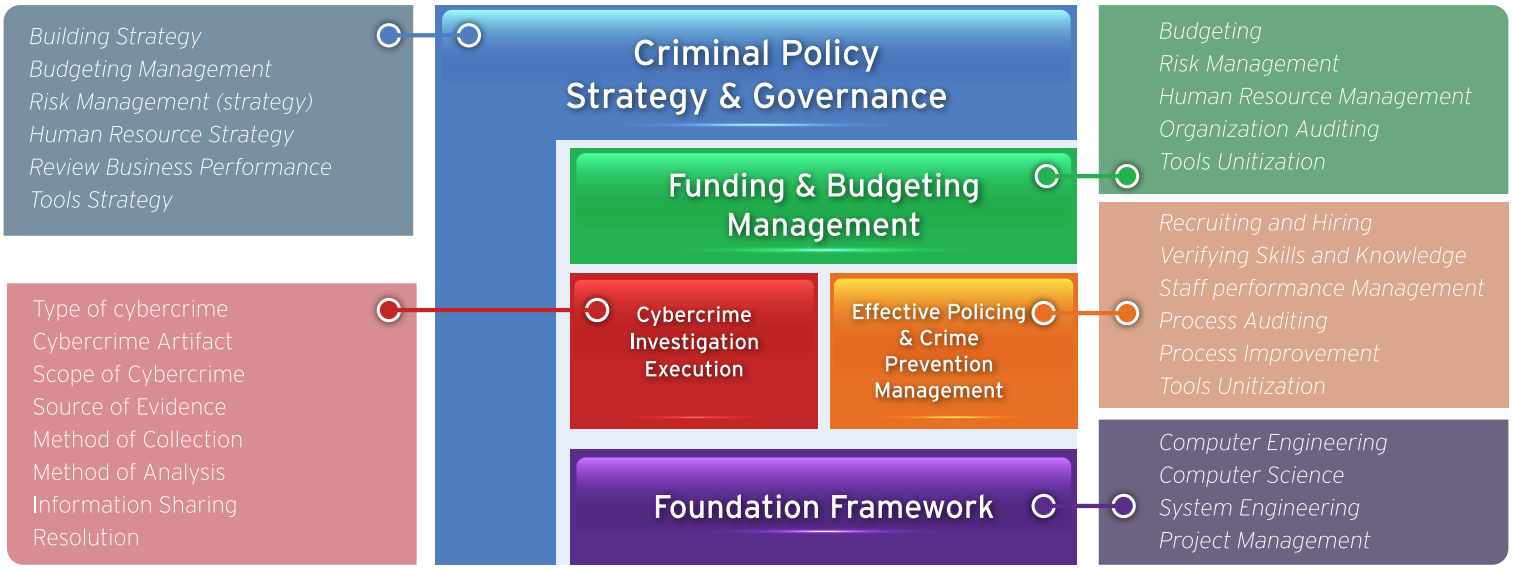
What is CIBOK

Cybercrime Investigation Body of Knowledge

Cybercrime Investigation Body of Knowledge is a guidance for knowledge on cybercrime investigation to show the systematic classification and organization regarding the knowledge, skills and approaches that must be commonly mastered in the implementation.

And it's able to be a part of the best framework for building up the organizational capability, by designing and operating the organization and linking the knowledge blocks into operation process.



