Platforms and Technologies

ATARC Application Development Working Group

Authors:

Dennis Jerome, Enterprise Program Management Office, Internal Revenue Service

Joel Krooswyk, GitLab

Rayvn Manuel, National Museum of African American History and Culture

May 2021

Table of Contents

Disclaimer: This paper was prepared by the ATARC Application Development Working Group members in their personal capacity. The opinions expressed do not reflect any specific individual nor any organization or agency they are affiliated. This paper is intended to be a helpful guidance on the subject topic.

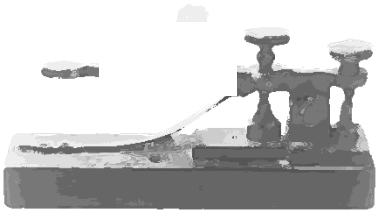
Platforms and Technologies

In an age of virtualization, platforms and technologies have become essential parts of business and government organizations. For organizations to survive it is paramount that Information Technology leaders keep up with the current technical trends and tools. Basic business practices such as cost containment and risk mitigation remain evident; however, they may be defined differently because of the constant changes in a "virtual" global marketplace. It is with the essential technical tool selection that will contribute to an organization's culture, communication and performance. The platforms which are chosen will come with a cost, the key to success will be the ability to define the return on investment with these platforms and new technologies in order to create profitability.

History

According to the Center for Public Impact, "history is, however, replete with examples of new technologies or methodologies having fundamentally changed how government operates. Advances in technology can not only enhance or streamline administrative tasks and service delivery, they can also change the role of government or entirely reorganize its core functions."

An example of a technology which transformed the way government agencies accomplished their missions is the telegraph. The Center for Public Impact states "the adoption of the telegraph was gradual and cautious. It involved learning to work within a new set of constraints, such as having to write more concisely to avoid incurring expenses based on the length of messages per transmission. The first nation-wide industrial monopoly emerged in the telegraph industry and became subject to state and federal government regulatory pressure. What eventually killed the telegraph was not regulation but the rise of a competing technology, the telephone."



Current State

Platforms & Commercial Off the Shelf

Today, technology platforms are much more advanced and complex than telephony. Understanding the definition of a platform is vital to how it will be implemented into an organization's daily operations. John Spacey's "*16 Types of Technology Platforms" states that,* "A technology platform is an environment for building and running applications, systems, and processes. These can be viewed as tool sets for developing or operating customized and tailored services." Examples of platforms include operating

systems, computer platforms, database platforms, web platforms, and robotics.

In addition to technology platforms, many organizations are looking to purchase "Commercial, Off-the-Shelf" (COTS) products from technology companies as opposed to developing technical tools in-house. The COTS purchase provides an immediate opportunity for usage whereas the in-house development process can be time consuming and may not be as efficient or effective as the already tested COTS product.

An example of an organization utilizing the COTS option is the Internal Revenue Service (IRS). The IRS services millions of taxpayer transactions per year, and the organization is always seeking to improve their technological capabilities. The IRS has partnerships with several COTS developers such as Microsoft, Red Hat, and Oracle. These partnerships have enabled the IRS to successfully deploy Windows Win OS 2012, Oracle Fusion Middleware 12.x, JBOSS EAP, and other technologies.

Acquisition

Acquiring the most up-to-date technologies is a quest for many private organizations and government agencies and is most likely dependent on one key item- the Fiscal Year (FY) budget. Organizations and government agencies must keep their FY budgetary concerns in mind when deciding to spend funds on new technologies and platforms. With the constant need for technology updates and upgrades, an organization's spending can become a concern and can significantly increase an organization's expenses if not managed correctly.

Most Senior Executives are concerned with the return on investment from a technology acquisition and the "bottom-line" impact to the organization. When it comes to spending on technologies and platforms, Senior Executives like to know exactly what operational benefits the new technology will produce. The amount of money needed for acquiring new technology is not always the amount of money available. This can be a hinderance to organizations when the technological managers are striving to advance the technical capabilities of an organization, and the fiscal managers are constrained by budgetary limitations.

