# Choosing a TMS:
## The Hidden Risks of Choosing "Generic" Software

ENVISAGE TECHNOLOGIES | August 30, 2018


### Abstract

Generic software is simple to use and built for a broad number of potential use cases, but that does not make it the best choice when choosing a training management system (TMS). The unique needs of public-sector organizations are best met by software built to serve the industry—a fact that holds both in the field and in the courtroom, where a lack of effective documentation can bring down even the most stringent training policies. This whitepaper will discuss the hidden and not-so-hidden downsides of "going generic" when considering a TMS by contrasting their value against purpose-built solutions, with topics that touch several aspects of first-response life: fieldwork, cybersecurity, certification, and learning exercises, among others.


### Introduction

Purchases at the state and local level account for 56 percent of all government technology spending.[1] This is an eye-opening fact that belies a growing expectation among law enforcement, firefighting, EMS, and other responder institutions: keep the public and internal stakeholders happy. These agencies must be able to provide better service using fewer resources. Because technology purchases excel at streamlining and automating processes, the right tools can do much to offset this facet of public sector life. With all of this in mind, it would be difficult to overstate the role technological assets like software play in the modern first response organization.

1. Across the country, state and local spending on technology is expected to grow by several percentage points in 2018, while federal spending is expected to drop—another sign of technology's increased role at the sub-federal level (Konkel, 2017).

As anyone familiar with public sector software purchasing knows, however, coming to the *right* decision is rarely a simple process. In a perfect world, decision makers, knowing precisely which features they need today and in the future, could quickly identify a product that matches their needs and specific price requirements without sacrificing for other considerations. In reality, balancing these two is a grueling act of compromise that tends to skew towards the *price* side of the equation, given the above-mentioned need to stretch every dollar to the fullest extent possible.

All too often, this results in first response organizations shoehorning *generic* software against their current processes and existing software systems. Generic software offer solutions that come with a set of features designed for broad general use, and not the highly-specific needs of public institutions. At best, this decision results in the organization altering its processes to better match features the tool offers. All too often, the same organization may find itself paying for a product that is not suited to manage the tasks for which they need it. While larger software makers sometimes offer products at a price that makes their practical deficiencies feel less glaring, this is hardly an optimal outcome in the long term.

Now consider the immense role training and associated recordkeeping play in the average first response unit. In all areas of the public sector, a well-trained workforce keeps the public more satisfied[2] and generally keeps the cogs of the organizational machine greased and ready to perform. Similarly, thorough, legally defensible documentation of training activity shields the institution from potential legal threats, a growing concern in an era where the definition of spoliation continues to evolve and encompass more meaning.[3]

Despite its critical role, it is not entirely surprising to hear training is a common target when budget cuts force tough decisions.[4] The impacts of a substandard training budget are not always felt at the time of the cut, and other needs, while no more important in the long term, may present an immediate challenge if improperly funded.

Problematic as this trend may be on its face, training-related cuts become concerning when considered alongside the

2. One study of Malaysian public sector employees found even rudimentary training for employees who directly interacted with the public resulted in a happier public and more competent workforce (Rashid, 2008).

3. Today, even accidental or good-faith destruction of certain records can constitute spoliation in the courtroom—and depending on the state, an inability to produce records could mean an automatic presumption that the paperwork was harmful to the case of the person who held it (Envisage Technologies, 2017).

4. In Michigan, a lack of training contributed to a vicious cycle that made every aspect of the law enforcement process more difficult: lower funding meant fewer officers, which meant less revenue generation via tickets and fines, which then impacted the state's ability to provide training to short-staffed police stations across the state (Associated Press, 2015).

software-purchasing discussion posed above. An institution that lacks effective training and industry-specific tools to document the activity is effectively in double trouble if legal troubles related to training arise. Moreover, the day-to-day impacts of underfunded, under-documented training activity can create problems that cost responder organizations far more than they save from generic training management platforms. Because of this—and due to numerous other privacy, security, and performance-related concerns posed in this paper—organizations would be well-advised to move away from generic training management systems (TMS) and towards solutions designed to support their unique requirements.

## For Responder Agencies, Outdated Training Management Can Represent Multiple Problems

Understanding why a purpose-built TMS is better than the generic option is difficult if one does not understand the value of a TMS in the first place. Modern training management platforms serve a broad number of processes and carry out diverse tasks in first response organizations, but the high-level benefits are largely the same everywhere. Accordingly, given the number of ways training can influence an organization's processes, any tool that improves the efficiency of educational processes can have an immediate positive impact on the way that institution operates.

