eBook

Under Pressure: How Public Sector Organisations Can Rise to the Challenge of Secure Digital Transformation

Checkmarx

Introduction

Public sector organisations worldwide face a daunting set of challenges as society adjusts to the current COVID-19 environment. Whether it is local government, healthcare, law enforcement, or blue light responders, organisations across all disciplines that previously depended on in-person processes have been forced to pivot to digital alternatives at an uncomfortable speed.

In the space of a year, society has transformed beyond recognition and digital-first is now imperative. As a result, demand for public services application development is outstripping available coding and security expertise. Citizens urgently need digital-based public services so they can continue their lives in a world that appears unlikely to return to the familiar processes of the past. At the same time, the ever-present squeeze on public finances means resources are limited and any proposed investment must guarantee cost-savings and efficiency.

Lack of financial and human resources is not the only problem. Public sector organisations handle a wealth of sensitive personally identifiable information (PII), so any software application with access to this PII data must meet the high security standards demanded by regulation such as the EU GDPR and US CCPA. Beyond regulation, the functioning of society depends on citizen trust in the institutions that serve them. An organisation releasing vulnerable code risks breaching public trust and exposing itself to considerable fines and legal repercussions.

Ultimately, user expectations of digital services have never been higher. The need to deploy secure, public service-oriented applications is accelerating, but these applications need to match the exceptional usability experienced in the consumer space. Citizens have no patience for clunky, unintuitive experiences… and why should they? After all, it is public money that pays for them.

These cumulative and sometimes competing pressures create a considerable conundrum for the public sector: how to rapidly deploy secure, high-functioning, stable software that delivers future-proofed public services, with limited resources? And with public finances under pressure, how can public sector leaders build the case for software investment that equally prioritises application security with delivery and deployment speed?

This eBook examines the elements of the digital public services environment and how organisations can meet their obligations to citizens by building effective, secure software.

Table of Contents

Competing Priorities Put Pressure on Software Development Teams

COVID-19: A Catalyst for Permanent Change

In the context of digital transformation, the public sector has historically taken longer to adopt innovation compared to its private sector counterparts. This is often driven by the need to focus on immediate service priorities and deliver essential services to a heterogeneous citizen base that likely includes many people with limited digital skills and access - such as the elderly, low-income, and vulnerable populations - which has acted as a brake on innovation. Funding is often prioritised towards maintaining existing services that, while lacking the efficiency of digital alternatives, are familiar to users.

The stakeholders accelerating public sector digital transformation

Within the sector, there are two groups that are likely to press to maintain and accelerate digital transformation.

1. The digital natives within government entities are likely to want to keep their foot on the gas pedal of change and maintain these advances.

2. The private sector and citizens who have become much more used to working online and are therefore becoming more demanding around ease of access to services and the usability of digital apps.

Mike Stone, Global Head of Technology Transformation for Infrastructure, Government and Healthcare, KPMG

Devoting investment to large-scale digitisation projects has required a leap of faith that many civil servants felt uncomfortable in making. As a result, while pockets of digitisation have grown over recent years and many governments are pushing digital transformation at a strategic level, many citizen-facing processes continue to rely on in-person interactions.

COVID-19 flipped this overnight. With municipal buildings, courts, doctors' surgeries, and police stations closed to the public, in-person services ground to a halt. Everything from unemployment benefit applications, medical appointments, and education, to planning applications and crime reports had to take place digitally, or not at all. Citizens have been forced to adapt and those who may have resisted a change to familiar processes are now more open to digital alternatives; COVID-19 has proved a catalyst for permanent change. We stand on the cusp of a significant opportunity to transform the relationship between citizens and the state, but this brings its own challenges.

The enforced switch to digital alternatives is pressuring overburdened software development teams to build greenfield applications where none existed, and to rapidly scale the applications already in place. The applications they develop must offer seamless, intuitive experiences that meet user expectations shaped by digital giants like Amazon, which have set the bar incredibly high. Citizens want their interactions with government services to be as easy, intelligent, and responsive as online shopping, but when you bear in mind that today's retailers are releasing new software builds weekly, daily, and even hourly, you can appreciate the scale of the task at hand.

As a result of this rising demand and high expectations, application development, delivery, and deployment time frames are shorter than ever, and many organisations are adopting Agile fundamentals and the continuous integration and continuous delivery (CI/CD) processes of DevOps to meet the required pace.