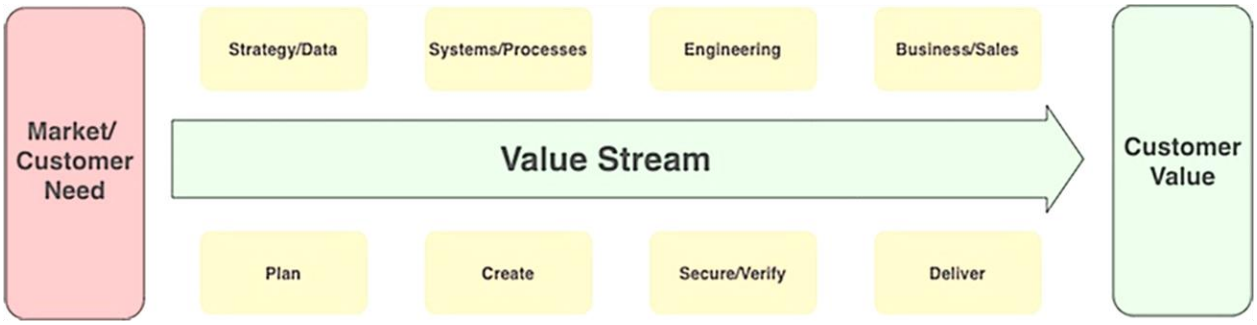
An additional concern of Senior Executives addresses the cost of fees associated with the acquisition of technology. These fees are connected to items such as patents, software, licenses, trademarks and intellectual property. Each of those items may be part of the acquisition process when purchasing new technologies or platforms, according to the article, *"The Difference Between Copyrights, Trademarks and Patents."* It is these additional costs which Senior Executives consider when passing approval for a pending acquisition.

Technology acquisitions can be divided into different organizational motivations, according to the document, *"Technology Acquisitions"* from the University of Cambridge. Some of these motivations include but are not limited to: developing technological capabilities, increasing strategic options, gaining efficiency improvements, and responding to the competitive environment. Each motivational element strives to answer key questions for the organization, such as "should the firm create and establish a new product," or "is the acquisition seen as a means to reduce costs and development time." The answers to these questions help organizations decide whether or not an acquisition should take place.

Value Streams

Value streams define the end-to-end flow of work from idea to deployment, defining the flow of value out to customers. Value streams provide visibility to process efficacy, awareness of delivery capabilities, and insights to blockers for delivery. Platform technologies are only as valuable as their ability to reflect and accentuate the processes and workflows in use, giving visibility and feedback on the impacts and effectiveness of those processes over time. This consideration requires information to be readily accessible and highly visible within a single platform or across applications. Value stream focus also enables technology platform optimization for continuous improvement.

When examining value streams, many factors should be considered. The platform should provide visibility to planned work, to work being done, and any output of the work. Platform traceability from concept through creation and review should be clear, auditable, and detailed. Approvals and work ownership should be verifiable in singular locations. Context of work should be available throughout a process, providing the understanding that the final product is what was originally specified, that the product was developed effectively, that the product is secure, and the work has been reviewed and approved as necessary.

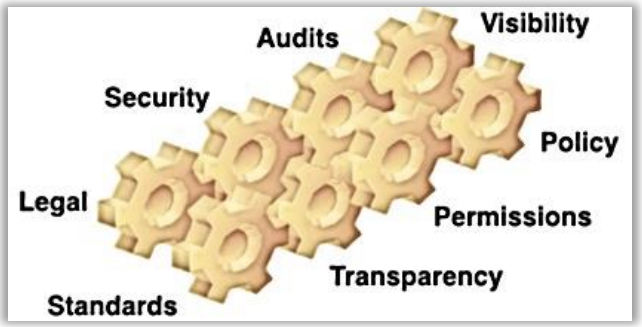


An industry trend in COTS is broadly featured platforms designed around value stream delivery. For instance, Gartner, in its "*Market Guide for DevOps Value Stream Delivery Platforms"* anticipates that 40% of organizations will pivot to value stream delivery platforms to streamline application delivery by 2023 vs 10% in 2020. COTS platforms also provide other benefits such as minimized administration effort and reduced risk via fewer attack surfaces. Additionally, reducing the number of technology tools required reduces acquisition and integration costs.

One final thought on COTS software is that many current, popular products are not financially profitable or may not have a viable business model over time. Acquisitions are also commonplace in the industry. Buyers can reduce toolchain risk by choosing an industry-leading platform on which to base development to avoid sudden changes, team re-training and/or the loss of automated services.

