Criminal Justice Technology Adoption and Implementation Guide

Criminal Justice Technology Testing and Evaluation Center

A Program of the National Institute of Justice

NIJ | NATIONAL INSTITUTE OF JUSTICE

ADVANCING JUSTICE THROUGH SCIENCE

How to Use the Guide

The Criminal Justice Technology Adoption and Implementation Guide is a resource for criminal justice decision-makers who want to assess agency challenges and understand potential solutions. The guide provides criminal justice decision-makers with a resource to consider the technical, operational, and governance factors that accompany adoption and implementation of technology solutions. The guide is designed for a broad range of criminal justice decision-makers, including those in law enforcement, corrections, community supervision, and courts.

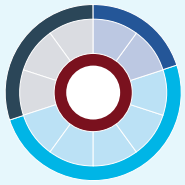
This guide has two parts. The first part focuses on problem analysis, helping criminal justice practitioners (CJPs) think through analyzing operational challenges and exploring potential solutions. The second part of the guide introduces a Criminal Justice Technology Adoption and Implementation Framework, which can help guide CJPs in adopting and implementing new technologies.

Part 1: Problem Analysis

Conduct Problem Analysis → Explore Potential Solutions → Identify Whether Technology Is Part of the Solution

Part 2: Adoption and Implementation Framework

If Technology Is Part of the Solution... → Consult the Criminal Justice Technology Adoption and Implementation Framework



About CJTTEC

The Criminal Justice Technology Testing and Evaluation Center (CJTTEC) is a program of the National Institute of Justice (NIJ) that uses research-based methodologies to enhance the capabilities of law enforcement, courts, and corrections agencies. CJTTEC leverages expertise from varied criminal justice community stakeholders to understand and test technologies and practices in a variety of NIJ's research areas.

This publication was made possible by Award Number 15PNIJ-23-GK-00931-NIJB, awarded by the National Institute of Justice, Office of Justice Programs, U.S. Department of Justice.

Suggested Citation: Camello, M., Gomez Cardoso, A., Krebs, C., Planty, M. (2025). Criminal Justice Technology Adoption and Implementation Guide. Research Triangle Park, NC: RTI International.

More Information:

Steven Schuetz
Senior Science Advisor/Physical Scientist
National Institute of Justice
U.S. Department of Justice
Steven.Schuetz@usdoj.gov
Tel +1-202-598-9388

Jeri D. Ropero-Miller, PhD, F-ABFT
Project Director, CJTTEC
RTI International
jerimiller@rti.org
Tel +1-919-485-5685

Problem Analysis

1 Define the Problem

Regularly convene stakeholders to identify emerging problems and issues throughout the year. During this step, agencies should assess whether each identified problem needs to be addressed, each problem's impacts, and what would happen if it was resolved or not resolved.

2 Gather Data and Engage Stakeholders

Gather quantitative and qualitative data related to the problem. Depending on the problem, this may include collecting data from a variety of sources and stakeholders (e.g., line-level officers, supervisors, community members), including administrative records, internal and external agency interviews or surveys, and community feedback.

3 Identify Causes

This step involves uncovering the underlying factors that contribute to the problem. Decision-makers should systematically explore each potential cause and its relationship to the problem, ensuring that they address the fundamental issues rather than just the symptoms.

4 Develop Targeted Solutions

Design targeted interventions or solutions that address the root causes of the problem. Interventions or solutions may include new or revised policies, procedures, or practices or new technology. Develop an implementation plan that outlines the steps, resources, and timeline required to execute the solutions.

Questions That Agencies Should Ask

- What issue are we facing?
- How do we know this is a problem? What are the indicators?
- What evidence supports this?
- Who is affected, and how are they affected?
- What are our goals in addressing this problem?
- What will success look like once this problem is resolved?

- What data do we currently have related to this problem?
- What additional data do we need to fully understand the problem?
- How reliable and accurate are our data?
- What trends and patterns can we identify from the data?
- Are there any gaps or inconsistencies in the data?
- What are the perspectives and insights of staff and other stakeholders?
- How does the community perceive this problem?