Skills Shortages and Outsourcing Changes Make Talent Hard to Find

High demand for both developer and security expertise as a result of the rapid shift to digital is making it hard for public sector organisations - with lower budgets than private companies - to recruit and retain the skills they need to meet digitisation ambitions.

At the same time, the move to disaggregate outsourcing contracts to avoid dependency on single suppliers is affecting accessibility to developer and security skills that were previously provided under such contracts.

To address the shortfall, organisations need to deploy application security solutions that fit within development processes, allowing existing developer teams to increase their efficiency in creating secure code without negatively affecting delivery schedules.

Regulatory concerns in a high-risk environment

As custodians of high value personal and special category data - from medical records and criminal records to social security numbers - public sector organisations are firmly in the sights of privacy regulators. With HIPAA already an established standard in healthcare and privacy regulations such as GDPR and CCPA now well into the enforcement phase, any new digital services must incorporate security by design and default, and that begins in the software development phase.

The privacy legislation juggernaut shows no sign of slowing on either side of the Atlantic. The need for a federal approach to privacy in the US is recognised on both sides of the floor and various bills have been introduced over the past 18 months to this effect. Though the COVID-19 crisis has diverted focus, the International Association of Privacy Professionals predicts that President Biden will renew the push for legislation.

It is not just regulators that are concerned over privacy. The comprehensive public campaigns that accompanied the implementation of the GDPR and CCPA have raised citizen awareness of their data protection rights to levels previously unheard of. And this applies even more acutely to public services, which must be rooted in trust in order to serve a functioning society.

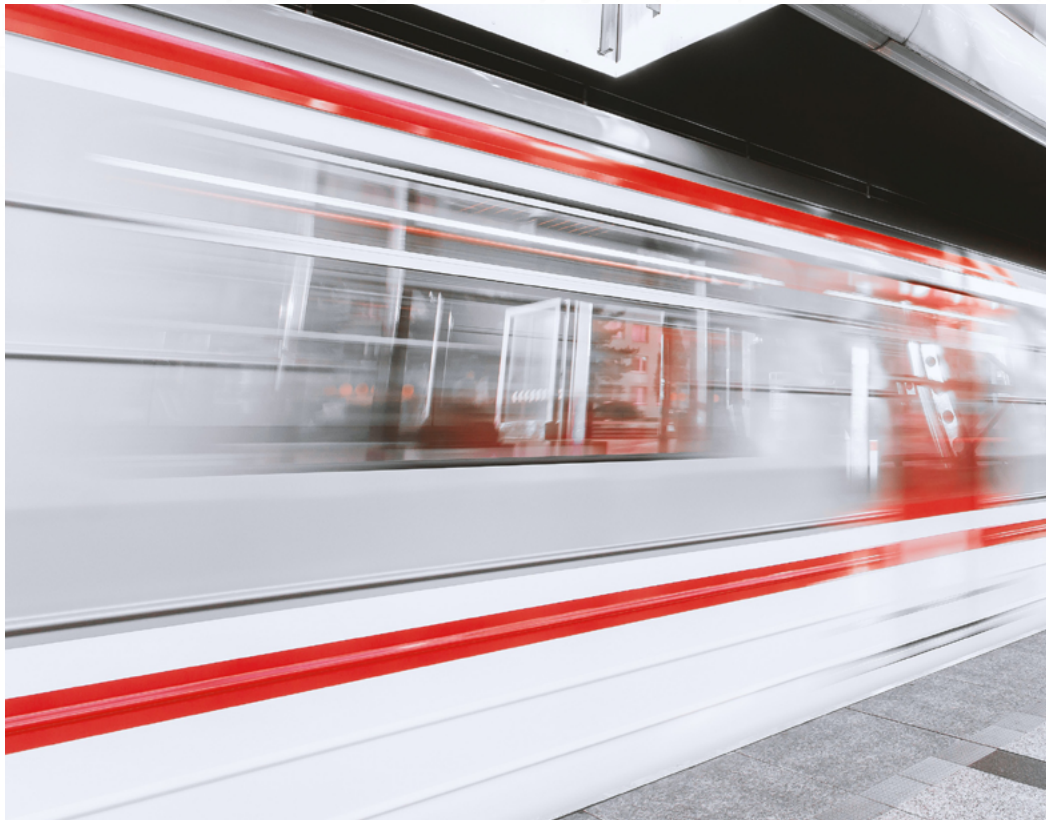
On the flipside of regulation is risk. The disruption caused by COVID-19 has encouraged a surge in cyber attacks targeting high value personal data for financial gain. Consequently, any application that expands the attack surface must incorporate robust security checks to keep attackers from infiltrating applications and extracting data.

