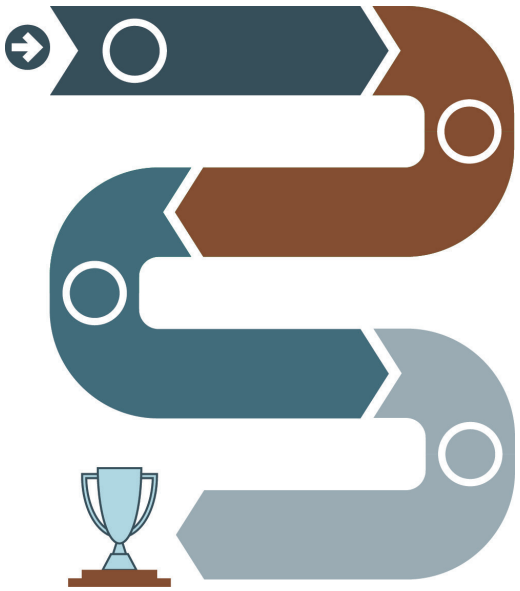
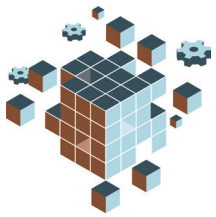
A Compliance Roadmap for Remarketers



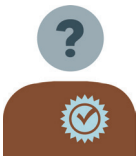
Introduction

Virtually all corners of the remarketing industry have watched the compliance burden grow with added security requirements, regulations, and other scrutiny. The auto lending community especially has allocated massive amounts of focus and resources to address these new and evolving challenges, and those efforts—and costs—quickly trickle down to the vendor community, and the end consumer.

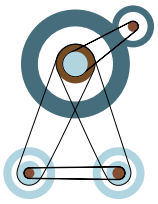
AutoIMS is an active participant and observer in the compliance efforts of our clients and partners, constantly evaluating how the tools and data present in AutoIMS can ease this compliance burden. While the intensity and impact of regulation may ebb and flow as administrations change, the age of consumer protection, data privacy, and greater transparency is here to stay. We hope this paper will provide ideas for all corners of the remarketing industry to consider, with the **ultimate goal of saving time and alleviating risk.**



IT Systems &
Data Security



Human
Resources

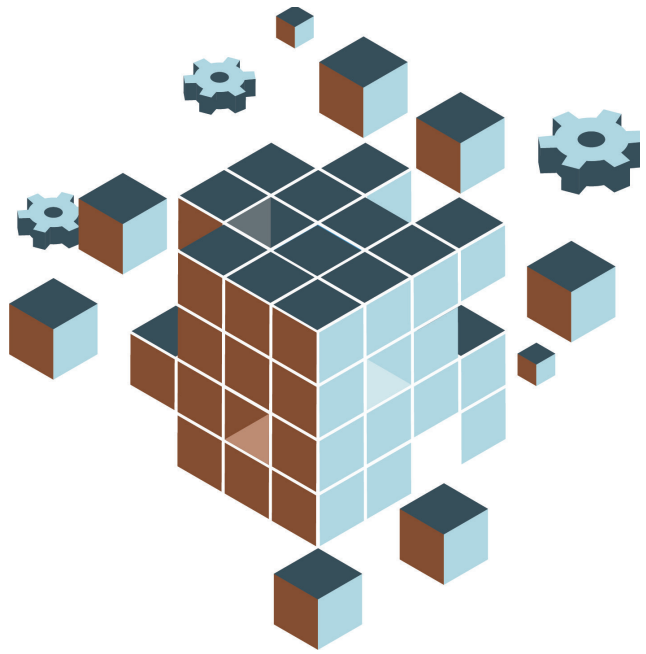


Business
Operations

Breaking it Down

Broadly, compliance serves as an ever-present undercurrent to virtually all that your business does. State and federal laws influence many of the routine tactics deployed by the automotive industry to sell and service the financial instruments behind selling cars. This approach leads commercial consignors—especially those in the lending community—to hold industry vendors accountable as though they were a part of the lender organization itself. Third-party risk assessments, detailed questionnaires, audits, and other tactics are deployed to set and enforce expectations. Those expectations come not just from the now-infamous Consumer Financial Protection Bureau (CFPB); but from the FTC, state attorney offices, OSHA, FCPA guidelines, and the constantly-moving target of data security. Savvy organizations will remember that many of these agencies and their regulations, especially the CFPB, work for the protection of the consumer, not the lender.

