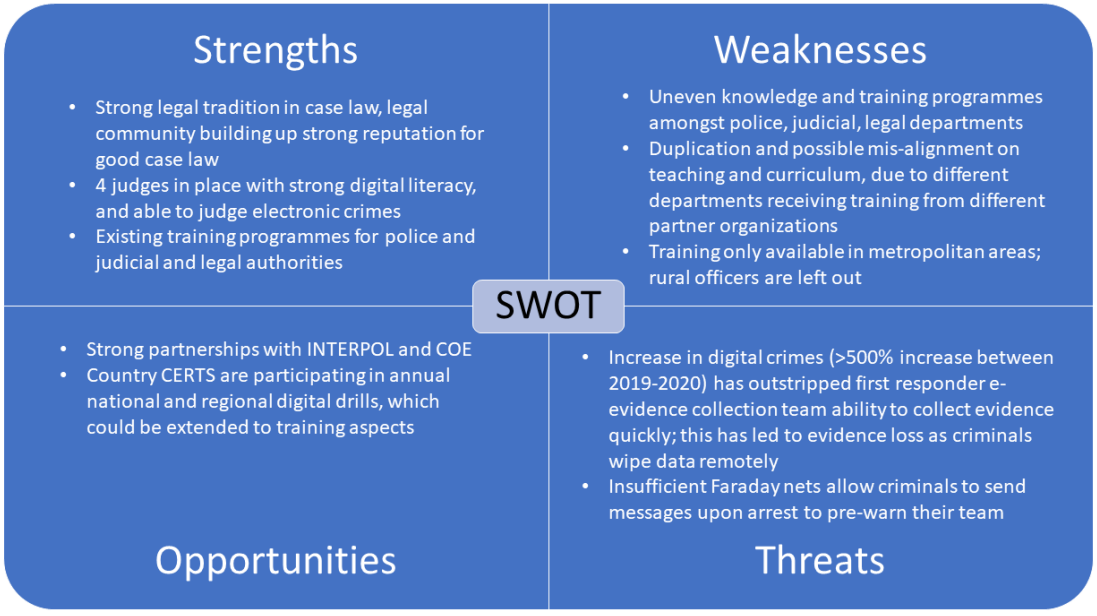


Figure 2: SWOT Analysis

3.2.3 Existing capabilities

Knowing what is there to know is a fundamental element for planning and defining what needs to be taught. Traditional police training institutions could produce training catalogues unilaterally within the organization. However, it is less straightforward for complex and ever-evolving topics such as cybercrime and electronic evidence. Institutions may need help from multiple stakeholders in listing knowledge and skills needed for law enforcement. The list changes: digital transformation is multidisciplinary and rapid, and the next criminal exploit and corresponding law enforcement capabilities develop with time.

Training institutions have widely accepted the training needs analysis (TNA) as a practical method of understanding what needs to be taught. However, the LEA should also be aware that field officers' TNA responses may not provide sufficient data in some technical areas: they may indicate some deficiencies in capabilities, but the field officers may not know what technological countermeasures are available.

In-depth interviewing of practitioners in the fields can be considered for landscaping capabilities. It is also a good practice to perform a comprehensive stakeholder assessment: identify key managers and partners interested in the success of the training strategies. These stakeholders can be key allies in supporting and advocating for the training and development plan as well as obtaining consensus from the senior leadership of the organization.

Gathering information can be time-consuming and involves desktop research and external communication. It is worth investing the time in this initial stage because the data gathered will help describe the "status quo" and identify opportunities, potential synergies, and partners that may become part of the training strategy.

3.2.4 Needs assessment

Each group of stakeholders will have their demands, wishes and objectives. The strategy team needs to liaise with them by grouping similar profiles together (e.g., cybercrime analysts and intelligence officers with online investigators). Stakeholders can be potential recipients of training, or they can also be partners in developing and implementing the strategies. Some external stakeholders may help in delivering training courses, undertaking research, or providing trainers or training materials. Others may perform joint operations or provide information or intelligence.

Joint workshops with different profiles can be helpful when several profiles exist within the same organizational structure (e.g., a cyber-unit with an included intelligence section and a forensic laboratory). It will facilitate a cross-check and review of the profiles and the associated skill requirements from different perspectives.

In the workshops and surveys with stakeholders who will be beneficiaries of training or even training paths and curricula, it is important to get an understanding of:

- Required capabilities, knowledge, and skills. These are the performance enabler that we want to develop through training, and they must be expressed in clear and plain language. Still, abstract terms are unavoidable for more theoretical and fundamental knowledge (e.g., required capabilities or knowledge for forensic analysts will be much more inclusive.)

- The volume of the potential trainees in numbers. It will shape the implementation method: a small number of participants (e.g., digital forensic examiners) may be trained in a centralized classroom, while larger groups (e.g., first responders) need scaled approaches such as e-learning or training-of-trainers programmes.

- The expectations and demands of other stakeholders. For example, the DFL experts may want the first responders to adopt specific procedures. The Cyber Security Incident Response Team (CSIRT) analyst may want the police officer to take specific actions for more information to be accessed. The prosecutors may advise tightening certain practices to the police evidence handlers.

One example of understanding stakeholders and their needs is illustrated in the Training Competency Framework 2.0 (TCF)[2] which defines key profiles and competencies associated with them.

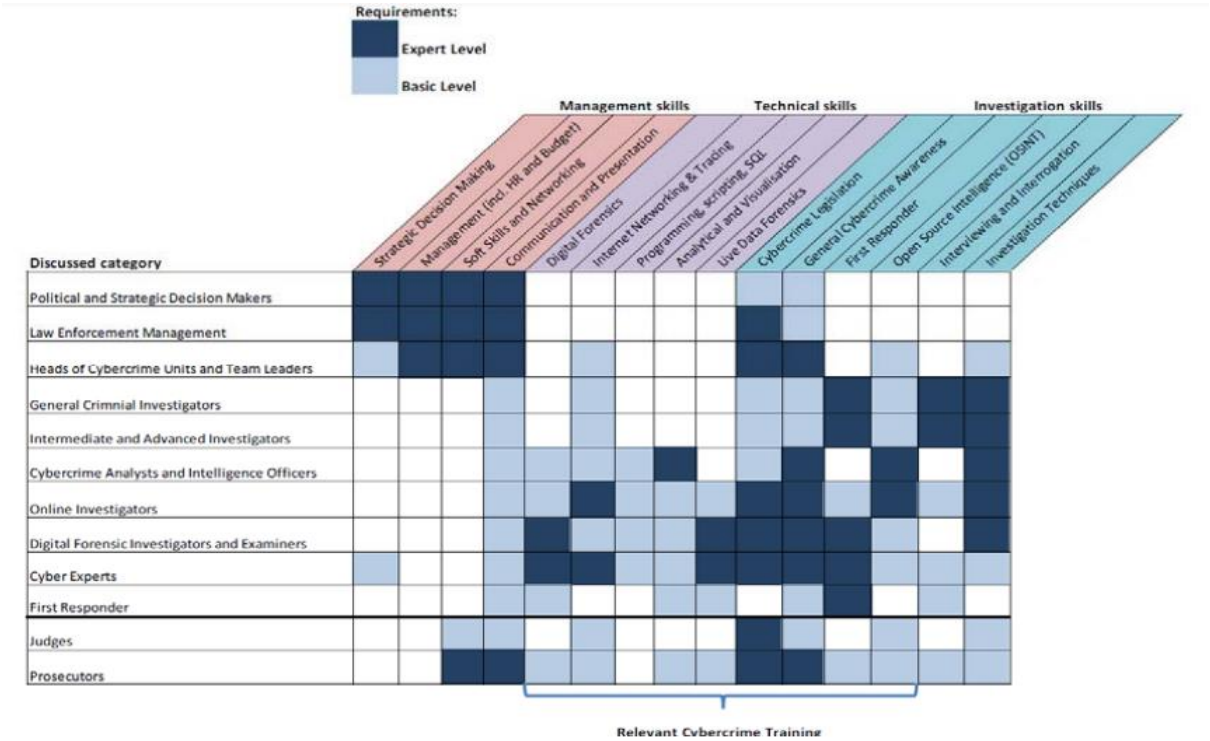


Figure 3: Competency Table, TCF Framework 2.0

Involvement of the stakeholders in the process will help create a training strategy tailored to the stakeholder's professional requirements and is more likely to be accepted by the stakeholders. Workshops with potential target groups and external stakeholders can help the strategy team identify existing solutions and potential synergies with future partners and trainers.

3.3 Building the strategic framework (Step 3)

A simple strategy may list action items without apparent structure, but complicated plans need a logical and plausible structure. Many organizations arrange strategic elements in a structure with **goals** giving logical directions of the sub-components.

Terms such as goals, objectives, target, outcome, or result are interchangeable as they all describe the aim of effort. This practice is suitable for simplicity, but they can be differentiated to describe a varying range of scope.

[2] Developed by European Union Agency for Law Enforcement Training (CEPOL), Eurojust, Europol, European Judicial Training Network (EJTN) and the European Cybercrime Training and Education Group (ECTEG)
https://www.cepol.europa.eu/sites/default/files/OTNA_Cybercrime_Attacks_Against_Information_Systems_2019.pdf

We can think of **three distinct layers** in a typical structure. **(1) High-level aim** provides overall directions. **(2) Mid-level aim** contributes toward high-level aims, and they are more area-specific and easier to measure. **(3) Actions** are the actual activities that help achieve the aims.

These three layers are logically connected. In the example below, we will use 'goal' for high-level and 'outcome' for mid-level. Strategic plans should define terms and use consistently within the same strategy.

- **Goal**: A goal is a high-level aim typically achieved when a set of (mid-level) outcomes are met. It provides overall direction to its components and signals its relationship with external plans.

  "To strengthen the capability to tackle cybercrime and handle electronic evidence."

  "A high level of competency will be reached by implementing training programmes on cybercrime investigations and the handling of electronic evidence for all levels of police officers at our national police academy."

