Internal Controls
Driver Licensing and Identification Processing

Best Practices

Introduction

The possessing of a valid or legitimate government issued driver license or identification (DL/ID) card has become accepted as primary evidence of personal identification. In the case of the driver license, it is being used as a form of personal identification in addition to the main purpose for which the document was issued; evidence that the holder is qualified to safely operate a motor vehicle.

The significance of the use of the DL/ID has been highlighted by the events of September 11, 2001. Consequently, the circumstances, which include not only the business process/procedures but also the supporting internal controls under which these documents are issued, are under scrutiny and review.

This document deals with internal controls within the environment of the DL/ID issuance processes, with a view to providing jurisdictions with information about current best practices and recommending specific actions with respect to this business process.

What are Internal Controls?

It is important to clarify what constitutes *"internal controls"* in order to fully address those controls within DL/ID processes. In looking at internal controls one must also look at risk. Identifying and managing risk means establishing controls to limit the potential for fraud. There are many definitions for internal controls within the audit field. For the purpose of this work, internal controls will be defined as *"mechanisms within the enterprise which have been designed to provide reasonable assurance regarding the achievement of the following objectives:*

- Effective and efficient operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations
- Safe and uniform application

Internal controls are basically good operating practices used to ensure that an organization achieves its desired objective. These controls provide assurances that information and data are recorded and reported as required. It is important to also note that internal controls in and of themselves should not be seen as the panacea to

organizations fulfilling their objectives but should be seen as an aid to achieving those objectives along with management of business process.
In Ernst and Young's recent *8th Global Survey – Fraud - The Unmanaged Risk* - 85% of some of the worst frauds were done by insiders, who were on the payroll of the organizations. The other trend that was evident in the survey results is that more organizations are now establishing formal fraud prevention policies. "*Internal controls, management review and internal audit remain the most useful fraud prevention and detection factors".*

There are two areas of internal control – *preventative/deterrent and detective.*

Preventative/Deterrent Controls are designed to discourage errors or irregularities. An example of such controls would be supervisory sign-off on any exception process.

Detective Controls, are designed to identify an error or irregularity after the fact. An example would be checking operator transaction logs against hardcopy supporting documents or even the typical financial audit; both are illustrative of detective controls.

Preventative/Deterrent	**Detective**
• Formal Values/Ethics	Audit/Investigation:
• Thorough employee training	
• Benchmarking and best practices	▪ Reasonableness checks
• Validity Checks	▪ Check digits
• Two person/stage processes	▪ Overflow checks
• System assigned numbers	▪ Date checks
• Pre-numbered forms	▪ Format checks (i.e.: only allow set formats)
• Good computer screen design	▪ Completeness checks
• Field highlighting	▪ Sequence checks
• Passwords/IDs	▪ Comparison controls
• Self-Help features	▪ Batch controls
• Management approvals/signoffs	▪ Time checks
• System or manual overrides	
• Comprehensive communication of the consequences of internal fraud	

The internal control challenges faced by motor vehicle administrators do not differ significantly from the challenges faced by any large organization with a large number of employees conducting a variety of complex business processes in a decentralized manner. Some of the approaches to mitigating risk within other large organizations are indeed applicable to the driver licensing and identification processes. These approaches can be broken down into four (4) categories:

- Human Resources
- Auditing
- Information Technology
- Business process

The analysis that follows will outline a series of *"best practices"* that jurisdictions could consider in addressing internal control challenges in the human resources, audit, and technology. The document will then outline two sets of recommendations, one dealing with specific control measures which jurisdictions must implement to address the key risk areas within the DL/ID business processes. The other recommendation deals with the need to for an audit plan.

Current Best Practices:

Human Resources:

- *Code of Conduct – Ethics and Honesty:*

Research suggests that the effectiveness of any control measure is based upon a set of core organizational values. Such values form the basis for guiding employee actions and behavior. These organizational values must be the cornerstone of all actions of employees and management.

These values should create a culture of honesty and ethical behavior. Such values, when articulated, demonstrated and reinforced, go a long way to set the tone of behavior within an organization. These ethical and honest values must be practiced by all levels within the organization, particularly the management level; otherwise, the values are viewed as just more "lip service". In some cases integrating these expectations into employee performance contracts serves to further emphasize the importance of this behavior.

Formal documents, which outline the organization or business unit's ethical practices or code of conduct, can be issued to each employee annually. This would serve as a reminder. The employee could also be required to sign a statement that they have read and understood the document. This practice can prove very useful not only as a deterrent to fraudulent behavior, but also to assist an organization in addressing a particular case of employee fraud.