AutoIMS weighs our approach to these challenges carefully, and we find that most compliance challenges can be found in one of three key areas on your compliance road map: HR/workplace, Business Operations, and IT Systems & Data Security. As you would expect, our biggest focus is on IT Systems & Data Security.



IT Systems & Data Security

The data is a great place to start when thinking through security strategies and other actions needed to meet compliance requirements.

The Purpose of the Data

Careful consideration about what data is needed to facilitate each business process can help mitigate many security concerns and speed decisions about contracts and data structures with various vendors. For example, a debtor's address or social security number may be critical data for a repossession or skip tracing vendor, but are those elements needed for the remarketing process once the vehicle was recovered?

Vendors need to take the stewardship of data in their possession seriously, and need to come up with processes and policies to treat data with the utmost level of professional care. Still, it's worth the reminder that specific to remarketing, **the data in a vendor's possession is typically low risk and is tied to a vehicle —not a person.**

Thus, for lender clients specifically, we recommend as best practice that remarketing business leaders educate their internal security and compliance teams about the business processes and types of data being handled by their vendors. A constant education and reevaluation of remarketing data can lead to vendors being classified in lower risk categories, easing the contract and compliance burden on all parties. The idea is not to ignore risks, but to better understand and classify them appropriately.

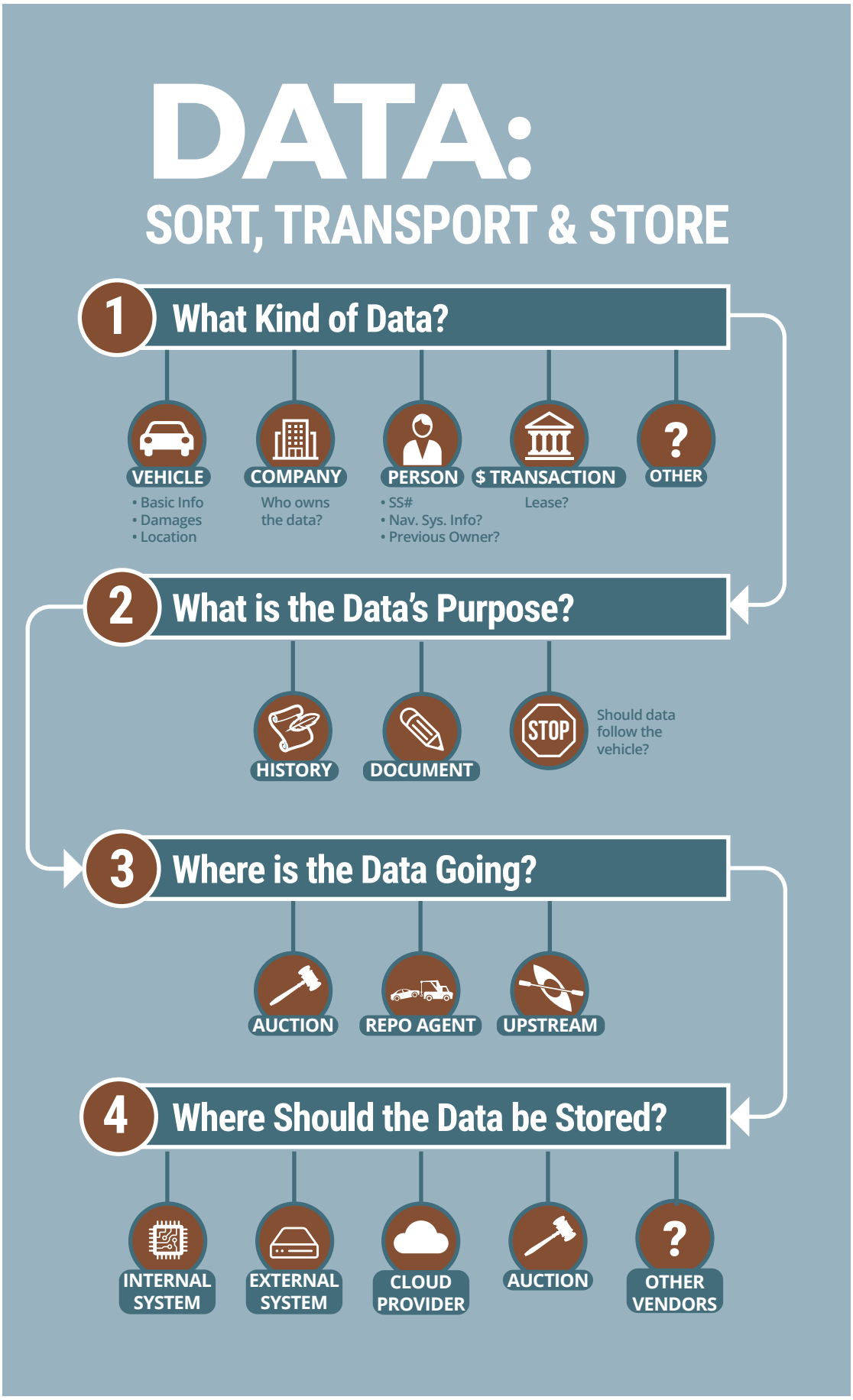
The strategies outlined above can help **keep costs for everyone reasonable** and allow the business users to focus on the functionality and benefits they are seeking from their stable of providers. As for vendors, taking steps to overachieve client expectations is a great way to get ahead of aggressive data security expectations and influence the classification process.