- **Outcome**: An outcome, or an objective, is a mid-level aim that is more specific and measurable than high-level aim. It works as a milestone for achieving a goal.

  "Specialized cybercrime units are set up in all regional branches and can perform investigation on reported cybercrimes through legally obtaining and analyzing potential electronic evidence."

  "Digital forensics labs are set up in local headquarters and can produce analysis reports on at least 80% received requests within 30 days."

- Action: An action, or activity, is a set of specific efforts that contributes toward the outcome.

  "Webinar Series on Cryptography for Criminal Justice Authorities, January 2022 for English speaking learners."

  "Workshop on developing first-responder e-learning course using INTERPOL materials"

Multiple mid-level aims have different depths and widths depending on how the team categorizes supporting actions. However, a strategy should not put disproportional weight on specific objectives: such imbalance can hurt the plan's consistency. Activities are grouped by similar categories, considering who implements the action: for example, capabilities of specialized units, processes of evidence collection and analysis, research on new technologies, legal tools, and international and public-private sector cooperation.

In the previous stage, primarily through landscaping capabilities and understanding the needs of stakeholders, the LEA could identify the gaps between desired and current capabilities. The strategy team can translate them in terms of goals and outcomes in S.M.A.R.T ways.

- **Specific (S)**: Effective goals are specific. What should be achieved by whom by which means?

- **Measurable (M)**: Progress can be known through measuring in quantity and quality. At which stage can it be considered to have been achieved?

- **Achievable (A)**: Goals and objectives should be achievable rather than aspirational desires. Reality check is based on internal and external environment scanning.

- **Relevant (R)**: The aim must be set to achieve higher-level goals or organizational mission.

- **Time-bound (T)**: The goals or objectives needs to be achievable within the timeframe of the organization.

Examples for strategic objectives are:

> *"In two years, the national police academy will have developed at least two new training courses on the handling of electronic evidence which have been delivered to at least 50 first responders."*

> *"At the end of the year 2023, training paths for cybercrime investigators will be available at the national police school, consisting of at least three training courses in the fields of cybercrime investigations, cryptocurrency investigations, and OSINT research."*

> "By May 2025, a national cybercrime innovation centre with at least 10 dedicated experts will be established. The new centre will be responsible for research, innovation and capability building in the field of cybercrime and electronic evidence."

On another note, LEAs almost always declare **a vision or mission**. It is a short but strong, inspirational statement of the organization's belief and attitude toward its roles. However, setting a vision statement is optional for strategy teams. They may skip this process or import and modify existing ones from the organization because an existing vision/mission statement can usually apply to the training strategy without modification. An example of a vision statement of the training strategy would be:

> *"To be the central agency that sets the agenda for cybercrime in the country, leading the country to be a regional and global leader in combating cybercrime."*

3.4 Planning for actions (Step 4)

Actions are movements of an organization with a specific intent, and a strategy sets out actions to achieve particular objectives by giving clear directions. Actions must be phrased in an outcome-oriented language to minimize confusion in the implementers' interpretation. Major implementors must participate in this step to ensure the execution of the strategy.

Several elements can help identify, formulate, prioritize, and structure the actions. Training strategy includes delivering classroom training and capacitating training institutions and instructors. Examples are:

- Actions that may strengthen the capabilities of educational institutions or instructors:

> *"Set up a curriculum team at the police academy with at least two experts in the field to oversee the course development and implementation according to ADDIE (Analysis, Design, Development, Implementation, and Evaluation) instructional design system."*

"Procure hardware and software for training, conduct analysis on the scale of hardware equipment to be transferred from the field offices and DFL to the training institutions."

"Set up the pool of instructors in the local agencies who will participate in development and implementation of the first responder's course."

"Establish a learning management system (e.g., in-house learning system) that will provide online trainings and record individual training history."

- Actions that may involve some type of trainings (classroom, online, OJT, etc.):

  "Revise the training course for the newly appointed cybercrime investigators according to the identified needs and quality standards."

  "Localize the INTERPOL's guide on handling of electronic evidence for first responders and execute first pilot batches with the train-the-trainer approach."

  "Participate in the training courses externally organized in high-tech areas including malware analysis, mobile forensics, and forensic challenges."

  "Deploy a technical mentorship programme for newly recruited cybercrime investigators and facilitate monthly on-the-job training (OJT) meetings in local offices."

- Actions that may change or strengthen organization's practices (HR, procurement, budgets):

  "Provide sufficient information for HR department to create and update the individual training history and propose professional development path for the investigators and analysts."

  "Develop and deploy the knowledge management plan for cybercrime and electronic evidence handling, where individual learning experience can be absorbed in the organization."

  "Co-organize an annual international workshop on cybercrime training with major stakeholders to keep the stakeholders informed of the outcome and update the strategy."

  "Implement a phased refund policy for cost-intensive external programmes to ensure that the staff are not leaving the public sector just after completing such programmes."

  "Hiring of experts or persons with a certain academic background (e.g. hiring computer science degree holders)."

Activities with similar kinds of output can be grouped under the same objectives. Avoid having too many objectives; three to five pillars are good. A strategy with ten objectives will be less accessible. Consider having three to five actions under one objective for the same reason. Multiple actions are better organized in a table, as shown in **Appendix C**.

A strategy is ready when action items are placed under corresponding pillars and supported by relevant stakeholders. Organizations can then take the procedures necessary to launch the strategy and enter into the implementation and monitoring phase.

Below, some tips and advice are provided on these action components to be more helpful. Note that these are not steps to be taken: they are advice for strategy teams and stakeholders when planning what action to take.

3.4.1 Advice 1: Triage before investing in trainings

The organization can obtain the capability through alternative actions: some capabilities are better obtained outside classrooms. It is crucial to undertake a triage assessment to assign the proper resources to actions.

The alternative methods may include a SOP, step-by-step guidelines with existing skills and abilities, on-the-job training through shadowing and mentoring, or secondments to other departments, ministries, and agencies.

Organizations should consider the cost-benefits. Technical training on electronic evidence can be expensive. Sometimes employees want training that is rarely used or require ongoing costs for software licenses that the organization cannot meet in the longer term. Other organizations and partners may already be able to provide this expertise.

The following graphic illustrates the relationship between the target group's size (left) and skills required for the roles (right). A good strategy should balance the investment made for one function (e.g., digital forensics examiners) and others (e.g., all law enforcement officers).

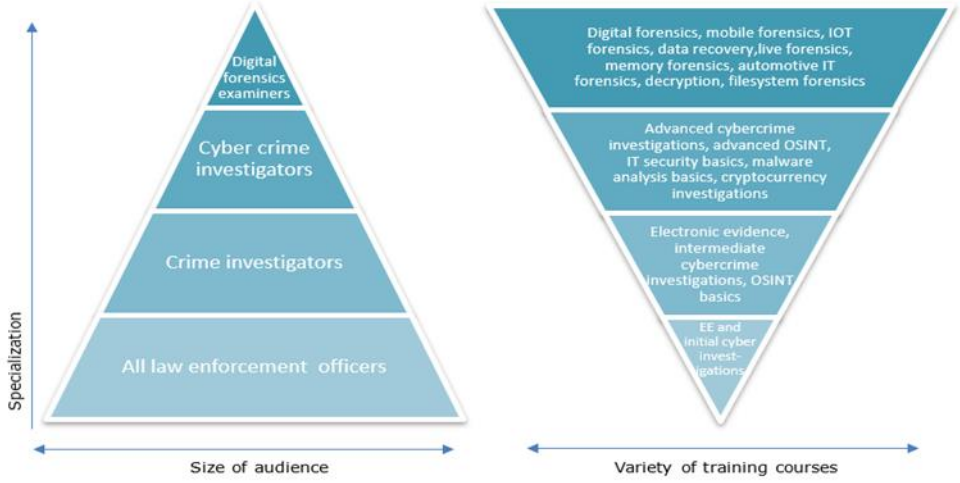


Figure 4: Roles and Training Requirements

The team may triage a training course by criticality:

- **CRITICAL:** The employee is not able to effectively undertake their role without the training; the organization or department has no expertise in a particular critical business area.
- **MEDIUM:** The organization or department has minimal resilience/or is due to losing an employee in a specific area of expertise and a critical business area; crime trends require increased resilience or recruitment in this critical business area.
- **LOW:** Development of new skills to enable more proficient working.

By balancing these factors, a short, medium, and long-term action can take place for developing the required skills. Departmental managers must take an active role together with the Human Resource, Learning & Development, or Recruitment departments to provide training and development to close these identified gaps.

3.4.2 Advice 2: Consider alternative training actions

A law enforcement organization may not have the capacity for developing and implementing the required training courses in-house. Alternative methods or a partnership with stakeholders may provide similar results. LEAs must explore alternative solutions when the size of the audience is too small to justify the development cost of in-house training, or when there are internal knowledge gaps on highly technical subjects.

Creative methods and partnerships should be considered when resources are limited. Consider the following breakdown of various formats of training:

- **Alternative delivery methods**. For **in-house classes**, the action should also consider developing, delivering and monitoring of the course. **On-the-Job training (OJT)** can be applied when audience is large. By providing learning materials and organizing learning events, organization can induce more learning. OJT approach includes internal training such as coaching, job-rotation, computer-based or interactive learning, temporary promotions, etc. **Hybrid training** or "blended methods" can be considered to accommodate various learning needs of a diverse audience in a variety of subjects: any combination of delivery methods can be considered, including computing degrees which will include **distance learning,** computer-based e-learning, e-learning labs, and short off-site residential training sessions at locations outside of the organization.

- **Other training providers**. Some **external organizations** may offer annual or repeated training (e.g., INTERPOL's malware analysis courses). Organizing **joint workshops** with other stakeholder agencies can be an opportunity for learning and interagency cooperation (e.g., Workshop with CERT on information sharing). External or **outsourced training** are methods where the training is provided outside of the organization: technical trainings can be provided by external providers and organizations often involving residential courses. External training, for this reason, can be costly but may well come with other benefits such as formal accreditation. **Appendix D** provides a questionnaire for assessing training providers and partners.