- What factors might cause this problem? What does research tell us about factors that contribute to the problem?
- How does each identified factor contribute to the problem?
- What external factors (e.g., socioeconomic, environmental) might influence the problem?
- Are internal processes or policies contributing to the problem?
- What proximal factors (e.g., opportunities) might influence the problem?

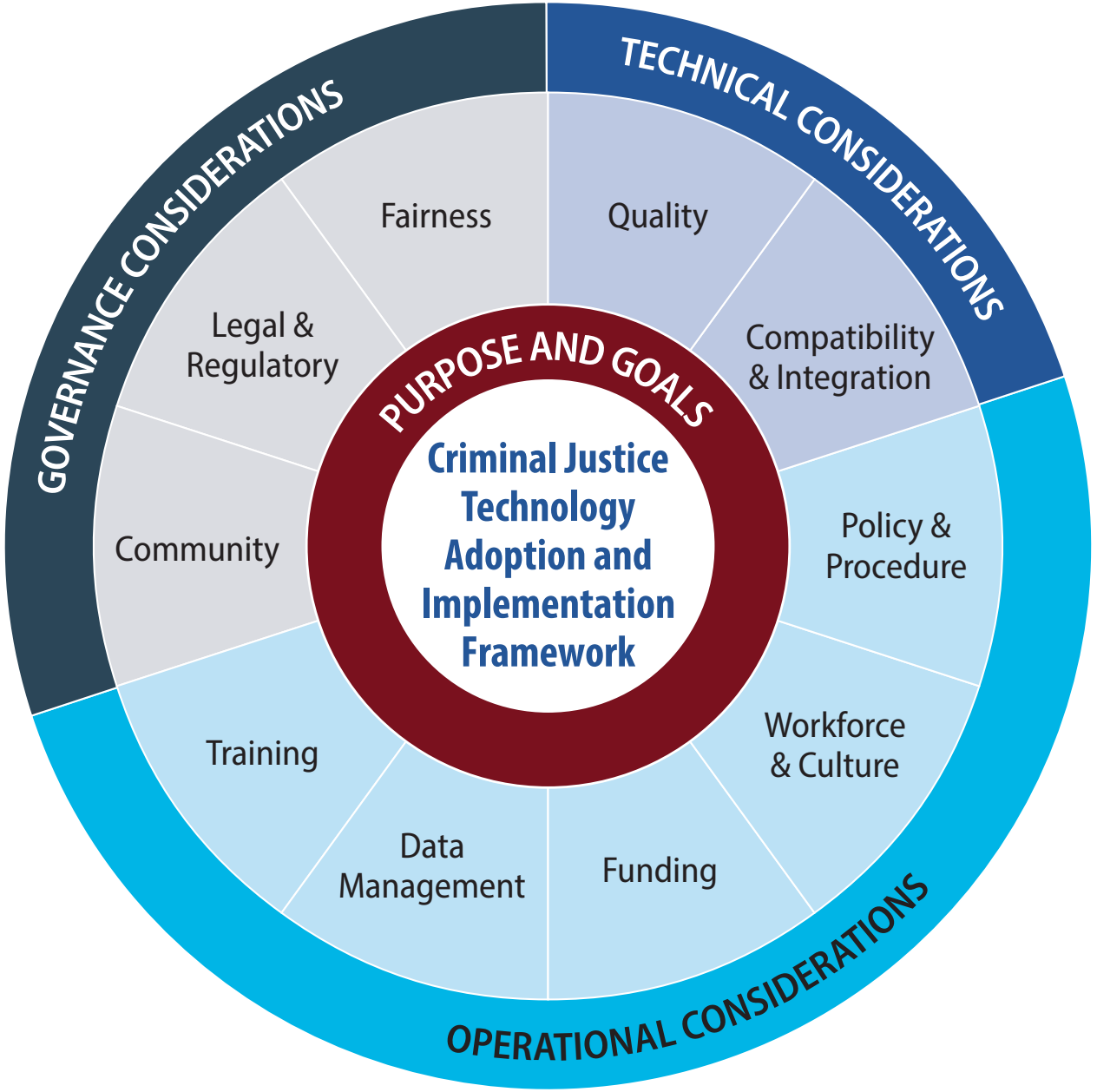
- What interventions or solutions can we design to address our problem? What does the research say? Have any technological solutions been shown to be effective?
- Could revised policies, practices, procedures, or technology address the root causes of our problem?
- Have others successfully adopted the proposed solution?
- What are the constraints for the different interventions or solutions?
- What do we know from research about using technology to deal with this problem (or a similar problem)?