Where the Data Goes and How it Will be Stored:

Only once the respective purpose for data is identified, can confident, intelligent decisions be made about where that data should go, how it will get there, and whether and how it is stored. Additional questions can guide decisions on this front:

- What security protocols for data transfer and storage do your technology providers have in place to safeguard your data and that of your clients?
- What if servers are compromised, ransomed, or otherwise fail?
- Is there a disaster recovery plan and is it tested routinely?

These questions aren't just for technology vendors anymore; but a fitting example in our industry can be found with auction management systems. Whether home-grown or purchased, cloud-based or on-premise, these systems are vital to the ability of an auction to operate. All parties—auctions, clients, and the AMS provider—need to work together to regularly verify the integrity of those systems.


DATA:
SORT, TRANSPORT & STORE
1 What Kind of Data?
VEHICLE
• Basic Info
• Damages
• Location
COMPANY
Who owns the data?
PERSON
• SS#
• Nav. Sys. Info?
• Previous Owner?
$ TRANSACTION
Lease?
OTHER
2 What is the Data's Purpose?
HISTORY
DOCUMENT
STOP
Should data follow the vehicle?
3 Where is the Data Going?
AUCTION
REPO AGENT
UPSTREAM
4 Where Should the Data be Stored?
INTERNAL SYSTEM
EXTERNAL SYSTEM
CLOUD PROVIDER
AUCTION
OTHER VENDORS

Food for Thought

As a technology vendor with responsibility over volumes of consignor, auction, and third party data, AutoIMS relies on numerous procedures, policies, and practices to ensure the availability, reliability, and security of our system.

Moving Targets: Routine system vulnerability scans keep us on the lookout for external hazards to servers. Annual Disaster Recovery (DR) tests are also conducted to ensure we are poised to react quickly and effectively should we need to implement a fallback plan. **A strong and ever-evolving 'checks-and-balances' procedure—**including increasing use of automated testing—ensures that new code releases and other system changes will not only work, but avoid any adverse impacts on the rest of the system and code.