- *Hiring the right employee – Background & Credit Checks:*

During focus group discussions with a number of government agencies, as well as commercial service providers, it was apparent that a key part of their recruitment process included the use of *background checks*. These checks would include a *criminal record, verification of information* provided as part of application/interview process and *personal references*. For example, verifying that the applicant did indeed attend the college that they stated. A number of organizations have also built in credit worthiness as a key component of the employee selection process. *Financial/Credit worthiness* can be seen

as a potential indicator of an area of possible exposure. Employees in extreme financial situations are more susceptible to bribery and theft, hence, the use of such financial checks in the employee recruitment process is also seen as a fundamental best practice. It is important to ensure that in using these sorts of checks that they do not automatically screen an applicant out, but are used as an indicator of potential areas of risk. Jurisdictions may choose to place different emphasis in certain areas dependent on the particular job function.

There may also be some other job functions where the use of *drug or limited scope polygraph examination* could be utilized as part of the employee selection and monitoring process. Another check which has proven to be an effective indicator of potential risk is that of monitoring an *employee lifestyle changes* and instances of seemingly *unexplained wealth.*

All of the checks outlined can be used for the initial recruitment and/or a part of regular performance monitoring - as circumstances may change during the employment period.

- *An Oath or Pledge of employment*

In some motor vehicle administrations, when an employee is hired they are required to *swear an oath*. However, it does not appear that this practice is renewed or ever referenced except if the employee becomes involved in fraudulent activity and disciplinary action is being considered. In other cases, this "oath" is not always applied in all employment situations. An example would be the case of a contract or temporary employee versus permanent staff. Typically, the temporary employee or contractor is not required to participate in the "oath" process. Nevertheless, the practice of an "oath" is a very positive action that begins to communicate to a new employee the expectations and values of the organization. This is a practice that can be easily enhanced to ensure that the full message is communicated and that the employee fully understands the consequences of inappropriate actions.

- *Employee Training*

The benefits of thorough employee training in minimizing fraud have been well documented. Specifically, the work being done on Fraudulent Documentation Recognition Training (FDRT) underscores the importance of having well trained employees. Such training would supplement other business process training that an employee should receive upon initial employment and on a periodic basis to refresh and update learning. It is also during these training opportunities that the organization values/ethics are reinforced and refreshed.

The use of formal documented policies and procedures are also a good measure to ensure employees are knowledgeable of the business process. In some cases, jurisdictions have built in details of their internal controls into policy and procedure manuals. A further example is that of a jurisdiction that has created brochures that outline to employees that

internal controls are in place within departments and the role of the employee is ensuring adherence to those controls.

- *Anonymous tips – "snitch line"*

Another control that compliments some of the previous best practices would be to create an environment where employees feel safe to "inform" management if they become aware of fraudulent activities on the part of fellow employees. *Snitch lines* allow information to be collected anonymously. As with any sort of anonymous arrangement, the appropriate due diligence must be applied to any information received and the appropriate follow-up conducted.

Some jurisdictions have formalized the "snitch" approach by having in place legislation that would indeed protect the "whistleblower".

- *Mandatory consecutive leave on an annual basis*

This practice is viewed by one of the organizations interviewed as a useful practice to create a break in the work flow of an employee. It is typically during such breaks that irregularities in practices become evident.

Auditing and Information Technology

Because auditing and information technology can be very closely linked, these two aspects of internal control have been combined into one section.

Why is auditing important for internal control?

Auditing may well be the most important aspect of internal control, and effective auditing is multi-layered. Having a *formal audit plan*, which would need to be multi-layered, serves as a deterrent at the same time it is an essential part of detective and investigative controls measures. Using audits is a way to be proactive in the approach to internal fraud – instead of waiting for the problem to present itself, a jurisdiction can take measures to identify fraud early. A critical aspect of any audit program is to ensure that the persons conducting the audits must not have a role in the process that they are auditing. Without this objectivity the audit process would be suspect.

Why is information technology important for internal control?

Information technology is important because it enables the capture of more information in a more rationalized systematic manner as well as removes the human element from parts of the audit process. Computerized random audits, controls, and reports are a natural progression of the already massive databases and systems in use. Using computer systems to generate reports and transaction controls is faster, easier, and less apt to be manipulated than human auditing and reporting.

- **Audit**

In a survey of jurisdictions, most noted that their *auditing is done in-house*. However, there are also jurisdictions that use *third parties* to either enhance or replace the in-house auditing procedures. Many jurisdictions that use in-house auditors do so with the belief that having dedicated agency resources is the best way to ensure that internal fraud does not occur. The jurisdictions using third party auditing believe that having impartial auditors lessens the chance of internal fraud occurring. The argument can be strong in both cases; however, the techniques used in either scenario should be the same.