These pressures in combination mean that security cannot be an afterthought to new software development. It must be an intrinsic to the process by incorporating application security testing measures and implementing vulnerability mitigation techniques before software makes its way into production.

The Application Development Dilemma – Speed Vs Security

The real-world impact of the urgent drive for digitisation on one hand, and the imperative for security and data protection on the other, is nowhere more apparent than in the tension between software developers and security teams.

The speed with which software teams are required to develop and release code, and the DevOps approach used to achieve this, can result in a security readiness gap where security may be compromised in a trade-off against speed. Research suggests that four out of five organisations have regularly or occasionally pushed code to production with known organic vulnerabilities . Of these, over half said they did so to meet a critical deadline and planned to fix the issue in a later release. **Concerningly, 81% of the same research cohort said production applications had been exploited in the preceding 12 months.**



Protect the integrity of your source code and other artefacts from day one right through to deployment. Test that you've secured it properly.

The UK's National Cyber Security Centre (NCSC) emphasises the imperative for intrinsically secure code.

National Cyber Security Centre

Traditionally, many public sector organisations have utilised pentesting approaches to help verify that some level of application security was being met. Often this activity was performed by third parties; **however**, this approach simply cannot scale when organizations need to develop, deliver, and deploy software at speeds that are required when needing to fast-track digitisation to serve their communities better. Clearly, pentesting has many shortcomings in contrast to today's software release velocity requirements.

Another approach some organisations have taken to validate that applications were secure was to test them once they were running using Dynamic Application Security Testing (DAST) approaches. **However**, DAST does not always fit well within Agile and DevOps methodologies since it almost always adds measurable delays. If DAST does detect a critical vulnerability that must be remedied before deployment requires developers to go back and fix vulnerabilities in code they may have worked on days, weeks, or even months ago. This dilemma only serves to add additional friction between development and security teams.

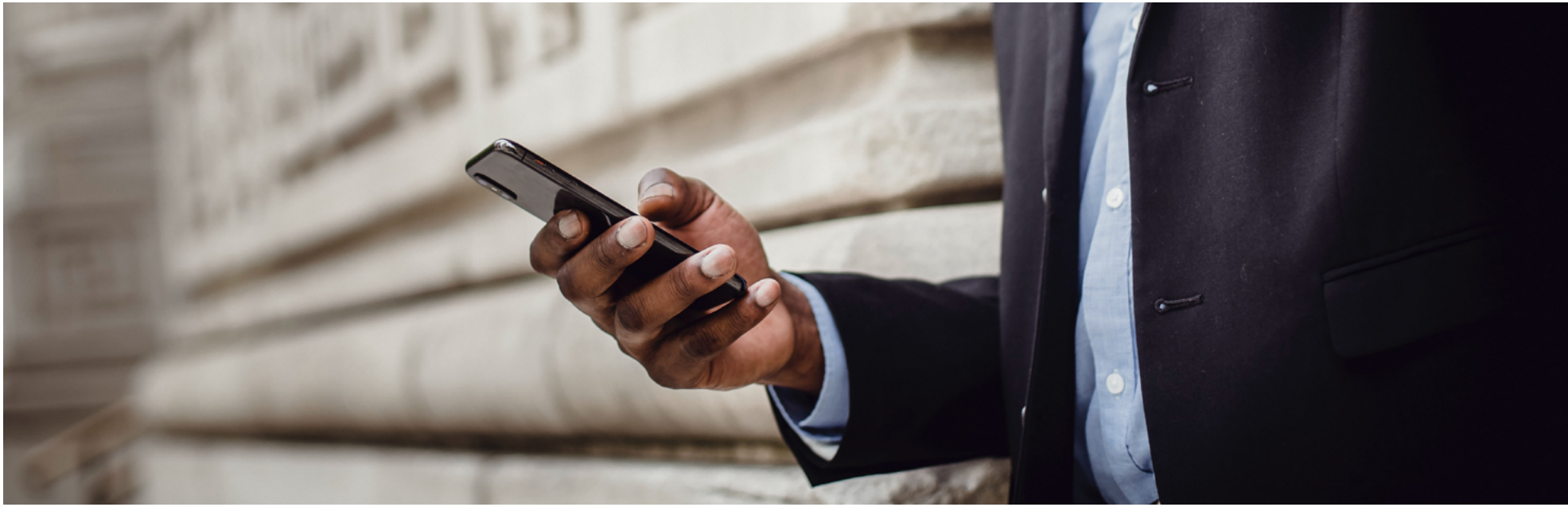
Further complexity arises through the usage of open source components and third-party libraries to accelerate software development. This fact opens organizations up to increased license and operational risk, plus it also expands the attack surface by potentially introducing known vulnerable code into a production build. On top of any organic vulnerabilities introduced in proprietary code, open source risk must be thoroughly acknowledged and addressed.