Getting Organized: Our IT ticketing system allows us to track all technical development projects and related activity. This ensures we have a record of the things we do both for the website and other areas related to the protection of data as autoims.com and its many components continue to evolve.

Fine Print: Our contracts now prohibit the sending of personal information (PII) and state that we will not be contractually obligated to protect it. This policy encourages our clients to think carefully about the data they send us. We routinely monitor and update our policies related to retention periods for everything from vehicle data, to emails, and contracts. We are in the process of rolling out a new, well-documented vendor/3rd party management program as we continue to augment our offerings with outside providers. We also accommodate custom requirements for encryption and security protocol at additional cost when necessary.

What if Godzilla steps on your building?

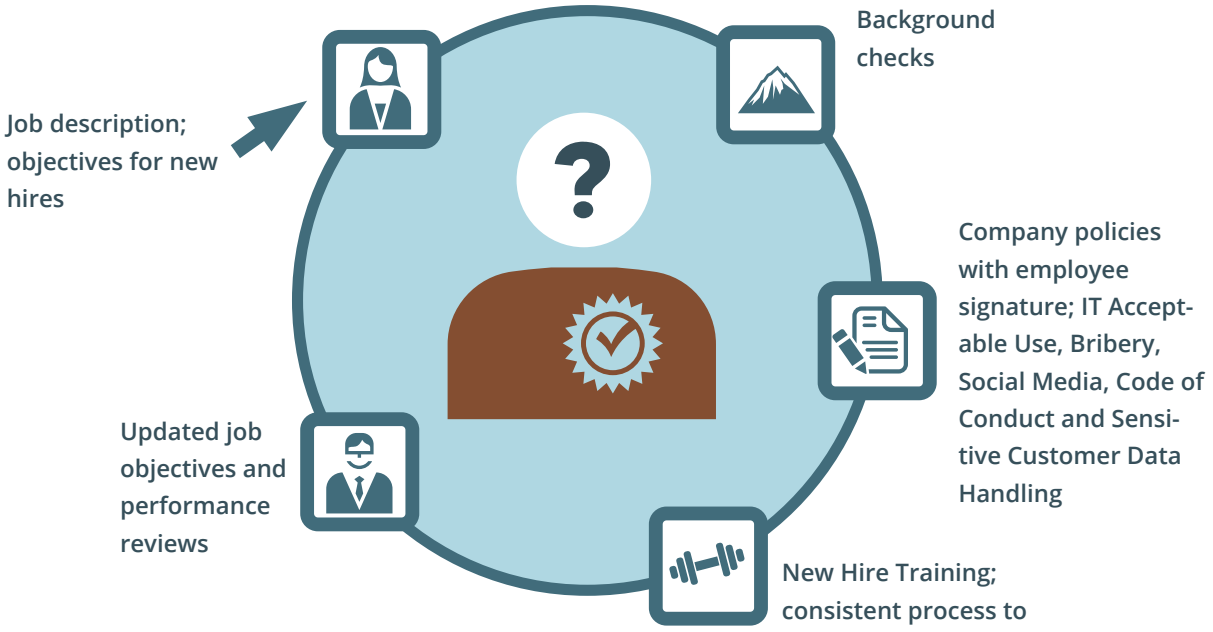
It's safe to say that we won't be attacked by prehistoric, irradiated, behemoth sea monsters, but for those managers who don't routinely think about business continuity, using an otherwise absurd metaphor to help strategize and plan for unforeseen events can help. Much of our Business Continuity Plan revolves around how we would continue to operate and serve our clients if Godzilla were to step on (ie. destroy) our building. Of course, it's far likelier that the rare, simple Atlanta ice storm will prevent us from getting to the office, and when it inevitably does, we want our clients to be none-the-wiser. Come to think of it, we're still not sure what's more destructive—Godzilla or an Atlanta ice storm!