Sometimes it is easier to explain the benefits of an upgrade via the problems an organization will face in the absence of an upgrade. Most agencies face one of two of these problems, or some combination of both:

- By choosing the *wrong* software, organizations lose functionalities designed specifically for their industry.
- By sticking with cumbersome manual processes, responder institutions miss out on every benefit digital systems have to offer, purpose-built or otherwise.

While no public-sector organization could reasonably expect to function using only paper processes, it is just as difficult to imagine every public office completely doing away with them. Foregoing long-term efficiency and savings to avoid up-front

costs is still an unfortunate necessity in some locales. In terms of manual processes, it is particularly easy to envision a first response agency continuing to maintain paper documentation for certain training practices—these records may only need updated at certain times of year (or upon hiring), making it easier to *work around* the inconvenience of manually updating them. Further, an organization may *split* personnel records between digital and paper sources, depending on their classification, importance, and the format of each recording. For example, disciplinary and performance records may be kept in a digital file, digital training history and scores in a separate software program, while range, driving, and other on-site training records are kept in a binder stuffed in a file cabinet.

The drawbacks of such a method are obvious. Each digital system may have its own set of login credentials and access-authorized personnel, making it hard for stakeholders to find the data (or even the systems) they need. Promotion considerations, qualification and compliance checks, and other basic functions require decision makers to pore over numerous employee records manually. With paper files, decay and damage from disasters like fire and flooding are an ever-present concern, threatening to erase large swaths of historical records in moments.

Then there are the legal ramifications. Building a legal defense with collections of documents from multiple sources is a time-consuming endeavor, considering the shape lawsuits against response organizations take. Generally, if the accused agency cannot prove their policy required appropriate training and that the training was completed—and more importantly, if they fail to do this all in a way that is legally defensible—liability may attach.[5]

5. It is estimated that one in five law enforcement officers will be accused of misconduct at some point in their career. This underscores the importance of a preemptive defense: the organization cannot begin building defensible training records after the summons arrives (Envisage Technologies, 2016).

## Why Security Matters More Than Ever

On the topic of legal defense, litigating attorneys are resourceful. Counsel representing a plaintiff in a failure-to-train case are likely to attack a perceived lack of policy or appropriate training on the organization's part, but they likely will not stop there. They may also turn a critical eye towards the security and auditing measures used to ensure

the provided documents remain secure, accurate, and untampered. Failure to counter these arguments may render the documents unreliable in the eyes of the jury or court, strengthening the plaintiff's position and leaving the accused with little ground to stand on.

Here, purpose-built training management platforms are preferable to generic alternatives because they are designed to account for the litigious realities of the public sector. In this sense, a training management platform designed for first response can handle security and the perception thereof: a small distinction on paper, but a potentially massive one in the courtroom. Although any competent TMS will have some security measures against intrusion and attack, and any learning system will provide a core learning experience, only a training management system made for first response users will offer audit trail and defensive features necessary to legal defensibility on top of the critical training functions it helps manage. In turn, this gives responders who have appropriate training and behavioral policies the tools they need to defend against a common secondary line of criticism.

Of course, the *perception* of security is not all that matters. Responder organizations have become a growing target for cybercriminals in recent years, with any number of motivations spurring breaches, attacks, and illegal behavior. In one startling example, a police department in Cockrell Hill, Texas lost eight years of evidence after refusing to pay ransom for data that hackers had seized via encryption.[6] In another, a group linked to the "hacktivist" collective Anonymous launched a distributed denial of service (DDoS) attack against the City of Denver's web properties, taking their main site and numerous linked properties offline for the remainder of the day.[7] The latter attack appeared to come in retaliation for a controversial officer-involved shooting.

At first, it may not appear that a TMS would present an attractive target to hackers, since training data on officers, firefighters, or emergency medical professionals have little cash value in the real world. Looking deeper, however, several potential threats emerge. One such example is the *weak link* or *leapfrog* concept, in which hackers use information obtained from a lesser system to gain access to their true target. A

6. The hackers demanded $4,000 for the ransomed data. However, the FBI told the police organization that there was "no guarantee" the criminals would keep up their end of the deal upon payment, leaving decision makers to cut their losses and start fresh with a server wipe (Storm, 2017).

7. DDoS attacks are particularly popular among hacktivists because they're inexpensive to obtain, require relatively little technical knowledge to effect, and—deployed against an unsecured system—can cause significant disruption within the targeted organization (Iyer, 2016).

hacker could obtain a high-ranking supervisor's email address through social engineering, guess their password via info on a public social media account, and use the two to log into a critical management system, for instance, and then steal valuable employee data like Social Security numbers or digital W-2 files.