- *On-site auditing*

This technique is used by a majority of jurisdictions, whether those auditors are motor vehicle administration employees or third party auditors. Several jurisdictions have formal auditing procedures in place that involve checklists and reporting. Based upon both polling of jurisdictional motor vehicle agencies and outside auditing agencies, the following is a list of items that should be included in an audit checklist, depending on each jurisdiction's procedures:

  - Are customers immediately assigned another test appointment after failing the initial test? Is the customer's record (or relevant report) updated immediately with the failure and new appointment?
  - Are the tests (automated and manual) updated or changed between customers?
  - Is each customer's documentation verified according to procedure/policy?
  - Is the office supervisor called upon to review questionable documentation?
  - Do each employee's drawer/cash counts match the transaction/fee report daily?
  - Are there random audits of cash drawers at least once a week, at a time other than when the drawers are normally counted?
  - Are all overages/shortages of the cash drawer counts documented?
  - Is there a pattern of overages/shortages of cash?
  - Are cash drawers locked when not in use?
  - Are there an unusually high number of canceled transactions?
  - Is a supervisor called upon to approve a canceled transaction before a new one is started?
  - Have all station computers been checked for unauthorized use?
  - Are all employees signing in using their own login ID and password?
  - Has an employee signed on to more than one station computer?
  - Are there any non-business related e-mails being sent?
  - Are there any non-business phone calls being made?
  - Has a daily inventory of supplies been conducted? Are the inventory counts correct?
  - Are there any patterns of incorrect inventory counts?

- Are security items placed in appropriately locked areas or safeguarded properly?
- Is system ID/passwords securely maintained?

These are just a few of the items that should be included in any auditor's checklist. Though random on-site audits generally focus on much more than internal fraud, the audits should be expanded to look for, at the least, the basic signs of employee fraud and not just procedural errors.

- **Audit Techniques**

Another method of auditing is to rank the risks by motor vehicle office or by transaction. If there are an unusually high number of people obtaining DLs at a more remote office in your jurisdiction, or if there are a high number of canceled transactions in another office, those offices should be placed higher on an auditing priority list, and should be audited more frequently. Random audits tend to be far more effective than announced audits, for obvious reasons, and would be very effective if given more often at potentially problematic sites.

On-site audits should also include random transaction/batch audits. Auditors should look at records for several transaction types over a few days. If an auditor notices that there is a spike in the number of cancellations, duplicates, etc. given at a particular station, further investigation may be warranted. The more often this technique can be used, the better, as it is far more proactive than waiting for suspicious activity to be reported.

- *Random Computer Audits*

Random computer audits are another effective method of auditing. This technique really illustrates how information technology can be particularly useful. This method can be used to audit the identification documents accepted by employees. The system could randomly select a transaction for audit by "freezing" the transaction until a supervisor can enter his or her password and/or user ID to clear the transaction again. The supervisor must check the documents the employee has accepted and verify the transaction before allowing the employee to continue. This method is most effective when the employee is prevented from conducting any transactions or signing on to another computer until the supervisor has cleared the current audited transaction.

- *Exception Reports*

Exception reports are a key tool used by any audit function. These reports should be generated whenever a transaction or procedure is not completed the way it was designed. For example, certain data must be entered but is overridden and the transaction is processed. These exceptions should be "reported". Such reports are best investigated by a unit other that the one that processed the transaction, preferably at a location removed from the site of the processed transaction.

- *Database mining/auditing*

A particularly effective auditing method that can be done off-site is data mining, or database auditing. This also brings the benefits of information technology to the table. Jurisdictions can search the transaction/inventory databases for anomalistic trends. Not only can transactions be randomly audited, but document inventories and fiscal inventories can be audited as well. Another benefit of this method is that it does not require a team of auditors to visit the branches on-site, but the auditors should be used to visit the branch only if problems are found.

- *Audit Plan*

While there are a number of auditing techniques which are effective, the most effective thing a jurisdiction should do is have an *audit plan*. Any auditing technique is ineffectual if it is not written down and followed. It is understood that there are moments when intervening priorities prevail, but the audit plan should always be adhered to when the crisis ends. It is also understood that each audit plan may be very different. Though procedures and risks vary a great deal between jurisdictions, the core business processes in the case of motor vehicle agencies remain similar.

The most important part of any audit plan is to write it down and follow it – being proactive works far better in preventing internal fraud than reacting later.

See Appendix 1 for further details regarding an audit plan.