Compliance Considerations for the Rest of Your Business

While the lion's share of our paper focused on the technology aspects of compliance, we thought it made sense to share reminders or perhaps a few new ideas and perspectives we've encountered along our own compliance journey in other key areas of our business.

Human Resources

HR responsibilities, at a minimum, cover payroll, workplace policies, hiring practices, and other sensitive processes that directly relate to a company's most important and expensive assets: employees. Hiring is a fine example of a process steeped in compliance concerns, including:



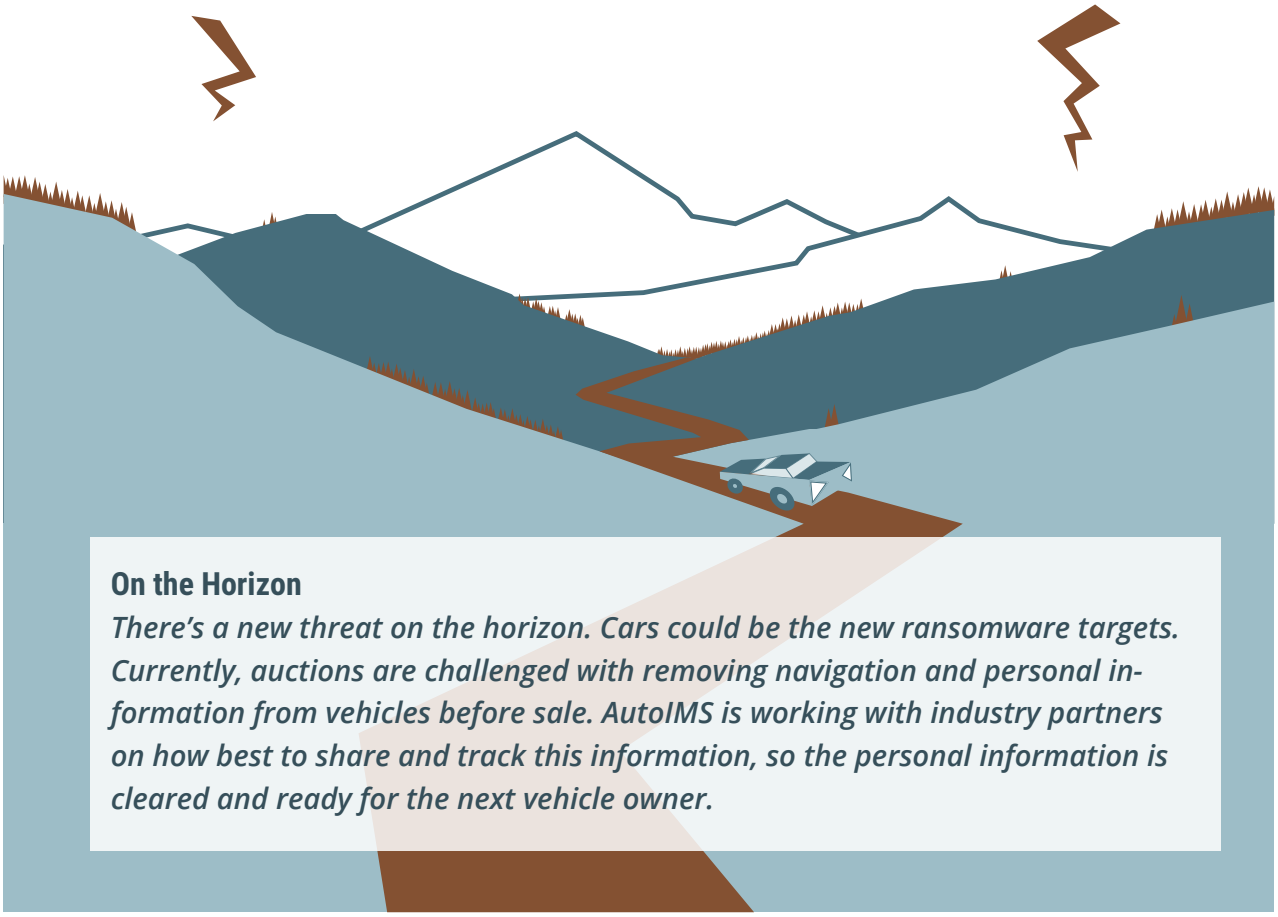
Why it matters:

- Compliance with Equal Employment Opportunity Commission
- Duty to clients and employees to maintain a safe workplace
- Documented understanding of expectations
- Meet client requirements
- Avoid discrimination and harassment opportunities
- Advance AutoIMS goals of being employer of choice, provider of choice, and investment of choice

Human Resources (con't)

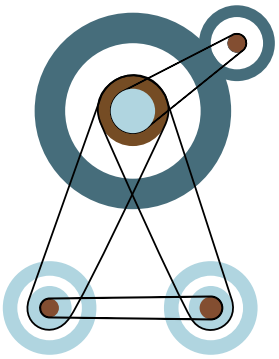
Strategizing around agreed upon policies can aid in determining salary guidelines, help you practice fairness in workplace rules, and provide validation for promotions or letting people go.

More and more, our lender clients look for practices where we inspect what we expect, including how we hold employees accountable for the jobs they were hired to do and the data they touch. While sometimes their questions and audits seem intrusive, in most cases they've helped us improve or at least validate several of our HR policies and practices.



On the Horizon

There's a new threat on the horizon. Cars could be the new ransomware targets. Currently, auctions are challenged with removing navigation and personal information from vehicles before sale. AutoIMS is working with industry partners on how best to share and track this information, so the personal information is cleared and ready for the next vehicle owner.



Business Operations

Inextricably linked to HR, but moving in to the other administrative areas of the business upon which every company must execute to succeed, business operations' functions are under a new microscope in the compliance world. **Smart companies will use this scrutiny to improve, rather than just check a box.**

Policy	Do	Don't
Business Continuity and Disaster Recovery	Understand the mission critical resources of every department	Assume that nothing bad will happen
Harassment and Discrimination	Be aware of state and federal law	Define harassment and discrimination too narrowly
Privacy	Put yourself in your employee's shoes	Put policies into place without consideration of negative repercussions
Work from Home	Set clear expectation of technology & environment required at home	Assume employees will self-manage workload from home
Pandemic	Have multiple plans for a variety of circumstances	Assume that you are immune
Workplace Security	Setup keycard/badge system & monitor entrances	Leave doors open and un-monitored

Well-documented policies and procedures bring structure, understanding and accountability into day-to-day operations. Reaping the benefits of these new policies without stifling creativity or speed takes the time and effort of managers from across the company upfront but will pay off in the long term.

Doing the Numbers

Financial stability is another area of concern for clients as they examine vendor businesses. Financial statements often seem like too much detail, and if they were to be shared, would they even be understood? Often, providing a high-level financial summary without specific numbers while **assuring a level of profitability or balance sheet health is enough to satisfy vendor management requests.**