From a security and compliance perspective, increasing risk through open source usage is obviously unacceptable, but for development teams needing to reduce time to market, it is a must have. Application security solutions used to detect, identify, and track open source in code bases are imperative.

Beyond that, organisations often note that traditional methods of application security scans of a full code base near the end of the development process take too long to complete, and the special requirements needed to initiate scans are time-consuming. Additionally, and in some cases, the security policies and scan queries in use simply look for too many potential vulnerabilities. A further issue arises when more-generic application security scans return an abundance of inaccurate results, or 'false positives', resulting in delivery and deployment delays driven by the need to investigate and determine the true nature of every vulnerability.

This is exacerbated by the fact that not every public sector development team has access to in-house security expertise, developers are often lacking in secure coding skills, developer security education is limited, and advanced vulnerability remediation skills commanding premium salaries are in short supply.

A Case for Automated Application Security Testing (AST)



As a result of these factors, security testing is often being pushed closer to the release deadline and problems identified at that stage are obviously more difficult and time consuming to address. If organisations are using outdated application security approaches to test just before, or even after delivery, this will only serve to delay production releases, further proving that security testing remains a drag on release efficiency and frequency.

Clearly this tension must be resolved. By integrating AST solutions directly into the software development and DevOps toolsets that developers use daily, organisations can achieve their time-to-delivery objectives without compromising on security.