Criminal Justice Technology Adoption and Implementation Framework

After completing these four steps—defining the problem, gathering data and engaging stakeholders, identifying causes, and developing targeted solutions—agencies may identify technology as a key component of their interventions. CJPs must ensure that the proposed technology not only addresses the identified problem but also is responsive to stakeholder concerns, while being feasible, fit-for-purpose, sustainable, and fair in its implementation.

To assist in this process, the Criminal Justice Adoption and Implementation Framework offers a structured guide for criminal justice decision-makers to assess the technical, operational, and governance implications of integrating new technologies. The framework helps agencies systematically evaluate whether the technology will meet their goals, address critical gaps, and align with community and operational needs.

Reviewing the components of the Criminal Justice Adoption and Implementation Framework will help CJPs assess the suitability of a given technology.



Purpose and Goals

An agency's core purpose and goals are the central tenet of the Criminal Justice Technology Adoption and Implementation Framework. This fundamental principle ensures that technology adoption is part of a strategic solution to enhance the agency's ability to fulfill its mission and serve the community.

When considering new technologies, CJPs should first reflect on their primary objectives, such as maintaining public safety, upholding justice, reducing recidivism, or improving operational efficiency. Each potential technological solution should be evaluated against its ability to directly achieve these goals. To prevent civil liberties infringements and mission creep, CJPs must define upfront how and why the technology will be used. By clearly delineating the technology's use case and purpose from the outset, agencies can establish proper guidelines, policies, training protocols, and accountability measures, thereby mitigating risks and enhancing public trust.

A new technology may be flashy and enticing, particularly to agencies in desperate need of a solution for a clearly identified problem. But technologies should only be adopted and implemented where the technology is an appropriate solution. The purpose and goals component of the framework helps prevent the adoption of unnecessary or ineffective technologies, while helping CJPs focus resources on technology solutions that genuinely advance their mission.

Questions That CJPs Should Ask: Purpose & Goals

What problem is the agency trying to address?	What are the key elements of my agency's overall mission?	How will this technology advance—or detract from—my agency's larger objectives and mission?
How does the purpose for wanting to adopt this technology align with the goals my agency is trying to achieve?	What is the goal of using this technology?	What desired outcomes might be accomplished by adopting this technology? How likely are these outcomes? How will the decision-maker measure those outcomes?

Technical Considerations

The framework's technical considerations component outlines the technical factors that CJPs need to consider before adopting and implementing a new technology. Considerations include both the technology infrastructure (e.g., hardware, software) and how well it performs. Within the framework, the technical considerations component focuses on two key subcomponents:

- **Quality:** Evaluate the dependability of the new technology to produce accurate and reliable results that align with its intended function.
- **Compatibility and Integrations:** Assess how well the new technology can work within the existing technological ecosystems. Decision-makers need to consider the technology's ability to interface with current systems, databases, and processes. This assessment includes evaluating data exchange capabilities, application programming interface (API) availability, and the ease of integrating the new technology into existing workflows.

Questions That CJPs Should Ask: Technical Considerations

Quality

- How reliable and accurate is the technology, and what measures ensure its reliability?
- Has the technology been validated and tested in a rigorous and transparent manner by an outside party? What has been the experience of other agencies that have adopted the technology?
- Are specific metrics in place to measure the quality and performance of the technology within my agency?
- Does the technology accomplish the requirements? How does it fall short?

Compatibility and Integration

- Is existing organizational infrastructure compatible with the technology?
- Can the technology integrate with other systems (e.g., computer aided dispatch [CAD], records management system [RMS])?
- What technical expertise is required to integrate the new technology effectively?
- Have the potential risks of interoperability and integration (e.g., privacy concerns) been thoroughly assessed?

