

Framework

# The Intelligence Cycle in Action

How to apply this timeless approach in the modern world.

## Contents

### History

### Evolution

### Framework

### Steps

### Application

### Enhancement

Security threats have always evolved rapidly in government circles, in the military realm, and in the private sector. Those threats look different in the 21st century than they did decades ago, but the Intelligence Cycle is just as relevant and essential now as it was when first conceived.

The Intelligence Cycle is a time-honored framework that started as an exclusive tool for government agencies and military strategists. Today, it's also used to safeguard corporate interests, protect high-profile individuals, and navigate the complex tides of global geopolitics.

This guide outlines the Intelligence Cycle's purpose, phases, evolution, and modern applications. Continue reading for a deep dive into what the Cycle is and how it's used today. Then take the next step by learning about [Ontic's Integrated Research](#), a product purpose-built for intelligence teams to take action at each phase in the Cycle.


## The History of the Intelligence Cycle

The Intelligence Cycle's purpose was (and remains) to provide a structured and systematic approach for transforming diverse information into coherent intelligence. The goal is to equip security leaders to make informed decisions, ensuring that intelligence is accurate, unbiased, and actionable. Historically, this methodology was the domain of governments and militaries, serving as a vital tool for organizing efforts and resources in a manner that best addressed the needs of decision-makers.

Its roots can be traced back to Dr. Sherman Kent, whose journey in intelligence began during World War II with the Office of Strategic Services (OSS), the precursor to the Central Intelligence Agency (CIA). Kent's insights into the challenges of each step in the intelligence process led to the formalization of the Intelligence Cycle. The model he developed, grounded in his experiences and scholarly background, emphasized a repeatable, methodical approach to synthesizing information into valu-




able intelligence. This framework was embraced and refined by the CIA and subsequently permeated various levels of government and law enforcement, including the FBI and local and state agencies. Eventually, it found its place in the private sector, adapted to serve business contexts while retaining its core principles of efficiency and clarity in intelligence gathering and analysis.



*“The beauty of the Intelligence Cycle is that it’s very tactical but can also be very strategic to help keep you on track. And it’s constant — the wheel is always in motion.”*

– **Fred Burton**, Executive Director of Protective Intelligence, Ontic

## The Evolution of the Intelligence Cycle



The Intelligence Cycle has demonstrated remarkable resilience and adaptability over the years. Its core principles, deeply rooted in the methodologies established by early intelligence practitioners and theorists like Kent, have largely remained intact. That said, the way intelligence is collected, analyzed, and actioned has evolved significantly, particularly in the last few decades.

The advent of technology has introduced new dimensions to the Cycle. It enhances intelligence collection capabilities at a practical level. For example, license plate readers streamline the process of tracking vehicles that regularly drive by an office building or an executive’s home. Technology also supports rapid decision-making and dissemination of intelligence at levels that were impossible when the Cycle was first implemented. But it’s important to remember that technology will never replace the human element in the Intelligence Cycle. It will always need people to interpret, analyze, and follow up on information for ultimate effectiveness.

“The idea of the Intelligence Cycle is generic, but it works if you follow it,” Fred Burton said. “If you lay a technology stack on top of it, the Cycle becomes quicker and more dynamic.”

The broad adoption of the Intelligence Cycle beyond government and military circles into the corporate world is a testament to its fundamental efficacy. Events like the 9/11 attacks and subsequent global responses have underscored the necessity of a structured approach to intelligence in various sectors, including the private military and corporate security. Companies have learned that adherence to the basic principles of the Intelligence Cycle is crucial for effective decision-making. This understanding has driven the integration of the Cycle into corporate strategies, highlighting the importance of foundational intelligence processes even in a rapidly evolving world.

## The Intelligence Cycle Framework

Here's a snapshot of what the Intelligence Cycle looks like in action, including key questions and considerations as outlined by Ontic's security and intelligence experts.





## The Intelligence Cycle Steps

Each of these steps is vital to the Intelligence Cycle and requires careful execution and coordination to ensure the intelligence gathered is accurate, relevant, and actionable. Here's an explanation of what's included at each step, including key considerations and actions to take.

### 1 Planning and Direction

**Key question:** What are you trying to protect?

**The secret to success:** *Specificity.* Leadership must dictate what to look for as specifically as possible. This enables analysts to configure the appropriate resources.

This initial phase is foundational, setting the stage for what follows. The primary focus is on determining what exactly needs protection — be it a brand, a CEO, a physical location, or something else. This step drives the intelligence requirements for collection. The key here is specificity. Clear, directed questions shaped by organizational needs and stakeholder input pave the way for effective collection. This phase often involves examining company documents like 10-Ks for public corporations to define risks and [guide intelligence priorities](#). The planning and direction phase is about defining the scope and focus of the intelligence effort based on organizational needs and priorities.

### 2 Collection

**Key question:** What sources are at your disposal?

**The secret to success:** *Process.* Outline steps to take when issues emerge straight through to a post-event analysis that can help establish needed sources of information.

In this phase, the focus shifts to gathering the necessary information. Two critical questions emerge:

- What sources are available?
- Where are the gaps in these sources?

Efficient collection plans rely on the various sources available in our [new information landscape](#), including human intelligence and open-source data. Technology serves as a pivotal tool for centralization and seamless integration. Combining assorted data sources fosters a comprehensive understanding and prompts companies to customize their strategies based on specific intelligence needs and situational nuances. For example, an emergency evacuation plan demands different data considerations than long-term market analysis, requiring a security team to be agile, have foresight, and demonstrate a nuanced grasp of available intelligence source strengths and limitations. A well-structured process guides the entire collection journey, from issue emergence to post-event analysis, and aids in identifying missing sources and enhancing overall effectiveness.