Use case: Accelerating DevOps with Checkmarx

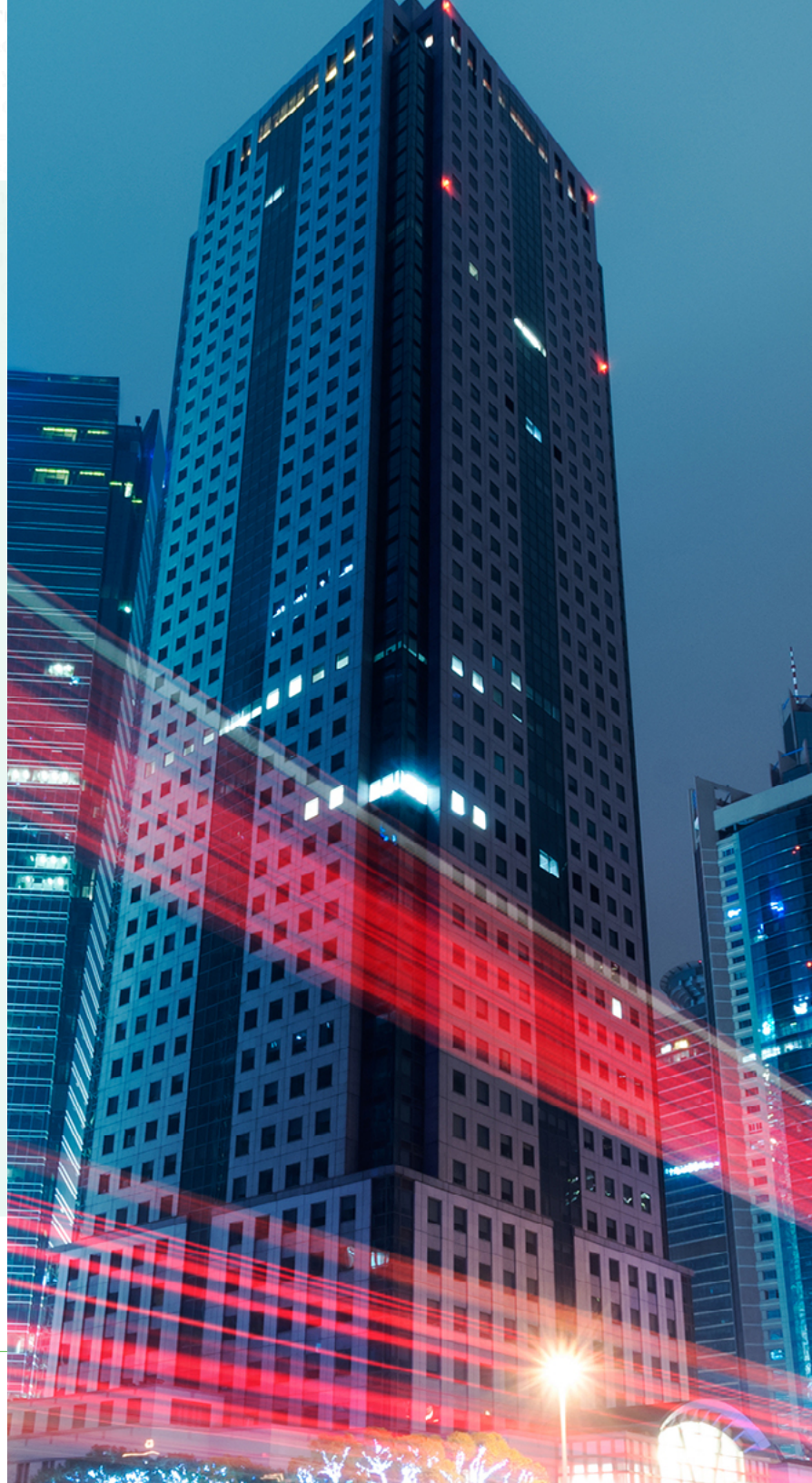
Healthcare provider Premise Health practices agile software development and strives to ensure that nothing gets in the way of fast releases. They run a CI/CD pipeline and have fast release cycles. Their security platforms need to seamlessly integrate into their development lifecycle.

Premise Health uses Checkmarx to find and fix vulnerabilities as early as possible in the software development lifecycle because the later you catch them, the more expensive they become.

Checkmarx's language support and its ability to keep up with new releases proved helpful, as did its code walk-through, which provides examples of how to fix or prevent vulnerabilities while you code. Plus, Checkmarx solutions are easy to use, with a friendly and simple interface.

The best use of Checkmarx is within our CI/CD pipeline – we use the Checkmarx Jenkins plug-in. In Jenkins we build out the code and deploy it. The code is then scanned whenever a build is created.

Timothy De Block, Manager of Security Engineering at Premise Health



In addition to more sophisticated testing approaches and integrated solutions, this requires a cultural shift from seeing development and security in opposition, to recognition that a DevSecOps method of incorporating security testing throughout the software development lifecycle (SDLC) – starting at the planning stage - will actually result in faster delivery, especially in a public sector environment which naturally has an increasing focus on security.

By deploying integrated code-scanning solutions that completely automate scans directly from Source Code Management (SCM) solutions, CI/CD tools, and Integrated Development Environments (IDEs) developers can increase efficiency, improve security, and measurably reduce delays. Upon pull, push, merge requests, etc., these events can automatically trigger incremental Static Code Analysis (SAST) and Software Composition Analysis (SCA) scans at key points in the developer workflow. As a result, code vulnerabilities can be identified and corrected at an earlier stage of the development process within the branch of code developers are currently working on. In addition, AST solutions can be integrated directly into bug tracking and ticketing systems to automate ticket opening, triage updating, and issue closure.

It is also important that AST solutions are highly accurate, with low false positive rates, and that they avoid disrupting developer workflows. If solutions can also point coders toward best fix locations within the many lines of code, this will also reduce the need for dedicated security expertise while, at the same time, build awareness and improve security skills within the developer community.

The result of deploying integrated and automated security testing solutions equates to a lower likelihood of repetitive coding errors making their way into production and introducing unacceptable security risks.