Technical Considerations: Examples

Example Technical Questions CJPs Should Ask for Different Technologies

	Smartphone Applications for Community Supervision	Contraband Detection Technology for Correctional Facilities	Automated License Plate Readers (ALPR) for Law Enforcement
Quality	• What is the app provider's track record in terms of addressing bugs, system crashes, or other technical issues that may impact daily operations? • How well does this app function across the range of smartphones that clients may already own? • Does the app accurately know the smartphone's location? • Does the app meet data security and restricted access requirements?	• What is the accuracy rate of this contraband detection technology? Have other agencies reported reliable detection in real-world scenarios? • How does the technology handle environmental variables (e.g., lighting, temperature, interference) that could impact detection accuracy? • How frequently do false positives or false negatives occur, and how are they mitigated to ensure reliable use in the field?	• How accurate are the ALPR systems in identifying and reading license plates in various environmental conditions, such as rain, fog, or darkness? • How consistent is the performance of the ALPR system across different types of vehicles, speeds, and distances from the cameras? • What is the system's error rate in terms of misreading plates or failing to capture license plates?
Compatibility and Integration	• How easily can the app integrate with current systems (e.g., case management software, GPS monitoring tools)? • What upgrades or changes to our existing infrastructure will the app require? • Does the app facilitate communication and data sharing between agencies and other entities such as courts, law enforcement, or treatment providers?	• How well does this contraband detection technology integrate with the currently used tools and systems (e.g., body scanners, metal detectors, drug testing kits)? • Will this technology require any additional infrastructure or hardware upgrades to function effectively?	• How easily can the ALPR system integrate with a department's existing databases, such as vehicle registration, wanted vehicle lists, or stolen car records? • Does the ALPR software interface with other law enforcement tools, such as CAD? • Will the ALPR system be compatible with systems used by neighboring jurisdictions or state agencies to allow for data sharing? Is there a data sharing agreement in place outlining clear parameters for use? • Can the ALPR system integrate with already-used third-party crime analysis or investigative software, such as facial recognition or suspect-tracking systems?

Operational Considerations

The framework's operational considerations component highlights the organization-specific operational factors that CJPs need to consider before adopting and implementing a new technology. The operational considerations component focuses on five key subcomponents: policies and processes, workforce and culture, funding, data management and governance, and training.

- **Policy and Procedure:** Assess how the technology will impact workloads and how it will integrate into internal processes. CJPs may need to consider creating or updating organizational guidelines and workflows to accommodate the new technology.
- **Workforce and Culture:** Assess how the technology will impact staffing, culture, and organizational morale.
- **Funding:** Consider the financial resources needed to purchase and maintain the technology, and where those resources will come from. CJPs need to consider all the costs associated with the technology, including upfront costs, operating costs, and maintenance costs.
- **Data Management and Governance:** Establish protocols for data collection, protection, storage, access, and sharing in compliance with relevant regulations. This also includes defining data ownership, quality control measures, and policies for data retention and disposal.
- **Training:** Develop training programs to ensure all relevant staff can effectively use and manage the new technology.

Questions That CJPs Should Ask: Operational Considerations

Policy & Procedure

- Are new or updated policies and procedures needed to deploy and use the technology?
- Is approval needed by a local governing body (e.g., city council) to procure and use the technology?
- Are procedures in place to prevent and identify potential misuse of the technology?
- Are policies in place to ensure the technology is regularly audited?

Workforce & Culture

- How will work routines and workload change if the technology is adopted?
- Are mechanisms in place for collecting workforce feedback about their experiences with the technology?

Funding

- What are the initial and recurring financial costs associated with the technology?
- How will funding be sourced, and what financial resources are available for the adoption?
- Are any potential long-term cost savings expected from the adoption of this technology?
- How will ongoing maintenance, upgrades, and support costs be managed?

Data Management

- Who has access to the system?
- Where are the data stored?
- Can the vendor ensure that the data are secure?
- Who owns the data?
- Does a privacy impact assessment need to be conducted?

Training

- What training is required on the use of the technology?
- Who, other than users (e.g., supervisors, IT personnel), need training?