More insidious are attacks with no financial motivation. With political tensions high and many hacking groups taking a decidedly anti-law enforcement political slant, digital threats against responders and their families have potential to spill out into the real world. On several occasions, hackers have obtained and posted personal identifying information (PII) of law enforcement officers to the internet, subjecting them to possible harm and immense personal stress. One recent example of this vindictive behavior occurred in 2016, when hackers released the names, home addresses, and other personal data of more than 50 Cincinnati Police Department officers in apparent retaliation for an officer-involved shooting.[8]

8. In this instance, police shot the suspect after he reached for an item in his waistband. The recovered weapon was later found to be a pellet gun—a hard distinction to make at a distance, let alone when seconds count and lives are may be on the line (Knight and Strickley, 2016).

Criminals have no shortage of reasons to come after first responders, especially those involved in criminal justice. Indeed, the sheer number of motivations may open responder organizations to more threats than any other public-sector institution or private sector business. While most training management systems will include some security measures, tools designed for the industry are far more likely to be built with robust, government-sanctioned security measures. For response organizations, as well as staff and their dependents, this marks an important feature in a field marked by high stress and political volatility.

## With or Without Guiding Regulations, Industry-Specific Standards are Best

If security has a third dimension beyond defense and perception, it is meeting the standards put forth by regulatory bodies, industry councils, and other oversight groups. This is of serious concern in the private sector, where noncompliance may result in an entity losing its ability to process credit cards, maintain software, or handle other basic business functions. To this end, it should come as no surprise that public

organizations—many of which must comply with multiple sets of rules at once—face stricter standards and sanctions. The tasks they fill and processes they serve are simply too important to handle without stringent controls in place.

For example, cybersecurity standards put forth by the National Institute of Standards and Technology (NIST) and the Federal Information Security Management Act (FISMA) place demanding rules on responder organizations and their third-party vendors. Meanwhile, some certification programs are so rigorous that undergoing the process is considered a mark of honor on its own: TMS and other cloud-based programs in the midst of Federal Risk and Authorization Management Program (FedRAMP) certification are considered a gold standard in many circles for this very reason.

Speaking frankly, these certifications matter because many companies making general-purpose TMS software do not have the resources, expertise, or even the desire to make their products compliant. Achieving a passing mark is a rigorous, technically-demanding, and expensive endeavor. It is not something a private sector vendor attempts without a pressing reason. In many cases, pursuing such a distinction without a large public-sector clientele (or product suited to that sector's specific needs) would be wasteful at best and disastrous at worst—a testament to the security commitment standards like FISMA, NIST, and FedRAMP show. In addition, this once again illustrates how a TMS designed for the industry will outperform something made for a general userbase.

For agencies with a direct connection to various standard-linked organizations, the message is clear. If there is even miniscule risk that standards-bound systems or data will touch a TMS, taking a risk on a non-certified training solution is a questionable choice. Of course, organizations unbound by federal-level cybersecurity standards are still wise to consider a system capable of managing them. Because policies like FISMA are so exacting and up-to-date, many state and local governments use them as a basis for their own standards.[9] With hackers and even state adversaries[10] placing a large target on public agencies in recent years, that level of security competence has value in and of itself. Training systems naturally include names, addresses, and other PII, for instance,

9. Further, the author says that publications put out by NIST are a "gold mine" of information, and that most security experts lean heavily on them for up-to-the-minute security information. (Lohrmann, 2006).

10. In another disturbing incident, "at least 32" officers from departments throughout the state of Milwaukee were discovered to be on an ISIS "kill list." Listings on targeted officers included PII like names, addresses, and phone numbers (Kirkos, 2016).

putting the onus on agencies to keep their staff safe from vindictive hacktivists and others who may wish to harm them. Whether attackers wish to use training systems as a point of entry, or the system itself is the top goal, certified, industry-built tools provide a layer of security most general-purpose generics simply do not have the resources to attain.

## Beyond Security: The Educational Importance of Industry Platforms

Of course, a training management system's cutting-edge security design is less of a selling point if the platform's primary objective—namely, automating and otherwise increasing training efficiency—fails to meet the mark. Here, industry-built training platforms excel for the same high-level reasons that make them so strong in the courtroom and at compliance audit time. Since they are designed with industry needs in mind, they consider intricacies of training and continuing education that a generic may fail to address altogether.