- **More ways of practical engagement**. LEA can **develop guidelines** for certain tasks (e.g., crime scene manual) as part of the training strategy. It can **participate in international workshops and conferences** (Joint Workshop on MLA, 24/7 Point-of-Contact Workshop, etc) to strengthen its professional network and grow capabilities in international cooperation. **Attending at a skills competition** (e.g., Capture-the-Flag competition, such as INTERPOL's Digital Security Challenge) can be considered for highly technical officials. **Training-of-Trainers** approach on certain topics with a large audience (first-responders' course, etc.)

In this context, actions can also be related to broader capacity building initiatives that go beyond training and capability/skills development: such as hiring additional staff, introducing core capabilities and services such as hardware, software, and infrastructure to operate learning management systems (LMS) and knowledge management systems (KMS).

3.4.3 Advice 3: Give clear directions to the course provider

Having determined that formal training is required, the strategy team should define the training course in terms of the who, why, what, when, and how. The definition must be very clear as it provides a prescription for later delegation to implementing partners such as the police training institution. Organizations can achieve a more coordinated outcome by minimizing confusion at the implementation stage.

At the minimum, the strategy must require certain capabilities and target audience it needs, the level of competency it expects, and restrictions and resources. Before declaring the action to be taken, be clear about the following questions:

- **Who needs to be trained?** Consider the existing list of trained employees and potential trainees. Various roles will require different levels of training to enable an employee to be competent.

- **Why do they need training?** Training courses are primarily for knowledge, skills, and foundational expertise applicable in the complicated task, leadership or less supervision, building a network of cohorts, for a better performance.

- **What do they need to know?** Identifying key requirements is essential in achieving training objectives. The list should include all desirable knowledge and skills, not simply those currently lacking. It should be a collaborative effort among leadership, employees, and external stakeholders.

- **When do they need to be trained?** As cybercrime increases globally and becomes more complex, there seems to be an ever-growing list of necessary skills and capabilities required to succeed in investigations. These competing demands require a prioritization and timeline for training for the different employees within the organization's conditions.

An organization may decide to have multiple in-house training courses delivered by its own training institution. For any course to be included in the catalogue, a clear specification must be set at the strategic planning stage. By answering these questions, the strategic plan's course specification will be formed, providing a basis on which to develop and monitor the actual course at a later stage. **Appendix E** provides a questionnaire for assessing training needs at a strategic level. The Strategy team should promote the specification and thoroughly communicate with the training implementation team to ensure coherent delivery of the intended course at the training institution.

Suppose the specifications are missing in the strategic planning stage. In that case, the risk is that the course aims, objectives, contents, or delivery methods may not be in line with the strategy and thus may obstruct the achievement of the objectives and goals. A list of elements that should be included in a course specification can be found in the **Appendix F**.

3.4.4 Advice 4: Capture staff's motivation to learn

Many law enforcement officials change their field of expertise after joining the organization. Officials who started as financial crimes investigators may be interested in cybercrime and electronic evidence. Training strategies can consider how to capture the motivations of individuals and support their success in transforming themselves by obtaining more skills.

In many areas of cybercrime and electronic evidence, knowledge and skills build upon one another. The qualification pathways can induce individual learning by signaling the next step of career development. A layout of qualification pathways can be visualized in a graphical learning path below.

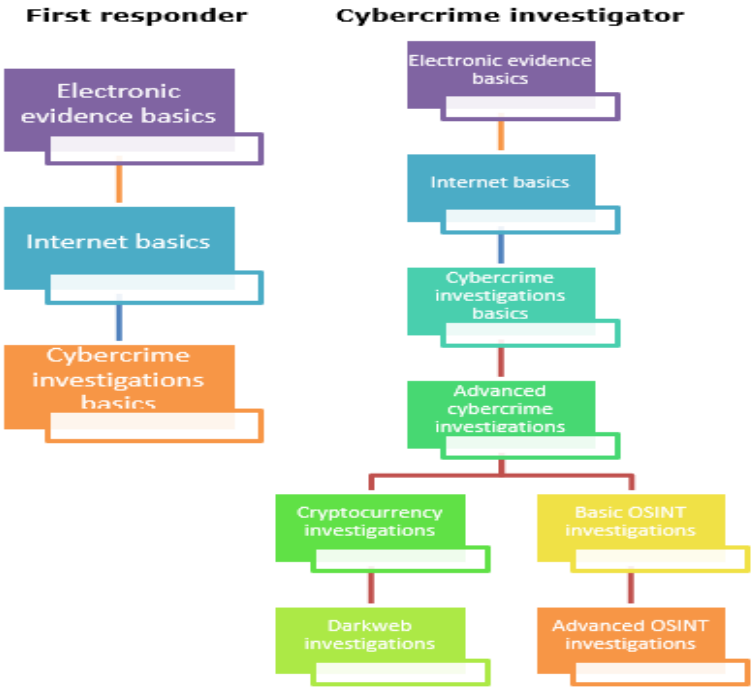


Figure 5: Examples of Qualification Pathways (more examples in **Appendix G**)

Similarly, improving policy communication with the staff and providing a comprehensive course catalog and strategic documents can impact individual career development plans. Organizations can capture training needs through many channels, including periodical individual performance assessment.

3.4.5 Advice 5: Trust is capacity induced through joint activities

Some competencies cannot be taught or built by in-house courses or external training. One example is the trust with practitioners in other domestic and international organizations. A sufficient level of trust is needed to perform cybercrime investigations. Similarly, forensic analysts and other technical experts learn to support each other through participating in a professional network. These should be included and considered as part of training strategies.

Organizations can often strengthen trust through joint activities such as workshops and conferences. Examples for such activities include:

- Workshop to establish and test collaborative processes involving external stakeholders (e.g., attacks on critical infrastructure).

- Workshops on cross-border cooperation with foreign countries, sharing police data or criminal intelligence, requesting data preservation or MLA.

- Other cooperation between LEAs, Internet service providers, CSIRTs, and the industry, using the threat intelligence in law enforcement purposes.

- Capture-the-flag competitions (e.g., INTERPOL Digital Security Challenge) where forensic analysts and cybercrime investigators from different countries compete in teams.

Besides the contents in these activities, there can be network-building which traditional training cannot deliver.

3.4.6 Advice 6: Keep managers and stakeholders informed

In strategic planning, it is important to involve management at several levels as strong commitment from management is essential. This applies to decision-makers and high-ranking managers within the police and external stakeholders. The more these decision-makers support the strategy, the more likely it will succeed. The training strategy brings resources together: sustainable budget provision, facilities, equipment, and personnel is the key success factor of many creative solutions.

Keeping the attention and commitment of decision-makers of the external stakeholder organizations should be considered in the earlier stage of the strategic process. A manager who followed along with the planning and the implementation process is more likely to commit themselves if problems arise and will more likely support the readjustment of the strategy.

For the manager of the strategy team, it is essential to frequently communicate with all team members, as well as with stakeholders and decision-makers. The member must quickly adapt to changing environments, as communication partners, organizations and political objectives may also change.

4 STEPS FOR IMPLEMENTING AND MANAGING THE TRAINING STRATEGY

The time spent defining the strategy is only "well spent time" when the strategy is later implemented effectively throughout the organization. There is an essential balance between forming the strategy and implementation, which is often more complex and time-consuming.

After developing a strategy, an organization may have various plans containing multiple action items. Implementors take these action items and push them in the direction set out in the strategy to achieve its overall objectives. Implementors may be the sub-departmental units, internal and external stakeholders, and practitioners. A well-developed strategic plan will communicate how each department will contribute by informing them where to direct resources. The departments and other implementors of the strategy will then attempt to align it with their short-term and long-term objectives (Step 5).

The strategy itself should be revised periodically, especially when it is found inefficient or unrealistic. The strategy team must regularly review the goals, objectives, and required actions were properly defined. This should be done on the basis of effective measuring of the results of implementation (Step 6) as well as structured reviews and evaluation (Step 7).

4.1 Implementing the action (Step 5)

Different stakeholders will be engaged as implementors, and various sub-groups may be formed to execute the required action. For example:

- To establish a training curriculum, cybercrime educators and curriculum planners will need to launch a separate planning process. It will engage a different group of stakeholders, including training providers and trainees.

- To develop a training course, the curriculum manager must coordinate its position in existing training courses, clarify learning objectives, consider in-house development or external delivery, and arrange trainers. A design framework such as ADDIE can be considered.

- To provide staff career pathways, human resources and staff/personnel management should cooperate, as staff training time and compensation upon training would be tied with new skills.

- Overall performance increase in cybercrime and electronic evidence would need to be monitored against benchmarks to allow continued commitment of the management in the cybercrime training strategy. The monitoring mechanisms justify staff time and energy spent on implementing the strategy.

- Coordinators engaged in inter-agency and international cooperation mechanisms will help develop and evolve greater strategic partnerships.

- Monitoring and Evaluation (M&E) of the implementation of the strategy would need to be done on a regular basis to ensure that the strategy was being implemented effectively and that challenges and opportunities were being folded into an evolving strategic approach.

In sections below, we focus on: promoting the strategy, aligning the budget, and monitoring the activities. We also advise on a specific case of in-house training courses as this is often the major action in many training strategies.

4.1.1 Promoting the strategy and activities

A strategy does not assure success unless communicated throughout the organization: top-down, bottom-up, and laterally with partners. To foster departmental and partner engagement, it must be easily accessible, with its purpose, values, and actions clearly defined in plain language. One piece of advice commonly applicable is that implementors, not just the strategy team, should promote the strategy and activities within the organization and stakeholders.

Communications promote the organization's strategic plan internally and externally. The communication campaigns should be repetitive and use all forms of communication, written, oral, videos, blogs, intranet, internal message boards, mobile applications, one-to-one or group meetings, management briefings, and posters. It should feature letters, emails, organizational communications, publications, published progress, and results reports.