CIBOK Macro Framework and Management Domains

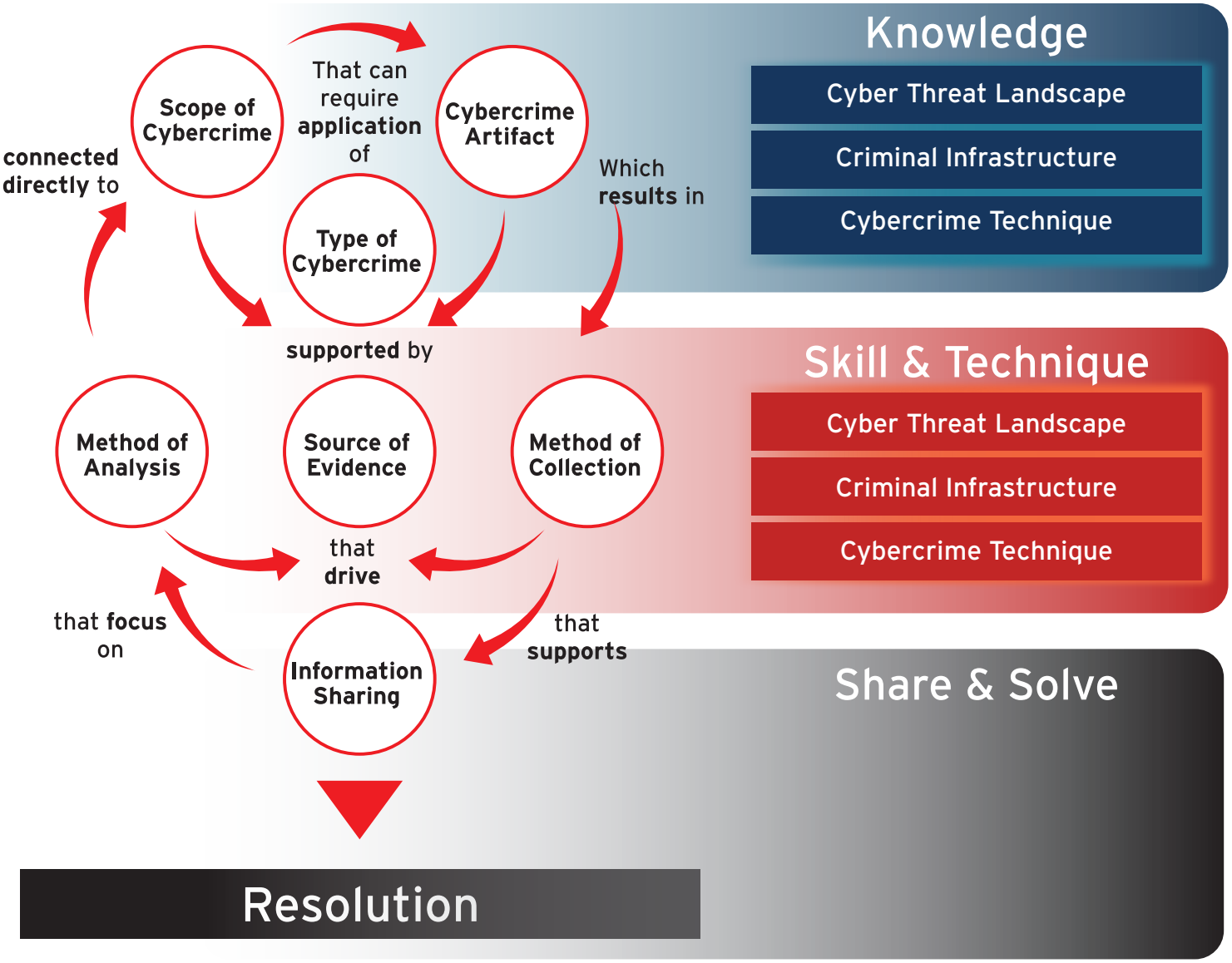
What's included in "Cybercrime Investigation Body of Knowledge"?

- Commonsense in cybercrime investigation
  - Consistent cybercrime investigations throughout the entire world
  - Participation of well-known authorities from worldwide, including reviews in development process.
- The positioning of other systematized customary practices
  - Demonstrating "Taxonomy"
  - Detailed demonstration in the scope of cybercrime investigations.
- Content that should be put into practice
  - Characterizing content that should be put into practice in cybercrime investigations.
  - Including how to utilize the topics concerning the contents.

Cybercrime Investigation Execution Framework

Cybercrime Investigation Execution Framework is one of the part of Cybercrime Investigation Body of knowledge.

It demonstrates positioning within the scope of other systematized customary practices and cybercrime investigations; these are classified in accordance with the cybercrime investigations execution framework, which is composed of the eight knowledge areas as below.



For more details, please contact: secretariat@cibok.org