Operational Considerations: Examples

Example Operational Questions That CJPs Should Ask for Different Technologies

	Smartphone Applications for Community Supervision	Contraband Detection Technology for Correctional Facilities	ALPR for Law Enforcement
Policy & Procedure	• How does the app align with current policies on supervision, monitoring, and reporting? • How will the app be integrated into routine supervision workflows, and how will this affect reporting and decision-making processes?	• How does the new contraband detection technology align with our existing facility policies on searches and contraband management? • How will a technology-based detection system affect or interface with our processes and security systems, policies, and reporting protocols?	• What specific policies will govern the use of ALPR technology, including when and where it can be deployed and for what types of investigations? • What policies are needed to ensure ALPR technology is not used for purposes beyond its intended scope? What policies and procedures are in place to minimize human errors (e.g., failure to update databases, failure to notice discrepancies in matches)? • What oversight mechanisms are needed to ensure ALPR data are used responsibly and in compliance with established policies?
Workforce & Culture	• How will the app change the daily duties of community supervision personnel?	• How will the use of detection technology change personnels' day-to-day responsibilities? • How will the use of detection technology impact officer or staff safety?	• What steps are required to ensure that all relevant personnel understand how ALPR technology can support their work?
Funding	• What is the total cost of purchasing, customizing, and deploying the app for our agency? • What ongoing costs are associated with the app (e.g., software updates, tech support, data storage)? • What funding streams are available to support the adoption and implementation of the app?	• What is the available budget? Would a lower-cost solution achieve our primary objectives? • What costs are associated with purchasing or leasing, operating, and maintaining the system?	• What are the upfront and ongoing costs associated with acquiring, implementing, and maintaining ALPR technology? • What funding is required for both the initial purchase of the technology and the long-term maintenance and updates?
Data Management	• What types of data will the app collect from users? • What security protocols are in place to protect the data collected by the app? • Who owns the data, and in what format are they stored? Does the vendor comply with city/state data retention policies? • Can the data be integrated with other systems? • How will sensitive information, such as location tracking or communication logs, be safeguarded from unauthorized access or breaches?	• What data will be retained from the technology? • Can the technology integrate with other security technologies, such as body scanners, metal detectors, and video surveillance? • Can the technology facilitate information sharing between correctional facilities, law enforcement, and other agencies?	• What policies will govern how long ALPR data are stored? What happens when the retention period elapses? • What measures are needed to ensure that ALPR data are stored securely and that only authorized personnel can access them?
Training	• Can any vendor-provided training resources (e.g., webinars, tutorials, technical support) help reduce the training burden on the agency? • What resources will be available to help users learn how to use the app effectively? • What ongoing training or support will be available to personnel after the app is implemented?	• What type of training will be required to ensure that officers and staff are fully equipped to use the detection technology effectively? • Will personnel need training on how to explain the use of contraband detection technology to inmates and visitors?	• What specialized training is required to ensure officers understand how to use ALPR technology effectively and within legal guidelines? • Do ALPR vendors offer training?

Governance Considerations

The framework's governance considerations component highlights the broader impacts and implications that CJPs should consider when planning and implementing technologies. These factors extend beyond an organization's internal operations, emphasizing their impact on people and public trust. The governance considerations component focuses on three key subcomponents:

- **Fairness:** Evaluate the technology's impartiality, ensuring constitutional protections and fair treatment of all groups.
- **Community:** Evaluate how decisions will affect the community. CJPs need to consider the potential benefits and drawbacks of their actions on public safety, community well-being, and their relationship with the community.
- **Legal & Regulatory Compliance:** Examine whether the technologies align with existing laws and regulations. CJPs must ensure that their actions comply with legal standards and must consider the potential for any legal challenges or conflicts with civil rights protections.

Questions That CJPs Should Ask: Governance Considerations

Fairness

- What potential biases may arise or be exacerbated from the implementation of this technology, and how can they be mitigated? Are there legitimate, nondiscriminatory reasons for the disparity (e.g., higher crime rates in a given area)?
- Can this technology decrease bias and enhance fairness?
- What are the potential unintended consequences of deploying this technology for different communities?
- Has any research been done on how the technology might impact vulnerable communities?