Communication campaigns should recognize the needs and cultural differences of the audience when messaging. Feedback questions reinforce the communication and measure the communication's impact. Include a "line of sight" agenda item for any organizational, departmental, employee, or partner meetings. To ensure the messaging is understood, keep it:

- **Simple** – develop messages relevant to receivers, keep the messaging simple and to the point;

- **Achievable** – prioritize resources, build on existing strengths and opportunities;

- **Relevant** – stay focused on what is important to the organization's success.

Organizations with an excellent internal communication can attract and retain more talented workers. Employees who understand the value of their contributions to the organization's overall mission are more engaged, productive, and creative. Partners and stakeholders will also feel rewarded when business strategies and goals are shared with them. Additionally, when employees are engaged and productive, stakeholders will see the positive value of cooperation.

4.1.2 Managing and aligning resources

Implementation of actions often involves costs for staff, equipment, and external expertise. The budgeting process is not truly aligned with its strategy or activities in many organizations as the strategy team is not always responsible for creating and securing the budget. It is often the implementors' responsibility such as the managers of the cybercrime units: the participating departments and teams need to understand the budget required by the strategy and prioritize the right resources and programmes. The participation in the strategy can provide justification for additional budgetary bids.

Figure 6: Aligning budgets with strategic priorities

Early involvement in any strategy budget meetings is recommended: identifying at the earliest opportunity key managers, leaders, and partners interested in the implementation of the training plan and apply for the allocation of budgets and resources. Any discussion of budgeting should be viewed as the mechanism to allocate resources to achieve strategic results.

Original budgetary assumptions may be countered, and plans can alter. When this happens, the review process should handle the new priorities and re-align the budget to support any change of strategy.

The following costs and impacts are typical contents of budget. In making bids for funding, the following costs and impacts should be considered:

- Trainer salary and time, consultant fees, training materials (workbooks, videos),
- Course fees, platform costs, (e.g., video tutorials, e-learning), facility or equipment rental,

- Subscriptions or memberships to professional bodies,
- Logistical expenses (travel, meals, and accommodations),
- Ongoing costs (e.g., licences, hardware, software),
- Trainee salary and time lost productivity due to participants being absent from their daily roles. (Including replacement time).

The cost of the training programme will depend on the type of training required. Many diverse types of training exist, each varying widely in cost. Before choosing, know what results are required and desired. Then, select the training activities that best fit those results and budget.

Training Type	Relative Cost
Coaching mentoring / Self-directed study / Shadowing	$ (Least expensive)
On-Line learning / Seminars / Group workshops (internal)	$$
In-house courses	$$
Consultant Training (in-house)	$$-$$$
External courses / Group workshops (external)	$$$
Degree courses / Technical Courses - accredited	$$$$ (Most expensive)

Table 1: Aligning costs

The training budget will need careful management to ensure that costs stay on track. Unforeseen events can lead to changing costs. A specially trained staff member might unexpectedly leave the organization before their knowledge is passed on to others. Training costs will increase if there is a need to rely on external resources.

There may be a temptation to use the least expensive trainers or training materials available. Ensure that an evaluation is undertaken before undertaking any commitment; the cheapest may not be the best. Similarly, the most expensive may not be the best fit for the purpose. Identify the best caliber of training to meet the needs of the training plan and strategic objectives. The right training programme will save money in the long term.

4.1.3 Monitoring the implementation

Implementors ensure timely and effective delivery of activities as requested by the strategy throughout the entire process. The implementors monitor the progress and provide feedback to the strategy team as part of a continuous cycle.

Implementors may face new issues and risks. Some of the issues, risks, and challenges may pressure implementors to revise their activity plans; other more serious ones may need to be raised for modification of strategic posture itself. For the strategy team, it is a change of environmental conditions. Monitoring also provides an opportunity to find new synergies and creative solutions proposed to the strategy team.

The cycle's success depends on the smooth, bi-directional flow of communication among implementors participating in the strategy and the strategy team. The strategy team must clearly communicate strategic directions, and implementors share the progress and results. They must remain flexible both in their plans and their actions.

4.1.4 Best practice for managing in-house training courses

A piece of action-specific advice for the in-house course implementors is to consider using an instructional design system (IDS) that is consistently applied to all courses.

The ADDIE (Analysis, Design, Development, Implementation, and Evaluation) method provides valuable references for developing and delivering an in-house training course or curriculum. The model is scalable and may be used in the course and curriculum planning.

The ADDIE process is useful for implementors of in-house courses (**Appendix H** for details).

- The first stage involves **Analysis**. The implementors take a deeper, practical assessment of the current situation and document the details of knowledge gaps and training needs to supplement the strategy. The strategy's directions, definitions, and requirements (e.g., training contents, audiences, duration, budget, delivery methods) should be sufficiently detailed for coordination among multiple other actions. Still, there must be sufficient room for practical assessment by the implementors.

- The second stage is **Design**, translating the requirement into high-level learning objectives. The training is developed, delivered and measured against them. A high-level outline is created at this stage and mapped to training needs. Stakeholders participate at this stage before starting to invest in building the content.

- The third stage is the **Development** phase, building the course contents. Internal cooperation with finance departments and human resources helps secure funding and resources.

- The fourth stage is the **Implementation** phase where the course is delivered to the learners. It may include logistics, communication with participants, and collection of feedback.

- The fifth stage is the **Evaluation**, where the course is reviewed against strategic requirements: did the course meet the prescription set by the strategy? Consistent evaluation of the course allows efficient training delivery towards the strategic outcome.

ADDIE is a cyclic process and returns to the analysis phase to ensure **continual improvement to the course and the strategy.** Each component provides parameters and natural progression for the in-house training courses. More details on the ADDIE training cycle can be found in INTERPOL's Guide on Effective Training (2018).

4.2 Measuring the results of the implementation (Step 6)

Measuring the results of implementation of the training strategy is crucial for assessing whether it is having the desired effect, and for enabling evidence-based revisions and updates. Methods can be qualitative and quantitative, but they must be suitable for communicating with stakeholders, including the training strategy team. The implementors may use existing methods or devise a new method to capture specific outcomes.

4.2.1 Assessing the training strategies through KPI

A Key Performance Indicator (KPI) is a metric to drive action that influences results; they are a valuable tool to keep the implementor focused, aligned, and accountable. While it is important to measure, it is equally important not to measure unnecessarily. KPI assessment is time-consuming, and organizations must carefully identify indicators for evaluation. Implementors must review KPIs regularly and remove indicators with negligible value.
Examples of monitoring KPIs with several sources for measurement and evaluation can include:

- Tracking the development of the training with timelines and milestones for implementation, prioritization of training, learning and development to employees, what is expected to be achieved, tracking the training, measuring the success of the training through a KPI checklist.
- Did learners learn anything of value?
- Has the training increased their performance on-the-job?
- Has it contributed toward generating the desired business results?
- Evaluation of the time to proficiency can be an important indicator of training effectiveness.
    - Was the learning easy and engaging for learners to shorten the learning curve?
    - What was the individual time taken by learners to finish their training?
    - Focus groups could be formed to assess the learner's performance both before and after training to see the time taken to reach a certain level of proficiency.

4.2.2 Learning impact

Alternative to the KPI measures, an implementor may measure the outcome of training activities by measuring the degree of learning. Training evaluation models provide systematic frameworks for investigating and analysing the effectiveness of training and learning. Some examples of training evaluation include the Kirkpatrick Model (see next section),[3] the Context Input Reaction Output or

[3] https://educationaltechnology.net/kirkpatrick-model-four-levels-learning-evaluation/

CIRO Model,[4] the Philips Return on Investment (ROI) Model,[5] the Brinkerhoff Model,[6] Kaufman's Model of Learning Evaluation,[7] etc.

Different models target different things. In general, they look at:

- Was the training successful?
- What did the participants learn?
- Did the participants use what they learned on-the-job?
- What was the impact on the organization?
- Did it achieve the organization's objectives?
- Was the training a worthwhile investment?
- Did the training offer value for money?
- Could the training be improved?

Monitoring these measures will help the organization manage the quality of training programmes, therefore ensuring the larger training strategic objectives are achieved as intended. Quality control provides timely and valid feedback about organizational performance so that timely and effective change and adaptation become a routine.

One of the best practices in measuring the success of individual training is Kirkpatrick's model for course evaluation. It includes four levels of evaluation:

- **Level 1** – reaction and feedback from learners.
- **Level 2** – scoring patterns from learners.
- **Level 3** – observed behavioural change.
- **Level 4** – business impact and results (ROI).

[4] https://kodosurvey.com/blog/ciro-model-definitive-guide
[5] https://roiinstitutecanada.com/roi-methodology/
[6] https://www.watershedlrs.com/blog/learning-evaluation/brinkerhoff-method/
[7] https://lucidea.com/blog/kaufmans-five-levels-of-evaluation/

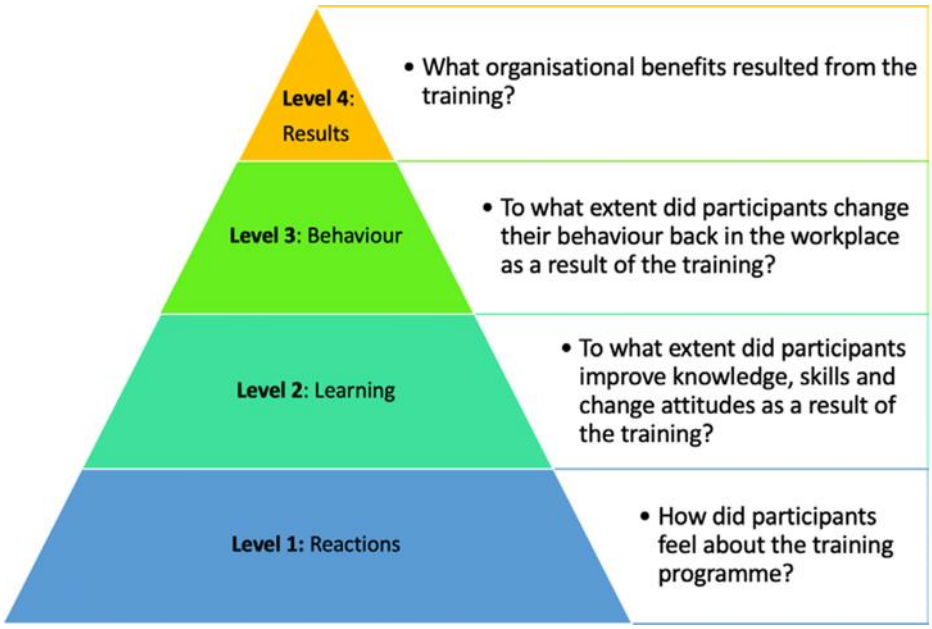


Figure 7: Kirkpatrick's Four-Level Training Evaluation Model[8]

Greater details of the measuring success of an individual training courses can be found in INTERPOL's Guide on Effective Training (2018).