Compliance and Risk

Risk management of platforms continues to grow in its criticality. Whether it is about visibility to security events, reliable remediation efforts, policy compliance, or audit management, ability to mitigate risk is an essential piece of any platform.



Risk assessment often begins with policy enforcement. Policy management outlines user roles, user permission granularity, license types, API models, data access regulation and credentials inventory. Too often, risk is encountered from breaches due to improper access policy management. Additionally, policy management covers legal or regulatory frameworks such as SOC2, SOX, FedRAMP and others. Platforms may even help define rules and policies in addition to enabling automated auditing for verifying compliance.

Risk management continues with audit traceability, where all actions taken within the platform are adequately logged and reviewable. This should extend beyond just approvals into creation of new projects or items, new user permissions or altered permissions, security finding remediation, alert dismissal, and administrative actions. This allows visibility to non-compliant behavior and provides a clear history to help avoid intrusive security breaches. Access to this data within the application, potentially on a compliance dashboard or in event logs, is highly desirable for simplicity in audits, particularly during events involving suspicious activity.

Automation of compliance workflows is critical for effective policy enforcement and separation of duties to minimize risk. Where applicable, automation of risk mitigation related to security findings simplifies compliance with standards as well as specific agency policies. Execution of security scans regularly and consistently is desirable. Automated or platform-advised remediation methods for security vulnerabilities further accelerate value stream performance while reducing risks via minimized human interaction.

Lastly, centralized visibility to risk conveyed by organizational or cross-project dashboards enables at-a-glance assessment of security health as well as potential risk of current platforms. Consolidated dashboards enable rapid and educated decision making regarding risk mitigation strategies.

Security Concerns

There are essentially three basic categories of security concerns when it comes to safeguarding computers and mobile devices: preventive, detective, and responsive. In the computer security field, it is important to strive to prevent a compromise or breach of information before it occurs. If a compromise or breach does occur, then one must have mechanisms in place to detect the intrusion. Once a threat is detected, the correct response needs to be selected and put into action, according to the article *"Information Security Principles of Success" by Jim Breithaupt and Mark S. Merkow.*

To maintain a secure network, organizations are instituting preventive measures with the hope of preventing and deterring cyber-attacks. Organizations are hiring a multitude of cyber security experts who have been trained and certified in areas of computer and network security. According to Aqua Security, a technology company based in Massachusetts, "Aqua Security's cyber research team has seen increasingly sophisticated attacks on containers – threats that evaded detection by static scanners. These malware attacks include cryptocurrency mining, credential theft, data exfiltration, or DDoS attacks – threats which are only detectable in running containers. To protect against this stealthy malware, Aqua's container analysis sandbox solution, Aqua Dynamic Threat Analysis (DTA), dynamically detects risks hidden in container images by mimicking the threat surface as if the images are running in production. It finds malicious behaviors that can only be observed when an image runs as a container."

The importance of computer security and its evolution has been evident during the COVID-19 pandemic. The pandemic has forced many countries to go into sequestration which has led to commercial enterprises and educational institutions adopting new technologies and platforms in order to continue operations. Many users choose the platform Zoom Video Communications Inc for teleconferencing and videoconferencing. Zoom offers approximately 40-50 minutes of free time before charging a fee for their services. This sparked a global trend, and Zoom's membership has greatly increased; however, the company wasn't ready for such a rapid increase of usage and security issues soon emerged. Zoom realized their vulnerabilities and was forced to choose a technical partner in Oracle in order to keep operations safely running in a secure, virtual environment, according to the article *"Zoom taps Oracle for cloud deal, passing over Amazon, Microsoft" by* Jessica Bursztynsky.

Once decisions are made and platforms and technologies have been purchased it's best to identify which areas of your platform or new technology may be at risk. It's recommended to put your new products to a test and check into the reliability and safety of your new purchases. Too often consumers are caught off-guard and don't have a full understanding of the platform or technology they have just purchased. An example of a vulnerability is a data breach. According to the articles "*Top 5 Ways to Handle a Data Breach,"* and *"How Organizations should handle data breaches,"* weak passwords and other vulnerabilities in software and systems unnecessarily expose sensitive information. All of these can lead a hacker to compromise your accounts and data. Some steps can be taken to improve an organization's security against threats: 1) create stronger and more complex passwords, 2) access data

from a trusted device, 3) review your organization's website frequently by monitoring your own data and any transfers of data to other organizations, 4) limit access, 5) two factor authentication, and 6) use encryption for messages of importance.

