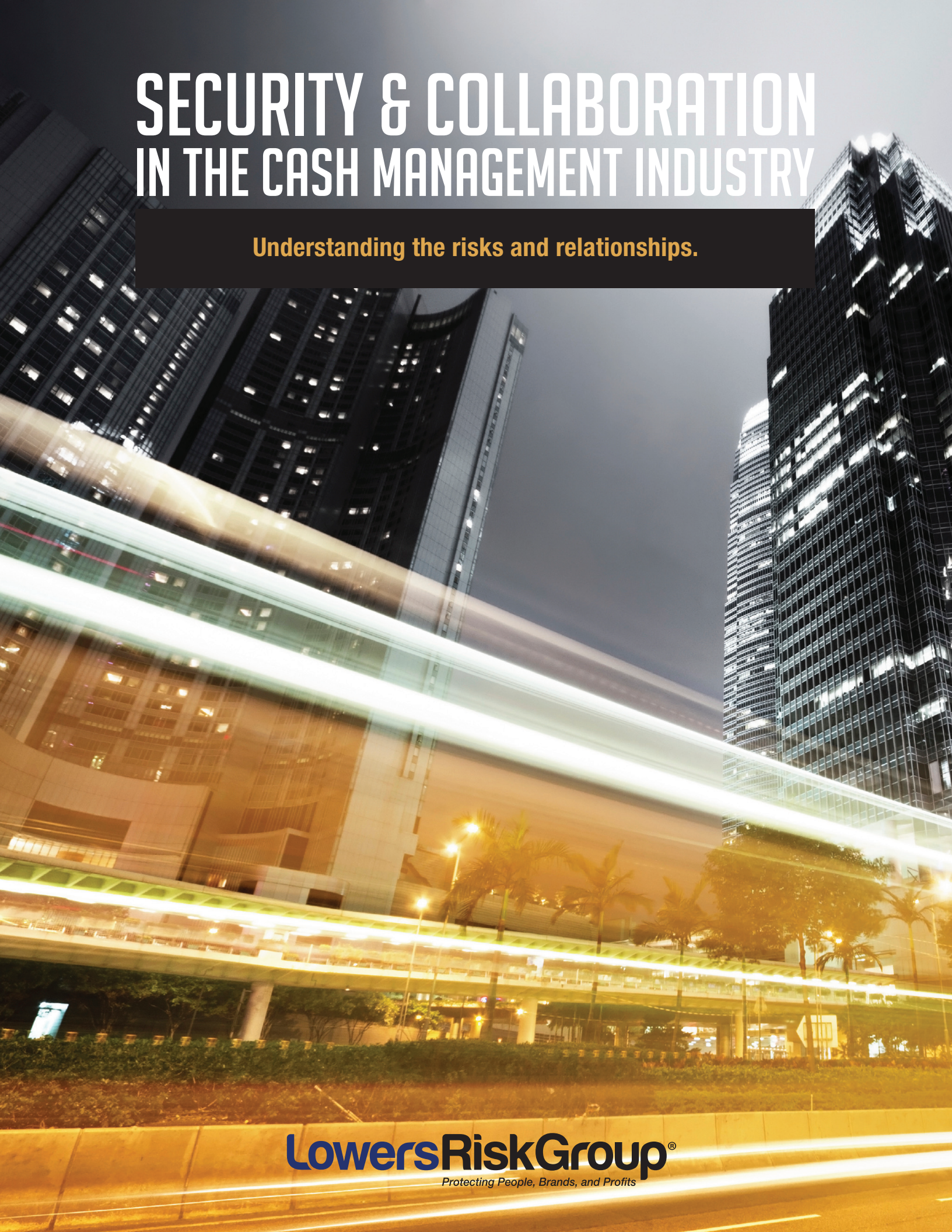


SECURITY & COLLABORATION IN THE CASH MANAGEMENT INDUSTRY

Understanding the risks and relationships.

LowersRiskGroup®

Protecting People, Brands, and Profits

We live in a world where it is so common to make purchases by using a debit or credit card, it would probably surprise the vast majority of the general public to realize that billions of dollars in old-fashioned cash and coin flow through our economy every day. This flow accumulates in banks, cash and coin processing centers, and retail establishments as millions of consumers make purchases and deposits.

At some point in this payment and deposit process, cash and coin ultimately have to be processed—perhaps physically transported, relocated, or stored in a vault as a result of the accumulation. Among other things, this may involve depositing or crediting funds into accounts, providing liquidity to cash registers at retail establishments, or replenishing ATMs.

