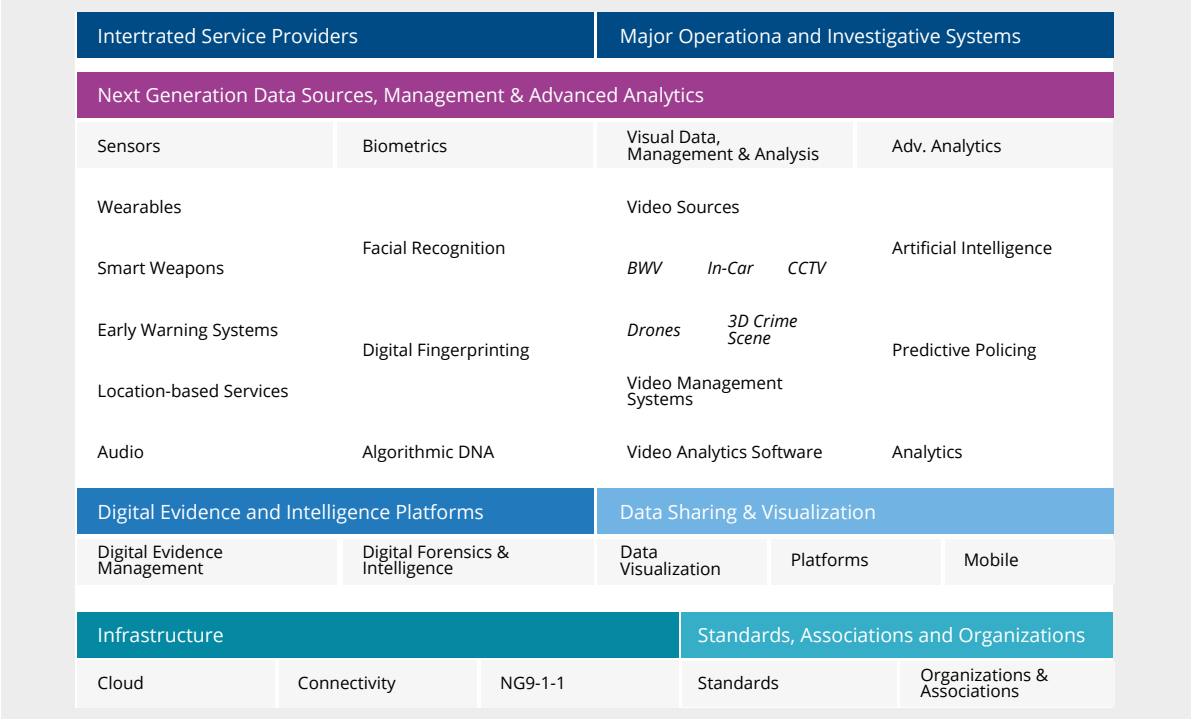
IDC ANALYZE THE FUTURE

IDC Government Insights

Guidelines for Successful Data-driven Policing Implementations

Data-driven policing refers to the process by which police agencies making decisions based on collected data that leverage cloud and advanced analytics to objectively unearth patterns, inform decision-making, improve process and actionable intelligence, and help agencies better allocate resources and understand their agency's focus.

However, generating insights and situational awareness is increasingly becoming unmanageable given not only the volume and variety of digital assets coming into agencies but also the velocity at which those digital assets arrive. This includes net-new data sources such as large, heterogenous data sets generated by communications service providers, cloud service providers, laptops, and smartphones, as well as the skyrocketing volume of video and photographic evidence.



IDC ANALYZE THE FUTURE

This complicates decision-making immensely and has led to the use of advanced AI-driven automated tools and technologies to navigate the digital deluge. At the same time, agencies are having to re-establish trust in policing in light of social justice protests, and address a burgeoning backlash against the use of technology to actively or passively surveil people.
Thus, agencies looking to optimize enterprise intelligence will also need to underpin their efforts by embedding trust across their workflow and technology. The focus of this checklist is to provide tangible guidance as to how to succeed on both fronts.