Conclusion & Recommendation

Platform and technology use will only continue to grow as technologies expand and evolve. To optimize the adoption of new technologies, platform evaluations should occur at minimum annually. Platform evaluators should examine what platforms are available in the marketplace, understand how to evaluate a platform's ability to enhance current processes, and see clearly how to validate acquisition ROI. As the pace of innovation continues to accelerate, platform evolution is also happening faster. This typically happens via native engineering work as well as corporate acquisition, making annual market evaluations of platforms more beneficial than in the past.

As new technologies are developed, they often increase efficiency and reliability of applications, but they also often come with added complexity and new learning or certification requirements. Utilizing COTS platforms that simplify the adoption of new technologies can expedite time to value and speed to mission by reducing the time required for technology evaluation and adoption without the full educational investment.

Replacing platforms can be disruptive, so evaluations should focus on more than just replacement capabilities – they should also consider newer, more efficient ways of working in order to produce net gains over existing systems. As platforms grow in their capabilities over time, evaluations should also consider replacement of existing or antiquated systems as alternate, cost-effective solutions become available. For instance, if 3 siloed tools can be replaced by a single platform, cost savings, attack surface reduction and process efficiency may all be realized simultaneously.

With the current trend of technology platforms growing in breadth of capabilities, expect enhanced visibility and transparency across groups of people, creating an opportunity to streamline or optimize processes. Broader functional platform breadth enables consolidated process views, better collaboration, stronger security, and the ability to measure value delivery across a broader sub-section of the organization, if not a fully end-to-end view. This, in turn, unlocks opportunity for continuous improvement across groups and teams, not just within them.

Lastly, consider that COTS platform use in higher education is on the rise, leading the next generation of the work force to look for the modern platforms they are familiar with. Utilizing modern platforms helps attract and retain top talent while providing process benefits to the organization.

Works Cited

Aqua Security, editor. "Dynamic Threat Analysis for Containers." *Aqua Sec*, www.aquasec.com/products/container-analysis/.

Bursztynsky, Jessica. "Zoom Taps Oracle for Cloud Deal, Passing over Amazon, Microsoft." *CNBC*, 28 Apr. 2020, www.cnbc.com/2020/04/28/zoom-taps-oracle-for-cloud-deal-passing-over-amazon-microsoft.html. Accessed 19 Apr. 2021.

Ford, Simon J., et al. "Disentangling the Complexity of Early-Stage Technology Acquisitions." *Research-Technology Management*, DOI:10.5437/08956308X5503048. Accessed 19 Apr. 2021. Originally published in *Research-Technology Management*.

Gartner, compiler. *Market Guide for DevOps Value Stream Management Platforms*. *Gartner*, www.gartner.com/en/documents/3991130/market-guide-for-devops-value-stream-management-platform. Accessed 19 Apr. 2021.

Jelen, Sara. "Top 5 Ways to Handle a Data Breach." *Security Trails Blog*, 27 Nov. 2018, securitytrails.com/blog/top-5-ways-handle-data-breach. Accessed 11 Mar. 2021.

Kaukab, Farva. "How Have Governments Changed with Technological Advances?" *Centre for Public Impact*, BCG Foundation, 28 Feb. 2017, www.centreforpublicimpact.org/insights/governments-changed-technological-advances. Accessed 19 Apr. 2021.

Merkow, Mark S., and Jim Breithaupt. *Information Security: Principles and Practices*. 2nd ed., Pearson, 2014. *Pearson IT Certification*, Pearson, www.pearsonitcertification.com/articles/article.aspx?p=2218577.

Spacey, John. "16 Types of Technology Platform." *Simplicable*, 12 Feb. 2019, simplicable.com/new/technology-platform. Accessed 14 Feb. 2020.

Webb, Alexander. "The Difference between Copyrights, Trademarks and Patents." *NYTimes*, 16 Apr. 2020, www.nytimes.com/article/copyrights-trademarks-patents.html. Accessed 19 Apr. 2021.

Whitney, Lance. "How Organizations Should Handle Data Breaches." *Tech Republic*, 30 Jan. 2020, www.techrepublic.com/article/how-organizations-should-handle-data-breaches/. Accessed 4 Apr. 2021.