The cash management industry has evolved over the years to facilitate these processes, transfers, transportation, and storage. As the industry developed the "cash-in-transit" (CIT) system to manage cash handling services, it became necessary to manage the risks associated with it. As third party service providers, CIT businesses must provide the security, integrity, and accountability to the banks and other customers who require and depend on the supply of cash and coin to make markets work and businesses run.

The inevitable risks of cash and coin transfer and processing generally make effective controls and precautions designed to prevent and protect the currency mandatory. Cash and coin transfer inevitably creates the threat of potential risk of loss due to external crime (robbery, burglary, extortion), employee theft or fraud, and carelessness or negligence. These risks can lead to substantial losses in the millions of dollars, clearly justifying the creation and use of various risk mitigation techniques.

The components of the CIT system, including their functions and linkages, determine the vulnerabilities in the system and therefore the kinds of risk mitigation techniques that are required. In this paper, we outline the CIT system and the cash management industry, identify key vulnerabilities, and propose some best practice controls for some of these risks.

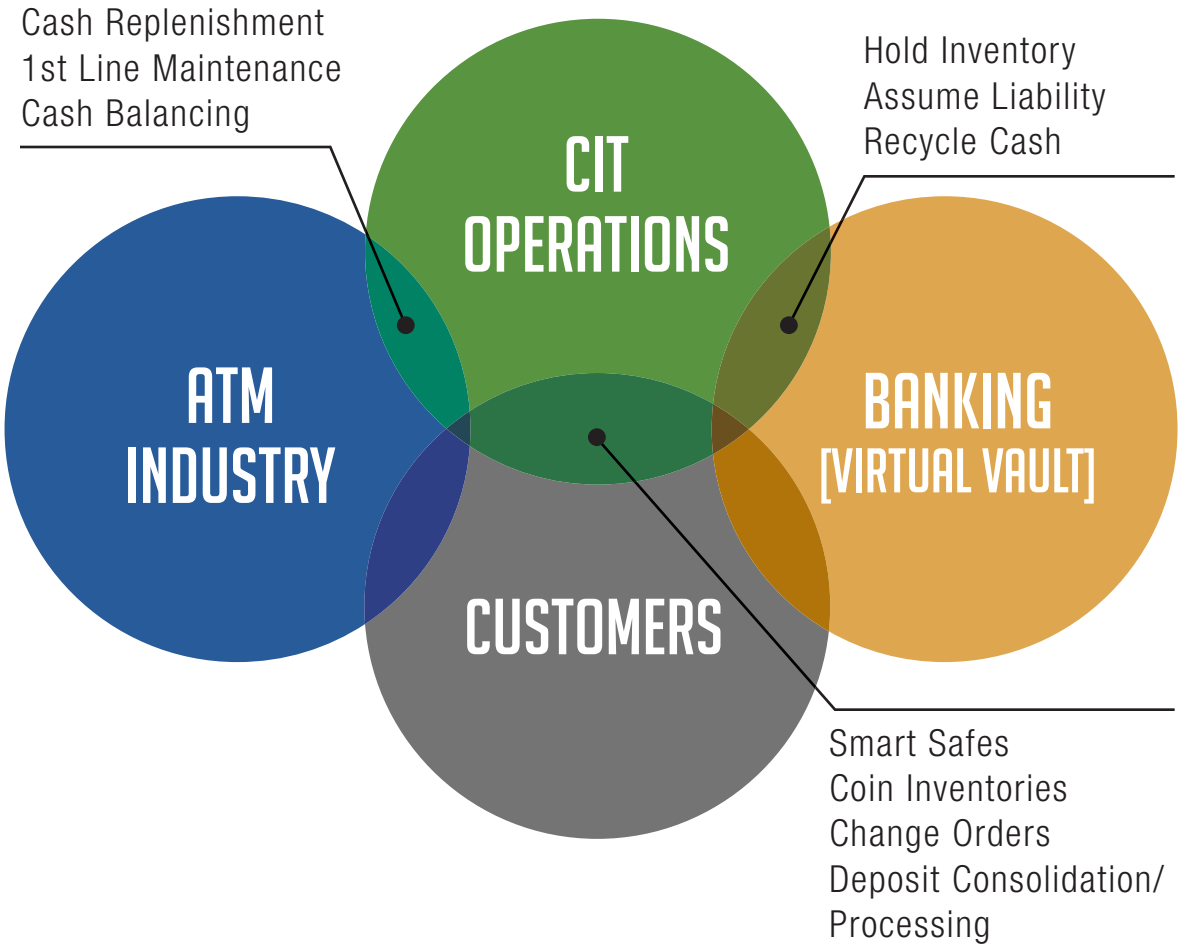
THE CASH-IN-TRANSIT SYSTEM

CIT is more than moving cash and coin from point A to point B. Although we continue to use "CIT" as common shorthand, the industry might be more accurately called the "cash management industry". This industry now provides services including virtual vaults, comprehensive ATM services, and auditing and banking functions such as deposit processing, branch bank orders, and check imaging. Armored carriers are just the most visible part of the system to most people.