Trust

In this age of social justice reforms, and an increasing societal resistance to surveillance technologies, trust in policing is actualized by strategically enabling privacy, ethics and transparency, while securely mitigating public safety risks.

Drawing from IDC's AI Ethics Governance Framework, data-driven policing solutions and workflow must be:

- Fair: Algorithmically fair using unbiased data
- Explainable: To many stakeholders
- Robust: Safe, secure, and private, with a human in the loop
- Traceable: Understand the provenance of training data sets and metadata
- Transparent: Reporting in action, communication of results, and auditable
- Digital trust must address numerous facets: data integrity, transparency and oversight

Trust Checklist

DATA INTEGRITY

- ☐ **Diversify the data.** Much of the bias in AI solutions exists because the data sets used to train the solutions are limited in terms of volume or skewed in terms of gender, age, or ethnic diversity. Agencies implementing AI solutions should work with vendors that have taken the appropriate steps to use diversity-based data sets; agencies should also steer away from "black box" solutions, mass-market solutions that are both untested or unverified for bias. It should be noted that steps need to be taken to diversify the AI development talent pool as those individuals researching and developing AI tools are predominantly young white men, who introduce their own biased worldview.

DATA INTEGRITY CONT.

- [ ] **Collect more accurate and systematic data.** Data also needs to be diverse, as ethical AI must include multiple viewpoints for a well-rounded, fact-based approach.

OVERSIGHT

- [ ] **Establish oversight boards.** In addition to creating standards, proper oversight mechanisms and processes need to be put in place to ensure solutions are being ethically deployed.
- [ ] **Invest in automated solutions.** Consider augmenting these capabilities with monitoring software, but always have a human in the loop to scrutinize data collection and algorithmic decision-making.

Intelligence

Data and insights are paramount for any organization today. However, apart from having data in place and driving insights, organizations need to implement processes and technology to support good decision making, as data and decision making have become inseparable. IDC defines organizational intelligence as an agency's capacity to learn combined with its ability to synthesize the information it needs in order to learn and to apply the resulting insights at scale.

- **The ability to synthesize** information is the process of converting data into information and then into knowledge
- **The capacity to learn** refers to the awareness about and understanding the relationships among various pieces information and previously developed knowledge, and their application to a particular problem
- **The delivery of insights at scale** is defined as having decision support and decision automation capabilities for everyone in the enterprise, from agency executives and managers to analysts and front-line workers and machines

Artificial intelligence and machine learning are pivotal to delivering on all three components of organizational intelligence and is critical to forward-thinking data-driven policing. AI can be used to enhance/facilitate the experience citizens and residents have in communicating with public safety agencies, but it can also be used as a tool to improve first responder productivity, and lastly, it can be leveraged to accelerate workflow innovation.

INTELLIGENCE CHECKLIST

- ☐ **Add value, not volume.** Deliver trusted and actionable information in the context of the recipient. The ability to synthesize information does not mean delivery of more reports, dashboards, or other human-consumable indicators of past performance or current status of the enterprise.
- ☐ **Become a data-driven entity, both culturally and architecturally.** Focus on an evidence-based culture and an architecture that accommodates purpose-built components and services for different workloads and use case patterns. Security, trust and data ethics need to be built into the agency strategy, and the solutions that are architected and procured from the start.
- ☐ **Track ROI Metrics.** Organizations need to be disciplined in their approach to value measurement, setting a baseline and tracking meaningful progress by project and program over time.
- ☐ **Align your data-driven policing strategy with the bigger technology picture.** Ensure that you are collecting the right data to underpin other initiatives and use cases related to the digital transformation of policing (mobile tools, body-worn video, digital evidence management, digital forensics).

To learn more about Data-Driven Policing, read IDC's new eBook, *Data-driven Policing: Moving to Digital. Re-establishing Trust. Optimizing Efficiencies.*

For more information on the Worldwide Public Safety Transformation Strategies research, see the IDC report, *IDC Government Insights: Worldwide Public Safety Transformation Strategies*.