- **Information Technology**

- *Passwords/IDs*

As briefly covered in the auditing information, using information technology is a highly effective internal control. Though it seems basic to assign an ID and password to each employee, the problem of maintenance and "sharing" arises. IDs and passwords invariably become common knowledge among staff in a particular location as they are often shared in an effort to keep customers moving quickly. It cannot be emphasized enough that those IDs and passwords should be kept confidential, as it eliminates the effectiveness of any auditing report techniques. It is also true that someone must maintain that list (should an employee forget an ID or password or an employee leave the motor vehicle agency) and the problem of security then arises. The ID and password list itself can potentially become a tool for internal fraud should that list be stolen or accessed. Rather than keep a written list of the information, IDs and passwords could be maintained on a secure site or separate database, with only authorized supervisors having access. Maintaining this list at a central site or office may be too cumbersome, as any problem with passwords could not be taken care of immediately and would have to wait for someone at another location for assistance.

- *Limited system access controls*

Some jurisdictions noted in their survey responses that certain employees must have access to a central data center in order to produce a document. This is particularly effective in controlling access to certain information. In order for the final document to be produced, a supervisor or someone with the data key must approve it.

Jurisdictions can also assign levels of access to each employee. In this scenario, each employee's ID and password would gain them access to information or screens that are relevant only to their specific program area.

- *Transaction controls*

Not only can computer systems/software be used to randomly audit a transaction, but systems can be used for transaction control as well. Controls can be put in place that will require an employee to "check off" on their screen which documents were presented to them in order to complete a transaction. If a certain pre-determined list or point system is not met based on the documents entered, the transaction cannot move forward. A control can also be put in place that would automatically stop a transaction if certain types of documents are being used together. This cuts down on mistakes as well as intentional fraud. Again, a supervisor would have to enter his or her ID and/or password in order to continue the transaction in these situations.

Information technology is a major source of assistance to the jurisdictions when it comes to internal control. As stated earlier, using computer systems to generate audit trails/reports, for transaction control, and for random transaction audits is a highly effective way discover internal fraud very early in the process. While use of these techniques would vary based upon the procedures in each jurisdiction, it is recommended that with any effective audit plan should come some information technology controls. Because the use of information technology is so varied within each jurisdiction, it is up to each jurisdiction's discretion what information technology controls are best applied within their own environment.

Business Process:

There are six key components of the DL/ID processes that are generic to any process that accepts/enrolls applicants for a fee and then issues some sort of credential.

- Application/Entry
- Verification
- Qualification/Testing
- Credential Issuance
- Record Management
- Revenue Collection

There are two best practices within the DL/ID business process, which are applicable across the six components and their associated risk areas.

1. *Two person transaction processing:*

The use of a two-person process for verification and validation of the completeness/appropriateness of an activity within a transaction is seen as the ultimate best practice. It is considered more difficult to compromise two or more people than it is one. However, it is not always practical or financially feasible to have two or more people handling a transaction when the volume of transactions handled daily by motor vehicle administrations is considered. There may be opportunities to utilize the two-person process as a way to minimize risk exposure in some key areas within the process.

2. *Surveillance cameras in the workplace*

Using surveillance cameras in the workplace can be viewed as an effective control measure. Although there maybe some negative reaction to their use, there is also a growing acceptance, particularly in situations where there is direct public interaction. In some cases, where cameras were installed as a security measure for the public workspace to deter robberies etc., cameras have had positive benefits with employee actions behind the counter as the employees can also be captured in the camera's coverage.

Business Process Components:

For DL/ID issuance purposes, the specific business requirements within the six components are as follows:

1. **Application/Entry** – the start of the process where an applicant arrives at the office presenting the necessary documentation. In most cases this requires the clerk to input certain information into a computer system.

2. **Verification** – an integral part of the Application/Entry process is the verification of the information/documents provided by the applicant. This would involve a physical check of documents submitted as well as automated verification – (e.g. PDPS, SSA, IRE, SSOLV, etc.)

3. **Qualification/Testing (DL issuance process only)** – the point at which the applicant has met the requirements of application and verification and is now ready to attempt the qualification requirements.

4. **Issuance** – once the applicant has met the testing requirements and the appropriate fees collected. This may include issuance of either a permanent or temporary credential document.

5. **Records Management** – ensures the ongoing integrity of the driver licensing and control record.

6. **Revenue Collection** – the applicant pays for the product or service provided.

Because these are complex processes with inherent risk exposure, a more detailed analysis of each specific component was undertaken to identify the particular risk areas and the appropriate measure(s) that, if implement would mitigate the risk.

This analysis is outlined in **Appendix 2**