4.3 Reviews and evaluation, for iteration and improvement (Step 7)

When an organization has set a 3-, 5- or 7-year strategy, why would we need to change it? Criminals constantly evolve faster than law enforcement, and an LEA should identify these changes through constant environmental scanning. When these changes and challenges occur, law enforcement needs to adapt dynamically.

Reviews and evaluations are processes to ensure timely and effective review of deliverables to determine whether changes or improvements are needed at any level. It analyzes supporting data and communicates the outcomes. A review occurs within different time frames based on project criticality and complexity. Examples laid out in this section are (1) Annual Strategic Reviews, (2) Communication and Reporting, (3) Quarterly Strategic Reviews, and (4) Monthly Tactical Reviews.

Effective reviews ensure that all activities are well-executed and that implementation is on the right path towards achieving the training goals. It also provides an opportunity to find out if the training has really made a difference and assist in identifying how to show/demonstrate to the planning team, partners, and stakeholders precisely what has been achieved. Reviews should engage both the strategy team and implementers.

[8] https://www.researchgate.net/figure/Kirkpatricks-four-level-training-evaluation-model-Reproduced-from-41-on-September-15_fig1_344232579

The most common question during the review is, "did the strategy and activities achieve what it originally set out to do?" Therefore, the approach is to return to the strategy's original goals and objectives and use them to identify and report on the indicators of progress.

The following table provides an example of the different reviews, the frequency, the anticipated attendees, the purpose, and the anticipated outcomes of the meeting.

Meeting Type	Attendees	Purpose
Annual Strategic Review	Project Lead, Department Heads, Executive Team, Key Stakeholders	To monitor progress of the organization from a strategic level and make sure that objectives are on track. Review implementation progress, Review Performance, Address Critical Issues, Exchanging Ideas, Finance and Resources.
Quarterly Strategy Review	Project Lead, Training Department Head, human resources (invite other attendees relevant to challenges and opportunities).	To monitor the training departments progress from a strategic level and make sure that objectives are on track. Review implementation progress, Course Development, Analysis and Feedback.
Monthly Tactical Review	Predominantly Training Department, (invite other attendees relevant to challenges and opportunities, if preliminary stages of implementation may require attendance member of project team).	Tactical discussion on the course development and delivery. Review Course development and delivery progress, Course Content, course feedback, challenges, exchanging ideas, opportunities, and improvement.

Table 2: Meeting Types, Attendees, Purpose

4.3.1 Quarterly and monthly reviews

A **Quarterly Strategy Review** or smaller interim reviews may be required to take place on a more frequent basis, particularly when starting new training programmes or when the organization is impacted by significant environmental change. Examples can include global or regional changes in cyber-criminals modus operandi, innovative technologies, cryptocurrencies, or adaptations of specific malware.

A Quarterly Strategy Review is not intended to be as in-depth as the creation of the strategy nor as granular as to discuss specific day-to-day problems or specific course content. The key emphasis is to identify any issues that will impact delivering the strategy, troubleshoot these issues, and provide recommendations for revising the strategy.

Those attending should be the training manager and, depending on the organizational structure or requirements, may include representatives from stakeholders, human resources, and finance. They can be permanent group members.

It is recommended that minutes and actions of these meetings be recorded. Any reports requiring escalation to the executive or the annual strategic review can be reviewed during quarterly meetings.

The **Monthly Tactical Review** is intended to be held internally within the departments with those responsible for implementation. This meeting should deal with the day-to-day progress, identifying the successes and challenges and areas for improvement. It should monitor and evaluate feedback and exchange ideas and opportunities for continual improvement.

It is recommended that minutes and actions be recorded of these meetings. This is in case there is a need for escalation of issues, and the reporting structure will need to be unutilized and follow a similar communication mechanism as recommended.

4.3.2 Annual strategic review

One of the methods to achieve this is to conduct regular reviews of our strategies and revise them to meet the new demands. The Annual Strategic Training Review should be a high-level meeting with a clear fact-based process in which organizations analyse and discuss the progress of their goals and objectives, identify opportunities or issues and make the necessary adjustments for the forthcoming year. It provides an opportunity to step back from day-to-day operations to assess the strategic foundations on which the training is built.

Strategic reviews can be accompanied by pressure to answer rapidly and conduct the review in a timely manner. The strategy team can be assigned full-time for a brief period to conduct the review. Before drafting a report, consider the target audience, as some may want an overview of the key findings. In contrast, others may require detailed information to support making crucial decisions about the proposed revised training.

It should be attended by the executive team, key stakeholders, budgetary and resource decision-makers. Major changes in the plan may require agreement from the senior management or other organizational branches. Any changes should be communicated back to the strategic team and stakeholders, with a possible re-evaluation of their roles and responsibilities. The organizations should review the changes and align the communication plans accordingly to ensure widespread participation.

5 CONCLUSIONS

Cybercrime and electronic evidence pose complicated, multi-layered challenges to the LEAs. Competency gaps may include lack of knowledge and skills, strategic capacity, legal capabilities, institutional competencies, or capacity to cooperate. As the gaps are multifaceted and evolving, LEAs need to adjust and adapt continuously. Cybercrime and electronic evidence training should now be compulsory for almost every police officer, law enforcement official and prosecutor.

To ensure resilient and dynamic capacity development, organizations must adopt a strategic attitude. A good training strategy provides clear directions and responsibilities for different stakeholders who implement the strategy. It should be a continuous process to ensure the knowledge and skills of the LEA representatives are up to date and follow the development of the technology. The benefit of such training will go beyond the specialized cybercrime or digital evidence units. They may assist other LEA departments with traditional crimes where electronic evidence is present or other crimes enabled by technologies.

This guide sets out the key stages in developing, implementing and evaluating an effective training strategy on cybercrime and electronic evidence. An LEA would first set up the strategy team responsible for the entire process and that will coordinate among different actors. They will start by scanning the

internal and external environment, assessing the needed capabilities, and identifying stakeholders and implementors. The team will work with stakeholders to formulate the strategic framework, specifying goals, objectives, and the activities to achieve them. Directions and specifications are set in output-oriented language to be used in the future by the implementors.

When the objectives and proposed actions are clearly defined in the development phase, implementation is a natural continuation. The participating partners will push themselves in the strategy's direction, perform their daily business, and measure the results of their day-to-day operation using the framework set out in the strategy. Reviews and evaluations help determine what changes and improvements are needed. Strategic planners and implementors perform periodic assessments and communicate the result with stakeholders. The strategy team and implementors should remain flexible toward the inputs from these reviews.

INTERPOL and the Council of Europe recognize that training strategies developed by LEAs play a critical role in enhancing national capabilities in cybercrime and electronic evidence. Through various cybercrime capability development projects, the two organizations will continue to support national LEAs to develop training strategies on cybercrime and electronic evidence that reflect and respond to their specific needs.

6 APPENDICES

6.1 Appendix A: Questionnaire for assessing a strategic plan

- Does the strategic plan(s) support and align with a larger mission and vision goal?
- Is it flexible and realistic?
- Is it able to be clearly communicated internally, and externally?
- Is it able to be centrally coordinated by a facilitator or project team?
- Does it have accountability for its results?
- Does it assist with decision-making on resource allocations?
- Is it able to be merged into organizations' existing system(s), allowing for continued business operations while it is slipstreamed into place?
- Does it include innovation and continuous improvement (rather than simple replication and copying)?

6.2 Appendix B: Stakeholder Analysis Template

Stakeholder name			
Contact			
Role in the strategy			
Profile			
Focus area			
Potential contribution			
Potential objections			
Engagement Strategy			
Comments			

6.3 Appendix C: Action Plan Template (with examples)

Outcome 1	**Action**	**Responsible**	**Resources needed**	**Start Date**	**End Date**	**Notes**	**Completed**
In two years, the police academy will have developed and delivered at least two new training courses on the handling of electronic evidence for first responders.	Hire two new expert trainers	Police academy	2 positions, rank A	06/2021	12/2021		
	Develop two new training courses on handling of electronic evidence for first responders	Police academy, ISF experts		12/2021	08/2022		
	Pilot the two new training courses	Police academy		11/2022	02/2023		
	Evaluate and update the two new training courses	Police academy		12/2022	05/2023		
	Permanently integrate new training courses into curriculum	Police academy		05/2023	05/2023		
Outcome 2	**Action**	**Responsible**	**Resources needed**	**Start Date**	**End Date**	**Notes**	**Completed**
The police academy will continuously update existing course materials.	Permanently monitor course evaluations	Police academy		05/2023	05/2025		
	Annually update needs analysis	Police academy		05/2023	05/2025		
	Update course materials and delivery methods based on evaluations and needs analysis	Police academy		05/2023	05/2025		
Outcome 3	**Action**	**Responsible**	**Resources needed**	**Start Date**	**End Date**	**Notes**	**Completed**

6.4 Appendix D: Questionnaire for training service providers / partners

This questionnaire can support in collecting valuable information from training partners.

- Which types of training can the partner offer to address the needs expressed by the beneficiaries?
- Can the partner tailor the training to law enforcement needs? Often external training typically offered to commercial customers do not consider the specific needs of law enforcement organizations.