Some CIT businesses offer comprehensive traditional banking services, while others may concentrate on ATM specific services. Within the ATM services spectrum, carriers may do some or all of the activities from installation and setup, to cash and coin handling including back office balancing and currency management, to maintenance. As these services have evolved, we have come to the point where a bank vault center and an armored carrier involved in cash services might look and operate identically.

The following diagram illustrates the primary functions of the CIT system and shows where the components overlap. In this picture, the "customers" are mainly banks, branch, or storefront banks, and ATM networks, but may include retail operations, credit and debit card processors, and other operations that depend on liquidity. And of course, the ultimate source of cash and coin is the Federal Reserve.

UNDERSTANDING RISKS & RELATIONSHIPS
IN THE CASH INDUSTRY



Today, CIT companies work collaboratively with their bank customers and the Federal Reserve to ensure funds are kept on hand to supply to the storefront bank operations and their customers directly. Banks and ATMs are everywhere and the desire to continue spreading their footprint continues. However, the typical storefront bank today is not designed or expected to manage or store large volumes of cash or coin.

In these circumstances, it makes perfect sense for banks to outsource cash management functions. CIT companies are established throughout the country with networks of hardened facilities and the capability to mirror all the necessary functions done internally at a bank vault. These third party bank vault operations can provide back office support in secure facilities that would be cost prohibitive for individual banks.

While with certain designs it is feasible for a bank teller to conduct ATM replenishment, it is undesirable when there is no indoor kiosk to protect against outside threats. **With the continued growth of ATMs and the increased risk in servicing these machines outdoors, many banks rely on CIT companies to do this service for them.** Even with an internal bank vault providing back office support, banks rely on CIT companies to transport cash and coin to and from the storefront locations and the vault center.

Retailers and other businesses establish a direct relationship with the banks and may see the carrier simply as a secure transport operation. However, the reality is that the carrier is often a one stop shop, providing the bank with all the necessary services in the currency cycle from providing cash and coin orders, processing cash and coin, vaulting short term deposits, processing deposits, and maintaining a currency and coin inventory.

PARTNERS IN RISK MANAGEMENT FOR CIT

Just as banks have transferred the responsibility to CIT carriers for total cash management, they have also transferred the risk.

The cash and coin in the CIT carrier vault still belong to the bank, and the carrier is responsible to guarantee that value to the bank. The risk of loss is very real: while a typical theft may not be all that substantial, the potential for a huge loss is there and it does happen.

CIT companies may be able to absorb certain losses internally, but a large loss could devastate them. Therefore, other businesses have developed products to protect against large losses.