Legal & Regulatory

- How does this technology align with existing laws and regulations? Do any laws prevent or regulate criminal justice use of the technology?
- Are any potential legal risks associated with the technology's implementation, and how will they be mitigated?
- Does the technology meet CJIS requirements?
- What are the potential implications on privacy and civil liberties?

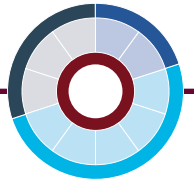
Community

- How will the implementation of the technology benefit public safety?
- Has your agency engaged in public outreach about the technology, particularly among groups most likely to be impacted?
- Will the implementation of the technology impact community trust?
- How would different communities likely react if the technology were to be implemented?
- What concerns might communities have about the use of this technology?
- Are mechanisms in place to gather feedback and input from various communities regarding the technology's purpose and implementation?
- How will the technology help or harm people (including personnel)?
- Who is responsible for the consequences of the technology?
- What are community perceptions of the technology?

Governance Considerations: Examples

Example Governance Questions That CJPs Should Ask for Different Technologies

	Smartphone Applications for Community Supervision	Contraband Detection Technology for Correctional Facilities	ALPR for Law Enforcement
Fairness	• How is access to the app for all individuals under supervision ensured, especially those who may lack access to smartphones or reliable internet? • How will the app account for different cultural and linguistic needs? Will it be available in multiple languages and adaptable for users with varying levels of digital literacy?	• Are there safeguards in place to ensure that the technology is used consistently and fairly across all inmates, without bias in detection or enforcement? • How will false positives be addressed?	• What guardrails are needed to ensure that ALPR technology is not disproportionately deployed in or targeting certain neighborhoods, especially vulnerable communities? • Are there procedures in place to regularly assess the technology's impact across different geographic and demographic areas?
Community	• How will the community of individuals under supervision perceive the use of the app? Will they view it as a tool for support or as a form of invasive surveillance? • Have you considered how to engage with individuals under supervision to understand their concerns or hesitations about using this technology? • How will the app balance the need for accountability (e.g., tracking appointments or curfews) with its potential to provide support and resources for individuals under supervision?	• What are ways to communicate the benefits of this technology to external stakeholders, including families of inmates, to build trust and understanding? • Have you engaged with prisoner rights groups, civil liberties organizations, and other community advocates regarding the adoption of this technology?	• Have you considered educating the public about the purpose and use of ALPR technology, ensuring transparency about how the data are collected, stored, and used? • How are community concerns around increased surveillance and privacy violations addressed? What safeguards are in place to maintain public trust?
Legal & Regulatory	• How does the app comply with federal, state, and local privacy laws regarding data collection and surveillance of individuals under supervision?	• Are there federal or state regulations that govern the use of contraband detection technology in correctional facilities? • How will the contraband detection process respect the dignity and personal privacy of inmates, particularly during body scans or searches?	• What are the legal guidelines for retention of ALPR data? • Are there scenarios where the use of ALPR technology might be ethically unjustifiable, and how will we identify and avoid such situations? • What are the legal restrictions on sharing ALPR data with other agencies or third parties?



Questions That CJPs Should Ask Before Technology Adoption and Implementation

This page provides a quick-reference resource, with key questions for each framework component, to support CJPs in evaluating and implementing new technologies.

Purpose and Goals

- What problem is the agency trying to address?
- What outcomes do the decision-makers hope to accomplish by adopting this technology? How will the decision-makers measure those outcomes?
- How will this technology advance the agency's overall objectives and mission?
- How is the purpose for adopting this technology aligned with the agency's overall objectives and mission? What is the goal of using this technology?

Technical Considerations

Quality

- How reliable and accurate is the technology, and what measures are in place to ensure its reliability?
- Has the technology been validated and tested in a rigorous and transparent manner by an outside party? What has been the experience of other agencies who have adopted the technology?
- Does the technology accomplish the requirements? How does it fall short?
- Are specific metrics in place to measure the quality and performance of the technology within my agency?