For each training:

- What are the aims of the training?
- What is the designated target group for the training?
- Which profiles does the training address?
- Which skills will the training address?
- How many participants can be trained in one activity?
- Are there any prerequisites needed (e.g., intermediate courses will require existing basic knowledge)?
- What is the duration of the training?
- What is the delivery method?
  - Is it an on-site training, a synchronous or asynchronous online training, a blended training?
  - At which facilities will the training be delivered? In-house/ at the provider/ online?
- What are the requirements for the facilitator?
  - Hardware: Is there any specific CPU/GPU/RAM/DISK/BIOS configuration required, e.g., if virtualization is involved?
  - Software: Is there any specific operating system in a given version and architecture needed? Any additional software that needs to be pre-installed?
  - Licenses: Are any licenses (files/dongles) needed to run proprietary software? If so: Will the licenses stay with the participants? When will the licenses expire? What is the annual renewal cost to maintain the license?
- What/how many sessions does the training consist of?
  - What are the objectives of the sessions?

  - What is the syllabus of each of the sessions?

- What is the balance between practice and theory?
- How is the successful attendance of the participants measured? Is an assessment or certification exam included? Are any academic title, certificate or credit points associated with the training?
- What is the cost for the training?
  - Cost for facilities/hardware/software/licenses?
  - Cost for trainers?
  - Cost for travel, accommodation, food?
  - Are there any packages that will reduce the cost, e.g., if a certain amount of participants/training are booked, if training passports allow a participant / organization to attend multiple training within a certain timeframe?
  - Any other cost?
- Are there any options to initiate long-lasting partnerships? For example:
  - Partner from academia being responsible for technical training on a permanent basis, while police academies / colleges add law enforcement specific modules.
  - Police academies / colleges become certified training partner institutions for private companies, allowing them to train an unlimited number of their own personnel.

6.5 Appendix E: Training Needs Analysis

A Training Needs Analysis (TNA) is a primary requirement when developing any strategy for an organization. Training specifically (and learning more widely) is the way to help employees improve their performance at work. TNA is also often referred to as Learning Needs Analysis (LNA), is a systematic approach to identify and understand the gap between:

- the current performance of an organization and its employees,
- the desired performance of an organization and the ability of its employees through training, learning and development are aligned to meet the organization's strategic objectives and goals,
- examine the roles and task for operational needs,
- identifying the new knowledge, skills, competencies, capabilities, and attitudes employees require to meet their own and the organizations development needs and undertake their role successfully,
- identify issues where training is not the solution, for example role or function design, shortage of or no provision of the correct equipment, flawed processes etc.,
- identifying and designing training and learning courses with commensurate resources to bridge the gap between current and desired capabilities.

The following are samples of the styles of questions that may be used to increase the effectiveness of a task analysis and focus on the driver of performance.[9]

- Focus on individuals: skills, knowledge, expectations, information, motivation.
- Focus on culture: environment, incentives.

When selecting tasks to be trained, consider the following factors:

- What will happen if we do not train this task?
- What will be the benefits if we do train this task?
- If we do not train it, how will the employees learn it?
- How will the learning platform help to achieve our business goals?

[9] https://www.wiley.com/en-us/Beyond+the+Podium%3A+Delivering+Training+and+Performance+to+a+Digital+World-p-9780787955267

- Is training needed to ensure their behavior does not compromise the company's legal position, i.e., Occupational Safety and Health Act, Equal Employment Opportunity, labor relations laws, or state laws?
- Can people be hired that have already been trained?

Below are some suggested questions that might need to be asked:

- How critical is the task to the performance of the job?
- To what degree is the task performed individually, or is part of a set of collective tasks?
- If it is part of a set of collective tasks, what is the relationship between the various tasks?
- What is the consequence if the task is performed incorrectly or is not performed at all?
- To what extent can the task be trained on the job?
- What level of task proficiency is expected following training?
- What information is needed to perform the task? What is the source of information?
- Does execution of the task require coordination between other personnel or with other tasks?
- Are the demands (perceptual, cognitive, psychomotor) imposed by the task excessive?
- How much time is needed to perform this task?
- What prerequisite skills, knowledge, and abilities are required to perform the task?
- What behaviors or outcomes distinguish good performers from poor performers?

6.6 Appendix F: Course specification elements

A course specification at strategic planning stage should include following items:

- Representative name of desired capability obtainable through the course. Naming is important as it is the most common means of communication. Intuitive and well representing the contents, e.g. Windows Filesystems Forensics Course.
- Course aims and objective.
- Course duration.
- Delivery method (e.g. purely online, blended, on-site).
- Course contents. Contents may overlap between courses. It is important to identify and address a desired audience. A good example is using the Competency Matrix such as the CEPOL Training Competency Framework[10] that analyses the capabilities by roles/ capability areas/ levels.
- Competency it wants to achieve, and the desired level of competency it wants to achieve. Some competencies can have multiple level (e.g. basic, intermediate, advanced), and some may have binary (yes, no).
- Consider the target audience in number and expected prerequisites. Who does the training target, and how many officials are needed? Be realistic, and if an extremely small audience is expected – consider other means than developing in-house courses. If extremely large audiences are expected, consider a Training-of-Trainers programme.

[10] https://www.cepol.europa.eu/sites/default/files/OTNA_Cybercrime_Attacks_Against_Information_Systems_2019.pdf

6.7 Appendix G: Examples of Qualification Paths

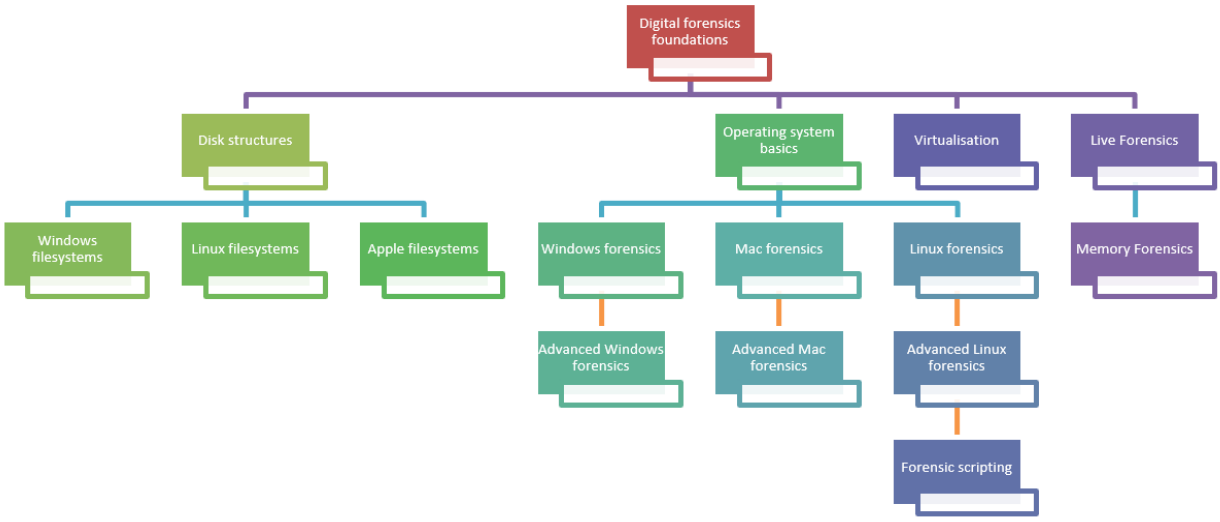


Figure A.2 - Qualification path for digital forensics examiner

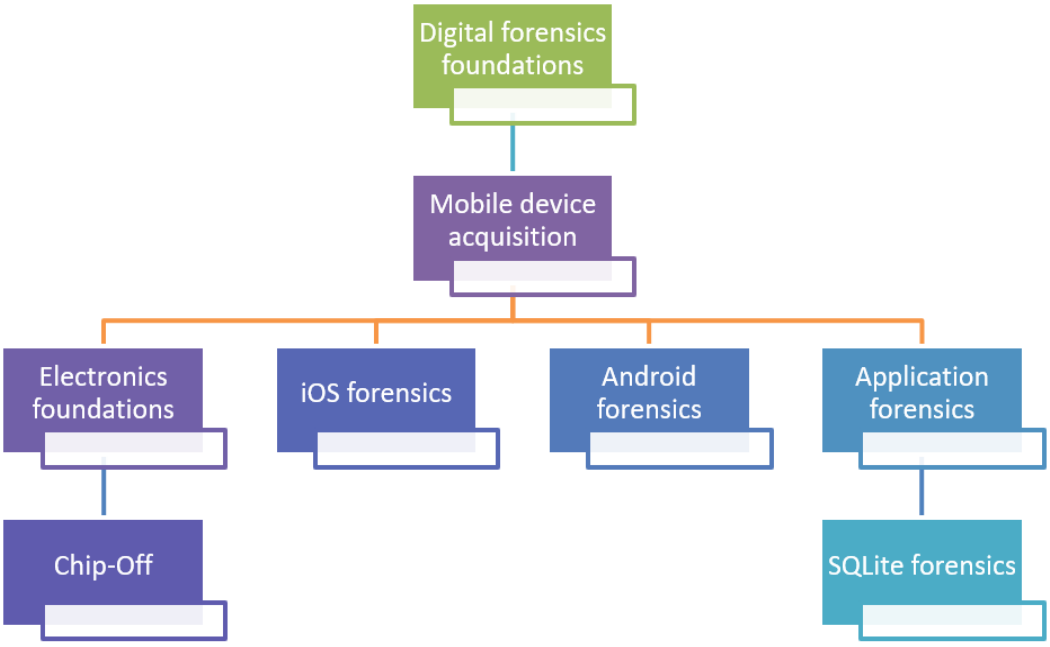
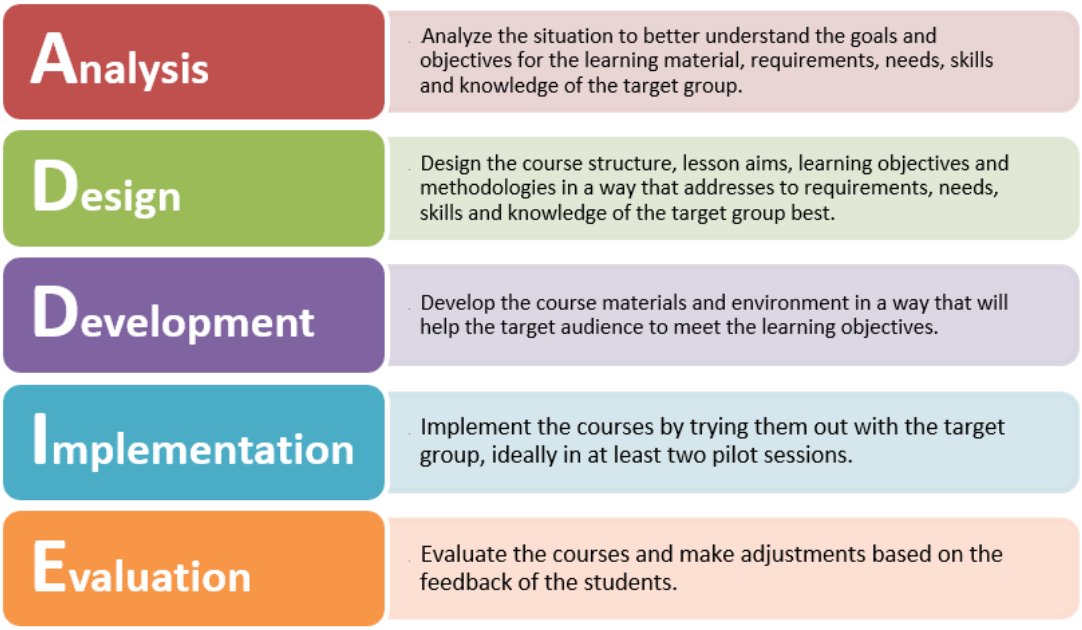