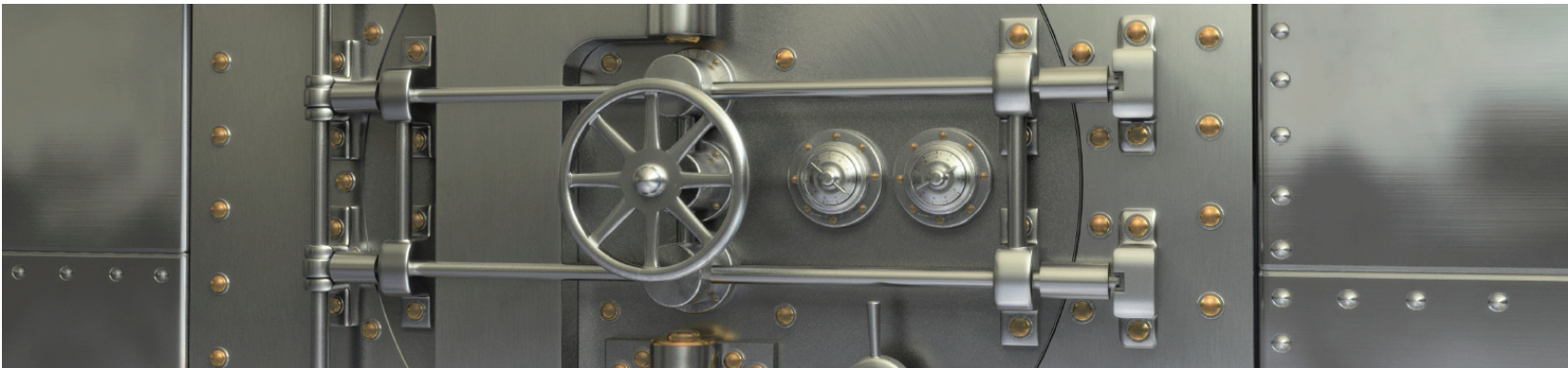
INSURANCE COMPANIES

Insurers that specialize in CIT coverage provide the necessary safety net. Since huge losses could also devastate the insurers, they will impose underwriting criteria to ensure that risks are managed using best practices. They will evaluate everything from transportation services to facility design to all processing activities.

THIRD-PARTY AUDITING FIRMS

These firms may be used by insurers, banks, or carriers to identify compliance, accountabilities, risk concerns, and corresponding solutions.

Every party in the system has a vested interest in identifying, measuring, and mitigating risk. Even though banks have transferred the risk, they want to know their cash and coin are guaranteed and that they will not suffer business interruption. Insurers want to ensure that the risk is low with the appropriate controls, and will base their premiums on the level of risk. Carriers want to satisfy their customers, the banks, by having appropriate insurance coverage and keeping premiums down by meeting underwriting standards.



KEY VULNERABILITIES

Wherever there is a lot of cash and coin flowing, there is a potential for loss. The CIT system is huge, and potential losses exist at innumerable points.

1 | LOSS OF LIFE

The potential loss of life is the top concern. While the numbers are generally low in terms of fatalities, attacks on crews or even the branch facilities are often violent. Even where controls are in place to minimize the street and branch attack exposures, the resulting losses can still be substantial. When attacks do occur, the cases are most often solved with the perpetrator put away, but this is an ongoing threat to the industry that cannot be understated.

2 | ORGANIZATIONAL FRAUD

As in most industries, the biggest vulnerabilities are internal, including losses from errors in processing and servicing as well as internal theft or fraud. There are many opportunities for loss in the transfer and handling of cash and coin, and of course cash is the perfectly liquid prize that can be hidden or exchanged.

However, one significant area of concern is when key management or even owners are involved. An owner-involved loss would not be insurable, which complicates things for CIT customers. It is a recipe for problems when the very top management can access and manage currency controls with no further oversight from an external source. Management or owner-involved losses may not be the most common type of loss, but they have the potential to be much larger and harder to detect when they do occur.

Risk escalates dramatically if management decides to exercise their authority over the rest of the staff in an effort to compromise controls. After a theft occurs, staff may recognize the lack of controls, but not necessarily the loss itself. For example, if the high level perpetrator keeps one set of records that is used at the branch showing actual balances, while a separate set with inflated numbers is used to provide balance information to the customer, this will be difficult for balancing staff to detect. A loss such as this could easily be in the millions of dollars.

3 | ATTACKS ON ATMs

Another significant vulnerability is with ATMs. Without question, a robbery event could result in a significant loss and, as previously mentioned with the nature of street attacks taking place against an armed CIT person, could involve a high degree of violence. Again, however, an internal loss can be far greater. A common servicing practice is for one person to be involved in the actual handling of the currency at the machine. In general, any single-control cash handling increases the likelihood of loss. ATM servicing via cash swap and unsealed cassettes, where direct cash handling and/or access capability is involved is essentially single-control. A sealed cassette may be no more effective in preventing loss, depending on the seal installation and controls around the seal usage.

High losses will invariably occur when a dishonest servicer begins taking large sums of money and is smart about covering up the trail. To conceal the theft, the servicer can take funds from the incoming replenishment in the amount of the shortage, and then add them to the residuals to make it appear in balance when this goes back to the branch for reconciliation. The machine will run short, but a servicer knowing the common threshold to manage to, will make this difficult to detect by an outsider.

Besides a direct cash theft at the machine, there are indirect methods that can pose a high loss potential. For example, a servicer who has the ability to change the ATM settings with master codes can manipulate dispense amounts by programming the machine to indicate the cassette is holding a lower denomination. Another example is an intentional cross-load, placing the wrong denomination in the dispensing cassette. A servicer doing this in collaboration with external accomplices will complicate a loss investigation and could impose a notable loss.