As the central hub for these sources, technology empowers companies to build a holistic understanding while managing data availability and identifying information gaps. With technology in place, a security team can be more efficient in collecting data, which in turn allows the team to be more agile as it adapts to intelligence requirements and contextual nuances.

### 3 Processing and Exploitation

**Key question:** Are we on the same page?

**The secret to success:** *Alignment.* For the Cycle to be successful, actions taken at this stage must be fully aligned with what leadership cares about most.

Once the information is collected, it needs to be organized and made ready for analysis. Think of collection as creating a pile of information and processing/exploitation as organizing what's in that pile. This step involves converting raw data into a format that can be easily understood and analyzed by intelligence professionals. Everyone must be on the same page, with a clear, common understanding of the information at hand. To help organize the information effectively, there must also be full alignment between the matters that leadership cares about most and the processing/exploitation process. This phase serves as a bridge from collection to analysis/production, where data is prepared for deeper scrutiny and interpretation.

### 4 Analysis and Production

**Key question:** What actions are we taking?

**The secret to success:** *Focus.* Reporting at this stage must be succinct. If you can't explain the issue in three paragraphs, keep working at it until you can.

Here, the collected and processed information is critically examined to draw meaningful insights and answers to the question: What actions are we taking? Connecting the dots forms a coherent picture. Diversity in thought and perspective is crucial in this phase to avoid echo chambers and biased conclusions. The challenge is to distill complex information into concise, actionable intelligence that can be easily understood and used by decision-makers who don't have time to read beyond a few paragraphs. Analysts must check biases and remain open to various interpretations, ensuring a comprehensive and balanced analysis.

### 5 Dissemination

**Key question:** Who have I told, and who really needs to know?

**The secret to success:** *Connection.* Identify who you need to connect with, and then ensure your communications resonate with that target audience.



The final step involves distributing the intelligence to the right stakeholders in an effective manner. Tailoring the dissemination to the audience is key — what’s useful for one group may not be for another. The intelligence needs to be packaged and presented in a way that resonates with its recipients, whether they are executives, security personnel, or other stakeholders.

Feedback is essential. Intelligence teams need to know whether the audience is consuming intelligence or if alerts are getting deleted from inboxes immediately and without reading. The dissemination phase also requires careful consideration of privacy and security, ensuring sensitive information is only shared with those who truly need to know. For example, a founder/CEO may want private issues (like a stalker) limited to a finite group of people rather than shared with all corporate security.

### **Applying the Intelligence Cycle**

In the private sector, the Intelligence Cycle has been instrumental in addressing a range of security and strategic challenges, from executive protection to global risk management to [vendor due diligence](#). Companies leverage this framework to safeguard high-profile executives, considering threats from various angles and ensuring robust security measures. The Cycle’s role in geostrategic planning is equally significant. Businesses use it to navigate complex international landscapes, preparing for potential geopolitical upheavals that could impact operations or personnel. This is particularly vital for companies with a global presence, where understanding regional dynamics is key to safeguarding assets and employees.

The Intelligence Cycle can also be used to assist supply chains, a task highlighted by recent global events and shifts. Companies use the Cycle to anticipate and mitigate risks, whether they stem from political instability, natural disasters, or market fluctuations. This proactive approach enables them to maintain operational continuity and protect their interests effectively. The Cycle’s adaptability allows organizations to tailor it to various scenarios, whether it’s a single analyst using open-source intelligence for specific intelligence tasks or a broader team addressing corporate-wide security concerns. The Cycle is also flexible when used on different timelines. The steps can be applied just as effectively on a 24-hour cycle related to an emerging issue as they can be on a 30-day cycle related to ongoing intelligence efforts. In essence, the Intelligence Cycle empowers private entities to systematically gather, analyze, and act upon intelligence, ensuring informed decision-making and robust risk management in an increasingly complex and interconnected world.

*In the new information landscape, the Intelligence Cycle and its principles are more important than ever before. Our globalized, connected world means that issues can emerge at a moment’s notice.*



There are more data points and information to sift through than ever before. As Ontic's Fred Burton put it, "We have at times too much information, which becomes paralyzing." By applying the key questions and secrets to success as outlined in our Intelligence Cycle graphic, organizations can take a systematic, disciplined approach to the Intelligence Cycle that yields the best possible outcomes — no matter the intelligence and security issues that emerge.

## Enhance Your Intelligence Cycle With Ontic's Integrated Research

Embrace the full potential of the Intelligence Cycle [in 2024 and beyond](#) with Ontic's Integrated Research, a product purpose-built to empower intelligence teams at every step of the Cycle. Ontic's Integrated Research helps to make the Cycle continuous by delivering intelligence insights that combine real-time and historical data. With Integrated Research in place, you'll get:

- **Risk and intelligence reporting:** Connect data to rapidly tell intelligence stories through metrics and reports.
- **OSINT, dark web, and public data monitoring:** Access complete visibility and leverage always-on threat monitoring.
- **Identity research and management:** Eliminate manual processes and centralize your entity research and POI management.

You gain access to a wealth of information, including identity data, records of criminal activity, civil litigation, adverse media, and global public records — all consolidated in one intuitive platform. Whether it's for risk assessment, threat management, or strategic planning, Ontic's Integrated Research is your gateway to optimized intelligence operations. Elevate your team's capabilities to act on critical intelligence with precision and confidence.

Ready to modernize your security program?

Learn More About Ontic's Integrated Research [→](#)

 **ONTIC**