Figure A.3 - Qualification path for mobile forensics examiner

6.8 Appendix H: ADDIE – Analysis, Design, Development, Implementation, Evaluation

The ADDIE (Analysis, Design, Development, Implementation and Evaluation) is a five-stage process that provides guidelines to identify, create and manage effective training course, the methodology can be adapted to the introduction and evaluation when developing training strategies.



Stage 1: A = Analysis stage of ADDIE system. The course specification provided by the strategic plan will be referenced and be inherited as core objectives of the course. More training needs assessment (TNAs) can be conducted to:

- Identify the issues and needs / the audience / why are we doing the training
- Establish goals and desired outcomes / Identify the trainees' current capabilities.
- What tools are best to deliver this type of learning?
- Confirm the detailed list of knowledge, skills, and attitudes (KSAs) that are to be taught in the course. These KSAs form the core contents of the course objectives.
- When does this need to be delivered?

At the end of the Analysis phase, a plan for the training course and knowledge of what the training needs to include should have been mapped out.

Stage 2: D=Design stage. This stage involves the design of the course using the information from the analysis stage, to identify the type and methods available to deliver the training. This phase is often time-intensive and requires attention to detail. Elements may include:

- Identify and design specific learning objectives.
- Structure of content and duration of the training session.
- Knowledge and skills trainees need to retain.
- Best tools and delivery format.
- Building content related assessments and exercises.

The course outline and overall design should be completed at the end of the Design phase.

Stage 3: D = Develop. This stage involves creating and developing the course modules or content, this will look at the methodology for delivering the course, the technical requirements for delivery, and bringing the content ideas to life. This means laying out the content visually, creating graphics, recording videos, carefully selecting material and exercises, anything that has to do with creating the actual end-product for learners. These can include:

- Develop lesson plans / course material / a prototype course / assessment materials
- Developing course guides
- Establishing testing and review process with stakeholders.
- Production of the learning product in line with the design. This represents the bulk of the work in the development phase. This part may be outsourced to a trainer who is a subject matter expert, or a training organization with relevant knowledge. It is the role of the instructional designer to ensure that the learning product will align with the specifications of the design and the findings in the TNA.

At the end of the Development phase, the entire training course should be completed.

Stage 4: I = Implement. At this stage the course has been created, tested, and approved. Now it is time for learners to take the course designed from information at stages 1-3, this stage can be best prepared by firstly undertaking reviews and analysis of the intended training with training peers followed by running a small pilot course to evaluate the course planning, course material, methods, and methods of delivery. Other elements at this stage can include:

- Develop a training implementation programme.
- Ensure technical equipment, demonstrations, and exercises function as expected to deliver the training in a manner that can be understood by the trainees.
- Ensure the training material and tools are complete and functioning for the delivery of the training.
- Identify methodologies for undertaking observations of the training in action.

- Once the course is running, pay close attention to see if any issues arise, note them for attention after the session. In the pilot stages or for the first few courses add additional time following each session or module, to undertake a quick evaluation, if it is possible have another trainer or stakeholder independently evaluate the course at this stage.

At the end of the Implementation phase, the pilot course would have been undertaken. This would include an identification of issues that have arisen, and steps taken to rectify or improve the learning material or delivery so as the trainees can have the best experience and have the greatest opportunity for learning.

Stage 5: E=Evaluation. This stage is extremely vital to the process, as much effort and thought needs to be applied to this process as in the design and development of the training. It should not be implemented in a manner that only represents the positives, in fact it should be utilised in a way that extracts honest and constructive observations about the course, the course objectives, the modules, the assessment and exercises, whether the learning objectives have been achieved, identify elements that were lacking in the course, review and measure the relevance and success of the training and whether the course is effective or are the trainees confused?

There is no single evaluation method for measuring or extracting this information, so the course structure should establish subtle methods in the training to ensure that objectives have been achieved, such as quizzes, demonstrations, surveys, and assessments.

Examinations can also assist especially where questions have been developed in a range of styles to establish whether the learning objectives have been achieved or not achieved, for example if 60% delegates get the same series of questions wrong, then undertake a re-evaluation of the specific module that relates to this issue, as it is a clear indicator that the training material or delivery has failed.

Other methods for evaluation include:

- Assessing the learning effectiveness during the training, including awareness, knowledge improvement, behavior, and results.
- Gathering essential information to see if the course needs to be revised and improved.
- Consider a form of knowledge assessment at the start of the training either in a formal manner using an exam or assessment or integrating it into an icebreaker session and course closure exercise to enable knowledge comparisons from the start to the end of the course.
- Pre and Post training undertake workplace assessments with the trainee and line manager post the training to establish what impact the training has had in the working environment.
- Use the findings from the evaluation to revise and improve future training, reflecting on the original Analysis phase where required.
- Establish the value or cost benefits that the training has provided.

At the end of the Evaluation phase, the documentation should yield detailed information about what

is needed to revise or improve for this course or future courses.

One unique feature of the ADDIE model is that it can be used as a continuous cycle. For example – gathering feedback in the final Evaluation phase, which then feeds back into the beginning at the Analysis phase, which starts an entirely new iteration of the end-product.

6.9 Appendix I: Cybercrime Training Strategies Survey Results

Purpose and methodology

In August 2021, Interpol Cybercrime Directorate conducted a survey to understand the extent to which Interpol member states engage in strategic planning and management to combat cybercrime. An email that included a link to the Cybercrime Training Strategies Survey was sent to the INTERPOL National Central Bureaus (NCBs, n=194). Of these, 321 LEA officers responded: 246 responses from 59 countries were used for analysis and 75 responses without country affiliation were excluded for analysis. The number of respondents per country varies, from 1 to 118. The mean value for 59 countries were included for analysis. The list of participating countries is attached below.

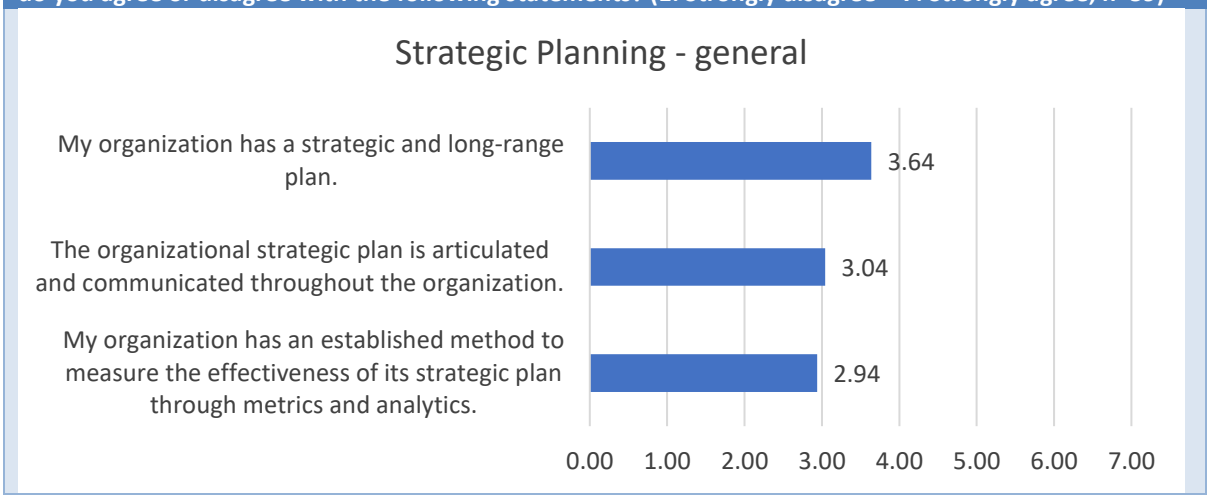
Key findings

- Strategic planning is being used by LEAs in many countries, particularly in attempts to combat cybercrime.
- The use of comprehensive strategic management is only beginning to develop in a small number of countries. Both strategy 'planning' and 'management' need to be conducted, which involve ensuring that strategies are implemented effectively and evaluated on an ongoing basis.
- Regarding cybercrime, LEAs run various training programmes, while they need to strengthen courses related to e-evidence collection and digital forensics.
- LEAs need to further develop partnerships with stakeholders in building and managing training strategies.