RISK MITIGATION STRATEGIES

A risk management department will investigate losses. But equally important, it should proactively address risk by evaluating routine performance compared to company control standards, with an emphasis on internal controls. Inspections, reviews, and audits at the branch level and above are essential to assess the integrity of the branch controls as well as the protected assets. These would involve department level and key function procedures, access device controls, and currency (cash and coin) audits.

CORE CONTROL CONCEPTS FOR CIT

There are core concepts of control in the CIT industry that extend to all currency handling entities.

DUAL CONTROL

Dual control is one of the most common controls, with procedural and physical variants. Procedural dual control means a second person will be involved in the verification, before the currency moves on to another stage of processing, deposit, or storage. Physical dual control requires enabling a physical constraint with the use of locks to make it necessary for two different people to be present with their respective key, combination, or code, to gain access to any restricted access areas.

A separate but related concept is dual custody, which generally means that two people are present for a given action.

SEPARATION OF DUTIES

Separation of duties ensures there are job functions that actively prevent currency manipulation. A person who counts and handles currency should not have the ability to also report to the customer, such that the reported balance differs from the actual balance undetected. The lack of separation of duties can very well make all other efforts futile. For example, if a customer inventory is balanced under dual custody, but the physical totals are not the same as reported to the customer "by a dishonest person who has manipulated the funds," the dual custody action will not have been an effective control measure.

ACCOUNTABILITY

In the end, there must be accountability when non-compliance is identified. If the consequences of a loss are not reflected by internal action, oversight will not prevent future losses. While appropriate corrective action may include re-instruction or retraining as appropriate, the message that intentional noncompliance or negligent actions will not be tolerated should be made forcefully.

ESTABLISH WRITTEN POLICIES & PROCEDURES

Policies that adopt industry best practices are at the forefront of a risk management program. Staff should be well trained in industry standards and in the company's application of them, and ideally, experienced staff will be in charge of oversight. In addition to best practices standards, staff must also use proper auditing practices to include depth and techniques to adequately assess via interview, paperwork, and observation (live and/or pre-recorded CCTV).

STAFF TRAINING

Taking the time and appropriate measures to find the right qualified staff to work in an environment, and training them accordingly, is fundamental to success. The HR hiring process must use every tool available to minimize hiring risks. The risk management team should ensure that this is a focal area which is included as part of the evaluation process.

RANDOM AUDITS

Random cash and coin audits are essential to detect theft and fraud when routine controls fail. These audits will help ensure that losses do not mount unseen. Random audits would be performed on customer inventory at the facility and also at ATMs (where no regular rotation of servicing staff exists).

EXTERNAL THREATS

A strong risk management plan would be remiss in this industry if it did not involve a proactive strategy to address external threats. These would include street surveillance that addresses crew safety and security performance, evaluating customer stop locations for risk concerns, and appropriate communications channels and tools to address higher risk events and threatening situations.

EXTERNAL AUDIT

It has become a standard expectation that CIT companies will have an internal audit. However, many companies are under pressure to cut costs, and their internal teams may be deficient for a number of reasons, such as:

- **A conflicting chain of command may make negative reporting difficult**
- **Competing managerial objectives might emphasize quantity over quality**
- **Quality of the auditing personnel skills and methods used**

A third party or external audit firm is a solution. A independent firm that is well versed in industry best practices will help resolve the conflicts and inadequacies noted above. The external audit component would involve evaluating company standards against best practices, collaboratively elevating the standards where necessary, and then independently testing for compliance to the prescribed standards.

The audit firm would also be used to conduct comprehensive cash and coin audits. Unlike a bank auditor that would be limited to their specific funds due to confidentiality concerns, a third party auditor would be able to perform a full vault audit, to include a reconciliation and direct confirmation with all of the carrier's customers.

A partnership with an external audit firm will give peace of mind to the carrier customers, as well as their insurers. Some banks or insurers may even mandate the practice. Ultimately, gaining valuable insight into industry best practices, from an outside source that sees the industry from a wider lens, is a key benefit. This process can recalibrate company controls to improve transparency, effectiveness, and trust among partners.

CONCLUSION

While the cash management industry evolves, certain things remain the same: the perpetrators of theft and fraud are always out there. Vigilance in the approach to managing and protecting currency at all levels is vital. CIT carriers' servicing staff and company management, retailers, and other serviced entities, the banks, insurers, and the third party firms should all be in sync, working collaboratively with the same goal: success in managing the risks of cash-in-transit services.

Let's discuss your risk management approach.

LowersRiskGroup®
Protecting People, Brands, and Profits

LOWERSRISKGROUP.COM (540) 338-7151