Learning Management Systems (LMS), otherwise known as the course delivery modules found within training management platforms, highlight this difference in design approach. Unlike private sector businesses, where training and continuing education are often a means to learn and adapt, educational efforts in police departments, firehouses, EMS departments, and other agencies are often required by law. They are also complex in requirements and content, with courses that run the gamut of formats and objectives. For example, a firefighter completing their annual slate of training hours may take an online course one day, an instructor-led classroom session the next day, and a field-based simulation exercise the day after that.

Whatever branch of service a responder works in, this multi-format, *blended learning* approach is the standard these days, and this basic need is why many agencies initially search for an LMS. For many training modules, building an online course that can be tweaked and reused year-over-year is far more affordable and convenient than forcing participants to leave their regular duties for the day and paying instructors to lead classroom-based courses. By decentralizing the training efforts

and allowing participants to take part in an automated, easy-to-access course, departments can turn lessons that might take a whole day in a standard classroom into short, self-directed affairs.

On the management end, a purpose-designed platform outperforms generic alternatives by providing administrative tools suitable for the industry. Whether stakeholders are dealing with a class of fresh recruits or a corps of veteran personnel going through annual POST requirements, even a single course can generate a significant amount of data. A tool that accurately attaches learning and exams to the correct personnel file can remove huge amounts of busywork from administering and administrating courses; that it stores the data in a federally certified, secure, and legally defensible way only makes the proposition more attractive.

Indeed, academy learning and the larger topic of academy automation present another leading advantage of industry-built LMS and TMS. Like all decision makers within an agency, educational leadership are routinely asked to do more with less. The same efficiencies that secure accredited online learning content so useful for departments translate perfectly to learning systems where dozens or hundreds of recruits might come through in batches. With such large rosters, changes that seem small on the individual level become substantial savings when applied across the classroom or the entire recruit corps. LMS-universal features such as test scoring and batch certification monitoring apply here. More importantly, features typically only found in industry-leading solutions—automated graduation processing and templates for industry-specific course creation—do as well.

## TMS Features: Complex Problems Need Complex Solutions

It would be disingenuous to say education is only one part of the TMS's overall importance to a modern first responder agency. Considering all the ways education touches organizations, it is more accurate to note the extreme complexity even simple training regimens can represent, and the dedication required to do a good job of managing it all.

Perhaps more than any other singular reason, this is why first response organizations should think hard before choosing a generic TMS to handle their training needs. Simply put, it is hard or even impossible to tackle a complex problem with a tool designed from the outset for simplicity. Although an industry-focused solution does not need to be user-unfriendly to properly manage first response training activity by any means, it does need to offer powerful features aligned with those complex needs. Otherwise, organizations risk having to needlessly alter processes to suit their purchases or become stuck with a tool that ultimately cannot handle the job.

Take, for instance, the fact that training comprises only one small part of the documentation a responder will generate in even a short time with an organization. Most generic TMS will approach this problem one of two ways: encouraging users to purchase another third-party software their product interfaces with, or allowing departments to integrate solutions themselves through application programming interfaces and other software development tools and techniques. On the other hand, a competent industry-built solution will offer modules that include multiple sources of documentation, effectively covering the personnel's entire history with the organization. Instead of logging into a different system to view discipline history, drug test results, range scores, and testing history, stakeholders can access the same data from a singular source.

A TMS designed for responders allows the same stakeholders to group, categorize, and view the data they need. For training compliance checks, promotion qualifications, role requirement reviews, and other basic functions, this can vastly cut down on the time needed to review multiple files at once; instead of manually compiling info strewn across multiple sources, everything is presented in a quick, at-a-glance format. This is a need unique to regulation-bound government roles like first response and would be grossly complex to configure with generic software, likely requiring outside programming or special consideration from the developer to make work.

Then there are the training-related records that focus on material goods and learning spaces instead of people. Where most training in a public sector organization requires a

boardroom and basic office supplies—and where generic tools are built to accommodate that specific flavor of training—courses in first response can require meticulous coordination of expensive, hard-to-track tools. A solution that allows leadership to assign, track, and monitor equipment usage in the same portal that helps them manage learning, then, effectively combines the capabilities of multiple single-purpose tools into one powerful group. Since the tools are combined, they can offer cross-functionality individual programs could likely never make available.

Returning to the people-management side of training, scheduling—arguably the single most challenging aspect of training management, and one that only scales in complexity as the group being trained scales in size—represents a night-and-day difference when weighing generics and industry-built systems. Although any calendar tool allows leaders to manually build schedules, few allow for automated provisioning of people, equipment, and learning spaces, often with the click of a button once the rules are set. Compared to bouncing between a generic TMS and the department's calendar tool of choice, a TMS with this level of automated support can turn scheduling from a burdensome, lengthy task to a near-afterthought. This is only true if the organization chooses a platform built for the challenges of first response training management.