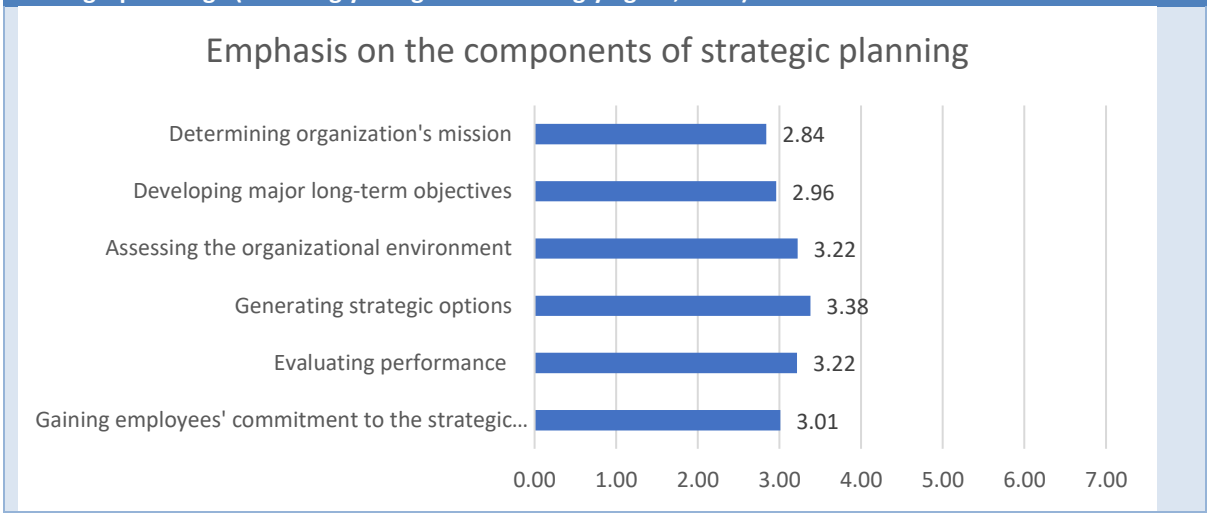
Survey results

A. Strategic management in place

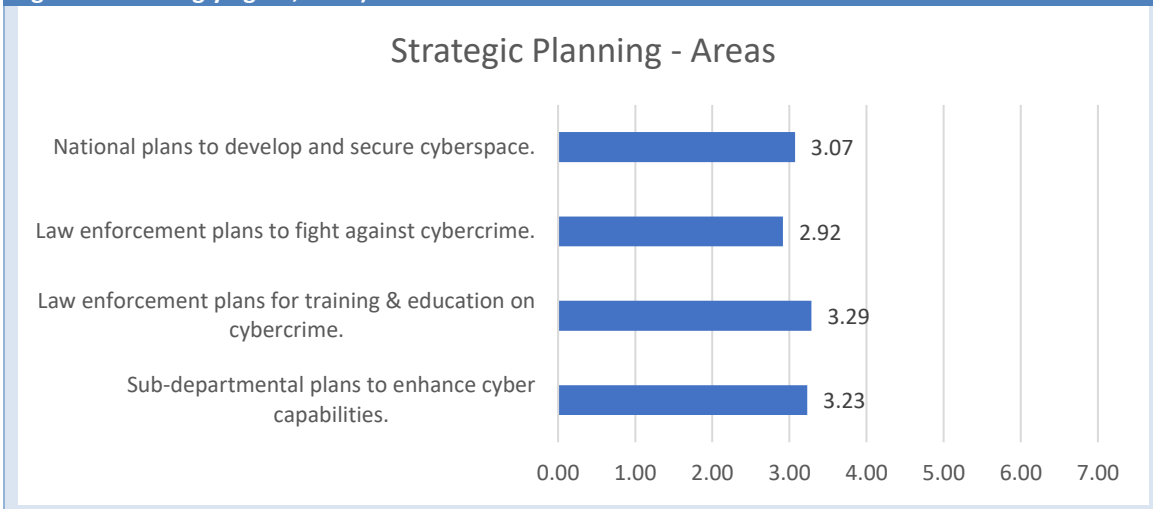
Q: Below we ask questions about organizational strategic management. Organizational strategy is a long-term plan that maps the route towards the realization of an organization's goals and vision. To what extent do you agree or disagree with the following statements? (1: Strongly disagree – 7: Strongly agree; n=59)



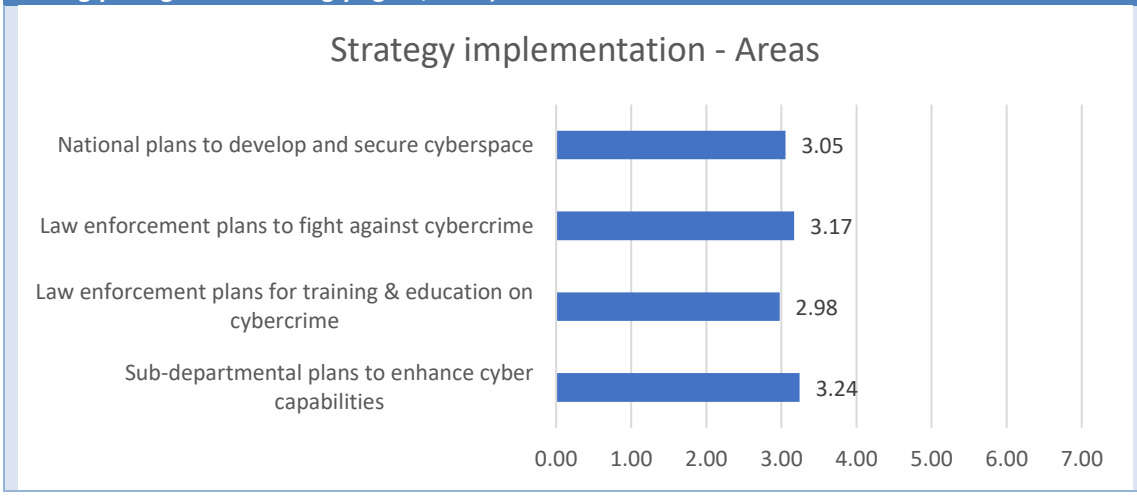
Q. In your opinion, to what extent does your organization put emphasis on the following components of strategic planning? (1: Strongly disagree – 7: Strongly agree; n=59)



Q: To what extent do you think your organization has "documented" the following plans? (1: Strongly disagree – 7: Strongly agree; n=59)



Q. To what extent do you think your organization has "implemented in practice" the following plans? (1: Strongly disagree – 7: Strongly agree; n=59)



B. Cyber training in place – general

Q. Think about your organization's training for all officers (new and current). Are following subjects established as part of law enforcement training curriculum? (%, n=59)		
	Yes	No / Do not know
National plans to develop and secure cyberspace	63%	37%
Law enforcement plans to fight against cybercrime	83%	17%
Law enforcement plans for training & education on cybercrime	71%	29%
Sub-departmental plans to enhance cyber capabilities	66%	34%
Cybercrime investigation for specialized units	86%	14%
Open-Source-Intelligence collection	78%	22%
Forensic analysis on computers	81%	19%
Mobile phone, malware, other high-tech	78%	22%
Cybercrime for managers and senior officials	51%	49%

C. Cyber training needs

Q. Does you organization provide an Online Learning System? (n=59)

- **Yes (38, 69%)**
- **No / Do not know (21, 31%)**

Q. To what extent would you "recommend" following courses to your organization to run? (1: Not at all – 5: Very much; n=59)				
	Mean	Std. dev	Min	Max
Crime scene and e-evidence collection (first responders' course for general officers)	3.65	1.47	1	5
Basic Internet Investigation (for general detectives)	3.35	1.46	1	5
Intermediate Cyber Investigation (for cybercrime detectives)	3.62	1.44	1	5
Cyber intelligence (OSINT, cryptocurrencies, darkweb patrol)	3.52	1.49	1	5
Digital forensics courses (for analysts)	3.89	1.33	1	5
IT course for police managers	3.28	1.53	1	5

D. Recruitment and partnerships

Q. To what extent do you agree or disagree with the following statements? (1: Strongly Disagree – 7: Strongly Agree; n=59)				
	Mean	Std. dev	Min	Max
My organization has a recruitment programme that recruits cyber experts from the private sector.	4.25	1.91	1	7
We can easily find experts in cybercrime or e-evidence.	3.86	1.95	1	7
My organization offers talent retention programmes (or career development paths) for existing experts to grow in the specialized field.	3.87	1.74	1	7
We get help from private sector companies.	3.50	1.90	1	7
We get help from universities on highly technical training.	3.61	1.85	1	7
We do NOT have domestic entities (public or private) who can help high-tech training.	3.38	1.70	1	7
My organization provides financial support for employees who need external training from private/foreign providers.	4.05	1.77	1	7
My organization takes train-the-trainer approach on cybercrime (talented colleagues teach others).	3.82	2.00	1	7

Survey participant countries/areas by region

Africa	Asia	Europe	Latin American and the Caribbean
Algeria	Bahrain	Austria	Argentina
Cameroon	Hong Kong	Bosnia & Herzegovina	Aruba
Congo, Dem. Rep	Indonesia	Czech Republic	Bolivia
Morocco	Iraq	Finland	Brazil
Niger	Japan	France	Chile
Senegal	Jordan	Greece	Colombia
South Sudan	Kazakhstan	Hungary	Dominican Republic
Tanzania	Korea, Republic of	Ireland	Ecuador
Tunisia	Lebanon	Italy	El Salvador
Uganda	Malaysia	Moldova	Guyana
Algeria	Palestine	Monaco	Mexico
Cameroon	Philippines	Netherlands	St Vincent & the Grenadines
Congo, Dem. Rep	Qatar	Poland	Uruguay
Morocco		Portugal	
		Romania	
		Serbia	
		Slovakia	
		Spain	
		Sweden	
		Switzerland	
		Ukraine	
		United Kingdom	
		Turkey	