This approach to Application Security Testing resolves tension, alleviates pressure, and reconciles agile software development practices with security risk mitigation.

The Citizen Contract

Resolving the secure software issue is critical for public sector organisations – perhaps only banking has a similar level of obligation to its users. The applications developed by the public sector for citizen use quickly become foundational to the operation of core elements of society from education to law enforcement, healthcare, and social services. They are built using public funds and as such are answerable to the public for both performance and how they protect the citizen data. It is a breach of contract and trust when citizen data is put at risk due to known code vulnerabilities released into production.

Getting digital public services right pays dividends for governments. Research by McKinsey found that "residents who are satisfied with a public service are nine times more likely to trust the government overall than those who are not." The German National Regulatory Control Council has also identified that, alongside 24/7 accessibility - important in a pandemic - digital public services can result in:

50% Around 50% **less time spent** interacting with public administration by citizens

50% More than 50% **cost savings** for companies when interacting with public administration

60% Around 60% **less case management** effort required for public sector employees through automated processing

Efficiencies and cost-savings on this scale underline the economic and ethical imperative for pursuing secure digital public services projects.

COVID-19 apps – a lesson in citizen cynicism

The challenges faced by public sector app developers were exposed during the various attempts worldwide to develop, roll out, and gain take-up for apps designed to help monitor the spread of the virus through proximity tracking. With speed of the essence, several apps were built and pushed to production, but glitches and security concerns (albeit mostly unfounded) saw many citizens expressing cynicism or concern that the apps either did not work, required too much user participation, or unacceptably infringed individual privacy rights. The level of public discussion over the performance and safety of the apps served to demonstrate the likely pressure on future public service software to meet increasingly high public expectations of security and usability.

The Way Forward and the Window of Opportunity

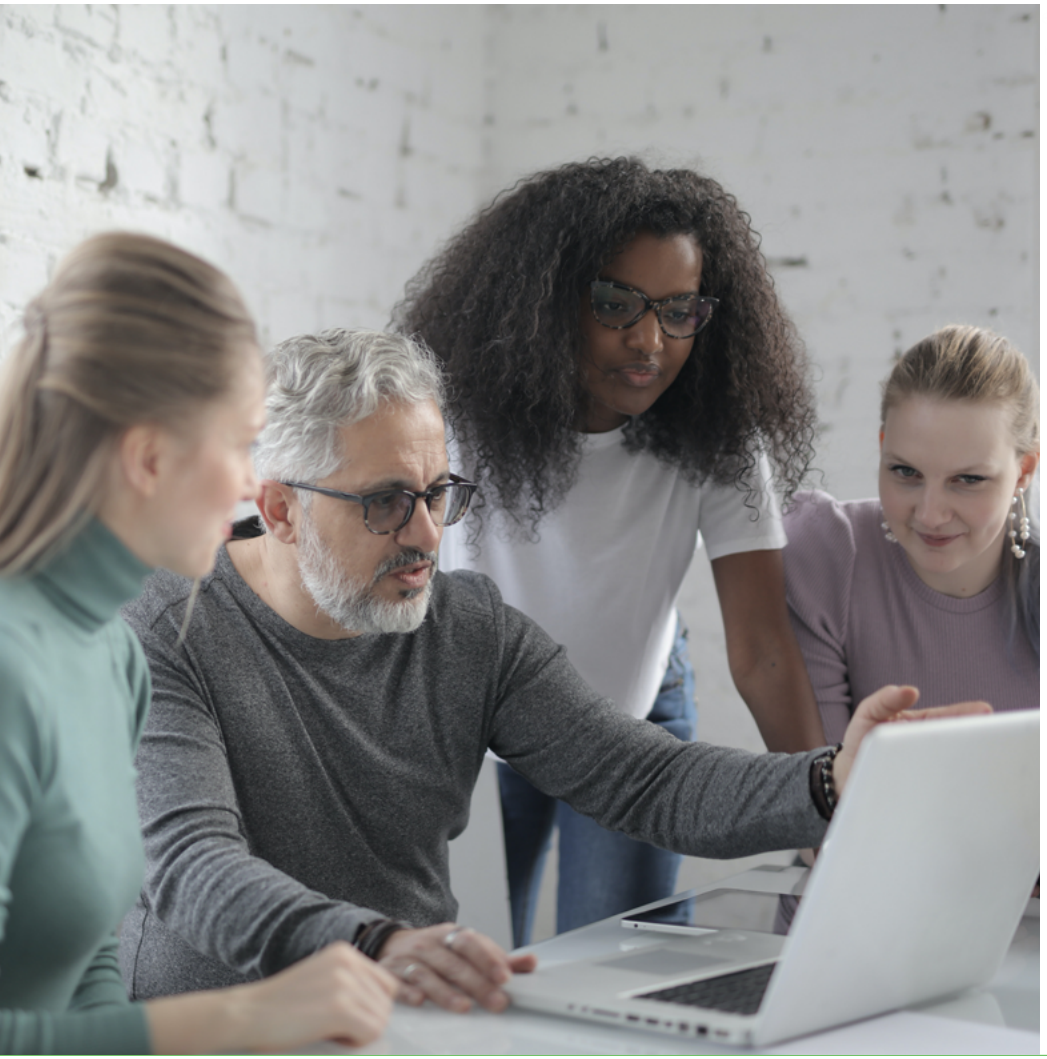
Despite the considerable risks and challenges around public sector service digitisation there is a distinct window of opportunity for organisations to move forward in the right way and build a strong business case for secure, robust transformation projects.