Finally, it should be noted that none of these features exist in a vacuum. While an agency that is using generic tools might deploy multiple software solutions to support their general-purpose LMS, these solutions will not offer a fraction of the interplay and integration a fully featured, response-specific TMS brings to the table. Putting it in terms of physical tools, it can be the difference between multiple fixed-head drills and a single electric piece with interchangeable heads: both have their uses, but only one has the flexibility to handle multiple interrelated tasks from a single source.

## Conclusion

In response agencies, training can simultaneously represent a tool, a shield, and a tremendous undertaking for the people tasked with managing it. Doing an efficient job means better

personnel performance, a safer public, and, where necessary, a stronger legal defense. On the inverse, treating it like a secondary concern opens the organization, its personnel, and the public they serve to unnecessary risks.

In other words, the effects of training are pervasive, and the work required to manage it properly can quickly become unwieldy using generic tools. This self-inflicted complexity only grows as the number of generic tools deployed does. Instead of attempting to make isolated tools work together, a purpose-built system offers the features, security, certifications, and capabilities responders need from the onset—and integrates them in a way that negates administrative headaches and greatly reduces the legal shortcomings plaintiff attorneys love to target. For all the advantages general-purpose training solutions offer organizations with simpler training needs, that makes a purpose-built TMS the clear-cut best choice for the organization weighing its options. Choose wisely.

**To cite this article:** Envisage Technologies. "Choosing a TMS: The Hidden Risks of Choosing 'Generic' Software" https://www.envisagenow.com/purpose-built-software, 30 August 2018.

## References


[1] Konkel, F. (2017). Forrester Predicts Less Money for Federal Tech, More for State and Local. *Nextgov*, 10 February 2017. Retrieved on Feb. 21, 2018 from http://www.nextgov.com/cio-briefing/2017/02/forrester-predicts-less-money-federal-tech-more-state-and-local/135351/.

[2] Rashid, M. H. (2008). Measuring and achieving quality customer service: a study on public sector in Malaysia. Thesis. Retrieved on Feb. 21, 2018 from http://scholarworks.rit.edu/cgi/viewcontent.cgi?article=1840&context=theses.

[3] (2017). Spoliation: Why Even the Worst Training Records Are Better than No Records at All. *Envisage Technologies*. Retrieved on Feb. 26, 2018 from https://www.envisagenow.com/spoliation/.

[4] Associated Press. (2015). Budget cuts pose threat to police training in Michigan. *Washington Times*, 23 March 2015. Retrieved on June 13, 2017 from https://www.washingtontimes.com/news/2015/mar/23/budget-cuts-pose-threat-to-police-training-in-mich/.

[5] (2016). Records Management: A Means to Legal Defensibility and Cost Savings. *Envisage Technologies*. Retrieved on February 26, 2018 from https://www.envisagenow.com/records-management-a-means-to-legal-defensibility-and-cost-savings/.

[6] Storm, D. (2017). Forrester Predicts Less Money for Federal Tech, More for State and Local. *Computerworld*, 30 January 2017. Retrieved on Feb. 22, 2018 from https://www.computerworld.com/article/3163046/security/police-lost-8-years-of-evidence-in-ransomware-attack.html.

[7] Iyer, K. (2015). Anonymous bring down Denver City website to protest against fatal police firing. *Techworm*, 25 April 2015. Retrieved on Feb. 22, 2018 from https://www.techworm.net/2016/04/anonymous-bring-denver-city-website-protest-fatal-police-firing.html.

[8] Knight, C. and Strickley, B. (2016). 'Anonymous' hackers release CPD officers' data. *Cincinnati.com*, 22 Feb. 2016. Retrieved on February 22, 2018 from https://www.cincinnati.com/story/news/2016/02/22/anonymous-releases-personal-info-52-cpd-officers/80722040/.

[9] Lohrmann, D. (2006). Is FISMA Compliance for State & Local Governments Too?. *CSO*, 5 December 2006. Retrieved on February 23, 2018 at https://www.csoonline.com/article/2135660/core-java/is-fisma-compliance-for-state---local-governments-too-.html.

[10] Kirkos, B. (2016). Minnesota police officers appear on kill list; ISIS connection cited. *CNN*, 6 March 2016. Retrieved on February 26, 2018 at https://www.cnn.com/2016/03/16/us/minnesota-police-officers-kill-list/index.html.