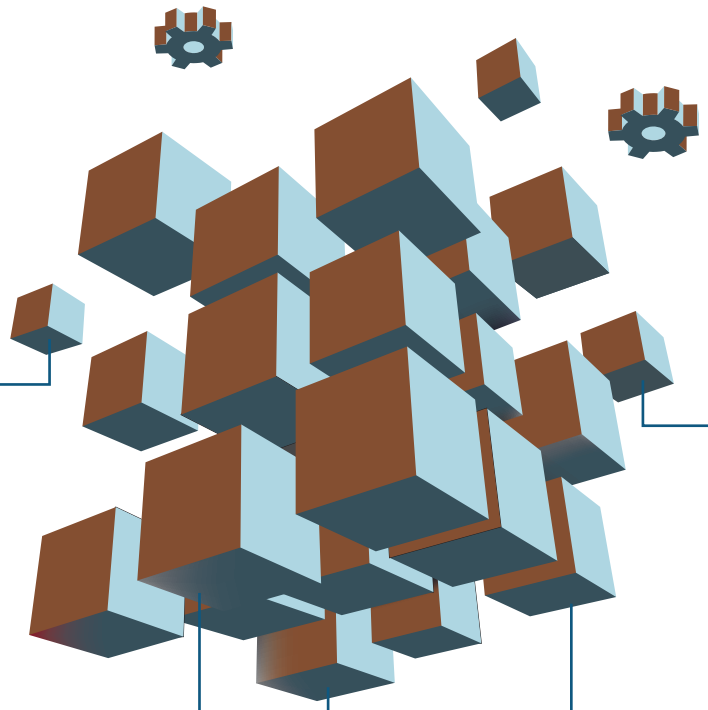
Internally, ensuring the financials read cleanly and clearly in relation to the primary revenue and cost centers of the business gives managers critical data for decision making and planning for a range of outcomes. Aligning key employee goals to the financials and providing the right level of visibility and transparency to the results is an important balancing act for the management team.

*Hoping for the **best** is fine; **planning** for the **worst** is **essential.***

AutoIMS Can Help You with Compliance

We explored far more than just the remarketing process in this paper. We hope that reading part of our compliance journey helps you with your own. Meanwhile, it's worth mentioning that clients lean on us for compliance concerns at the vehicle level, too:

In the past year AutoIMS added a field to indicate the presence of personal property. The consignor can use this to hold repo agents accountable for removing personal property before the vehicle arrives at auction.



LiveReports functionality can be used to track charges posted against the vehicle and track returns on pricing, especially if you are audited by the CFPB. Learn more here: www.autoims.com/auctioncharges.

Some clients have leaned on us to customize transmissions from AutoIMS to block sending sensitive data like client account numbers to auction systems or other places where it isn't needed.

SFTP connections are mandated for all integrated clients, providing a more secure exchange of the data that drives remarketing.

Documenting customer interactions in AutoIMS can turn a vague memory into a trackable trail. AutoIMS has multiple Note types to help, including a large number that are system generated and endless possibilities for custom notes.

Compliance @ AutoIMS

Keely Smith, Director of Contracts and Compliance. An AutoIMS long-timer, Keely touches every part of our business through her work in onboarding assistance, contracts, billing and all things compliance. “I care about compliance because every employee will come across it in their day-to-day work. It’s not just about rules & regulations—it’s about keeping people, companies and clients safe.”

Madiha Merchant, Contracts & Business Operations Specialist. Madiha works closely with Keely on all things agreements and compliance, providing additional perspective and research to keep AutoIMS compliant. “It’s imperative that we review our business processes routinely to anticipate risks and their potential impact, adjusting employee and client expectations accordingly.”

Beverly Heslin, HR/Office Manager. Beverly keeps our office (and our business) running smoothly and securely while helping boost employee engagement. “When employees and clients can rest assured that their information is secure, they can focus on other, more impactful issues,” says Beverly.

Don Stephens, Director of Systems & Security. Don manages the team that safely enables our clients and employees to execute the digital magic that they rely on for their jobs (everything from the servers that run autoims.com to employee computer support). Don could wax poetic, but he’d rather remind you, “The bad guys are getting smarter. Don’t click on anything that you weren’t specifically expecting. Call a System Administrator if you have any doubts!”

The Art & Science of Remarketing

AutoIMS is partnering with clients to address their compliance needs today, and to prepare for future developments. As an extension of the consignor or auction staff, the AutoIMS team has industry-wide experience and best practices to share. Our nimble approach is designed to help consignors and auctions save time and money, increase accountability and more easily navigate compliance requirements.

Client Support offers training and trouble-shooting for consignors, auctions and third party providers onsite or via WebEX.
clientsupport@autoims.com

The Solutions team works with clients who are ready for more advanced AutoIMS functionality or customization.
solutions@autoims.com

Reach both teams at 888.683.2272.

autoims.com **888-683-2272** **autoimssolutions.com**