Compatibility and Integration

- Is existing organizational infrastructure compatible with the technology?
- Can the technology integrate with other systems (e.g., CAD, RMS)?
- What technical expertise is required to integrate and manage the new technology effectively?
- Has there been a thorough assessment of the potential risks of interoperability and integration (e.g., privacy concerns)?

Operational Considerations

Funding

- What initial and recurring financial costs are associated with the technology?
- How will funding be sourced, and what financial resources are available for the adoption?
- Are any potential long-term cost savings expected from the adoption of this technology?
- How will ongoing maintenance, upgrades, and support costs be managed?

Workforce & Culture

- How will work routines and workloads change if the technology is adopted?
- Are mechanisms in place for collecting workforce feedback about their experiences with the technology?

Policy & Procedure

- Are new or updated policies and procedures needed to deploy and use the technology?
- Is approval needed by a local governing body (e.g., city council) to procure and use the technology?
- Are procedures in place to prevent and identify potential misuse of the technology?
- Are policies in place to ensure the technology is regularly audited?

Data Mgmt

- Who has access to the system?
- Where are the data stored?
- Can the vendor ensure that the data are secure?
- Who owns the data?

Training

- What training is required on the use of the technology?
- Who, other than users (e.g., supervisors, IT personnel), need training?

Governance Considerations

Fairness

- What potential biases or disparities may arise from the implementation of this technology, and how can they be addressed?
- Can this technology decrease bias and enhance fairness?
- Are procedures in place to protect individuals from potential misuse of the technology?
- What are the potential unintended consequences of deploying this technology, particularly in vulnerable communities?
- Has any research been done on how the technology might impact vulnerable communities?

Community

- Are mechanisms in place to gather feedback and input from communities about the use of the technology prior to implementation?
- How will the implementation of the technology benefit public safety?
- Will the implementation of the technology impact community trust?
- How would various groups likely react if the technology were to be implemented?
- What concerns might different communities have about the use of this technology?

Legal & Regulatory

- How does this technology align with existing laws and regulations? Do any laws prevent law enforcement from using this technology?
- What are the potential implications on privacy and civil liberties?
- Are any potential legal risks associated with the technology's implementation, and how will they be mitigated?

Additional Resources for CJPs to Explore

Other Technology Adoption and Implementation Guides/Toolkits

Christoff, T.E., Hickman, S., Thorkildsen, Z., Jenkins, M., Lafferty, J., Gutierrez, M., & Melendez, H. (2024). *Technology implementation guide. Addressing crime through innovative technology*. Washington, DC: Office of Community Oriented Policing Services. https://portal.cops.usdoj.gov/resourcecenter/content.ashx/cops-r1169-pub.pdf

Criminal Justice Policy Program at Harvard and Stanford Criminal Justice Center. (2020). *Emerging police technology: A policy toolkit*. https://law.stanford.edu/wp-content/uploads/2020/01/Emerging-Police-Technology-A-Policy-Toolkit.pdf

Problem Analysis

Bynum, T. S. (2001). *Using analysis for problem-solving: A guidebook for law enforcement*. Office of Community Oriented Policing Services. https://portal.cops.usdoj.gov/resourcecenter/content.ashx/cops-p018-pub.pdf

Clarke, R. V., & Schultze, P. A. (2005). *Researching a problem*. Office of Community Oriented Policing Services. https://popcenter.asu.edu/sites/default/files/researching_a_problem.pdf

Henson, N. (n.d.). *Problem solver's handbook*. https://popcenter.asu.edu/sites/default/files/problem_solving_handbook_june_2020_usa_version.pdf

Hollway, J., Lee, C., & Smoot, S. (2017). Root cause analysis: A tool to promote officer safety and reduce officer involved shootings over time. *Villanova Law Review*, 62(5), 883-924. https://www.villanovalawreview.com/api/v1/articles/13232-root-cause-analysis-a-tool-to-promote-officer-safety-and-reduce-officer-involved-shootings-over-time.pdf

Scott, M. S. (2015). *Identifying and defining policing problems. Problem-oriented guides for police, problem-solving tools no. 13*. Office of Community Oriented Policing Services. https://popcenter.asu.edu/sites/default/files/identifying_and_defining_policing_problems.pdf