First, it is important to understand that merely digitising the process that organisations follow already is short-sighted, with cost and efficiency gains typically limited to an initial benefit, but no long-term pathway to continuous improvement. True digital transformation involves a full redesign of processes and incorporation of multiple data sources to create seamless, intuitive services and eliminate unnecessary steps. Such services can form the foundation of comprehensive delivery of public services through online channels that has the flexibility to evolve and scale as needed.

Of course, all this costs money and, following the emergency expenditure of 2020, funds will be in short supply. But what the crisis has unequivocally demonstrated is that, when all other avenues are closed, digital is the only option. Many national financial institutions are currently cautioning against tightening fiscal measures and restricting public spending too quickly following the pandemic, meaning there is a window of opportunity to secure investment in projects that will deliver long-term efficiencies and cost-savings. This should be prompting public finance managers to seek out and fund projects that deliver high-performing digital services in the drive to build resilience against future disruption.

By ensuring that those digital services designed and delivered giving functionality and security equal weight right from the planning stage, public sector organisations will be taking a major step forward in building new, trusted citizen-centric digital relationships.

8 Tips for Driving Secure Software Development and Gaining Buy-In for Secure DevOps Initiatives



1. **Identify projects that truly transform public sector operations and promise long term efficiency gains and citizen benefits.** Go beyond simple process digitisation and instead aim to re-engineer the citizen journey and integrate multiple agencies in a digital citizen-centric approach.

2. **Promote an internal, organization-wide culture that recognises the obligation to protect citizen data** and integrates intrinsic security measures into the entire software development lifecycle.

3. **Emphasise the efficiency, security, and compliance benefits of a DevSecOps approach** beginning with the development of organizational security policies directly tied to secure software initiatives.

4. **Establish an AppSec awareness and education programme** and research training platforms that help improve, track, and report on in-house secure coding skills - growing your own expertise and investing in your human resources.

5. **Seek out knowledgeable AST solution suppliers, integrators, and value-added partners to support you** with the right skills and knowledge needed to help execute your application security program effectively.

6. **Evaluate vendors that offer AST solutions training, onboarding, query customisation,** software security consulting, risk analyses, fully or partially managed offerings, and many other applicable services.

7. **Select AST solutions that support integration and automation of incremental and full scans to address custom and open-source code vulnerabilities** at key points during development so security issues are not pushed close to release deadlines.

8. **Chose best-in-class AST vendors** that possess customer validations via referenceable testimonials, have widespread industry recognition of their solutions, and are recommended by well-known analyst firms.

About Checkmarx

Checkmarx is the global leader in software security solutions for modern enterprise software development. Checkmarx delivers the industry's most comprehensive Software Security Platform that unifies with DevOps and provides static and interactive application security testing, software composition analysis, and developer AppSec awareness and training programmes to reduce and remediate risk from software vulnerabilities. Checkmarx is trusted by more than 40 of the Fortune 100 companies and half of the Fortune 50, including leading organisations such as SAP, Samsung, and Salesforce.com. Learn more at **www.checkmarx.com**.