Access Governance: Flexibility with Escalation and Audit

Xia Zhao
Bryan School of Business and Economics
The University of North Carolina at Greensboro
x_zhao3@uncg.edu

M. Eric Johnson
Center for Digital Strategies
Tuck School of Business at Dartmouth
m.eric.johnson@dartmouth.edu

Abstract
Managing information access in highly dynamic business environments is increasingly challenging. With thousands of employees accessing thousands of applications and data sources, managers strive to ensure the employees can access the information they need to create value while protecting information from misuse. We propose an access governance structure with escalation options, ensuring both flexibility and security of information. Using a game-theoretic approach, we show that properly coupling information access, audit, violation penalties and rewards can enable self-interested employees to access information in a timely manner, seizing business opportunities for the firm while managing security risks. Surprisingly we find that providing employees with more access than strictly required can reduce control costs and improve profits.

1. Introduction
Pervasive and timely access to information is a source of competitive advantage for many firms such as investment banks, research laboratories, and hospitals. Technology has made information more available throughout and between organizations, enabling collaboration and fueling innovation. The literature on innovation has long discussed the benefits of free-flowing information, linking it to innovation productivity (e.g., Baker and Freeland 1972; Tsai, 2001; von Hippel 1994). Likewise, the services and supply chain literature have also extolled the benefits of increased information availability (e.g., Lee et al. 2000; Rathnam et al. 1995). With web-based tools linked to vast enterprise data sources, firms today have made much data and applications readily available to thousands of employees, business partners, and customers at very low cost. Thus, in environments where information can result in significant profits or is critical to outcome quality, firms are driven to invest in technologies that increase information availability.

Unfettered information access, however, can create significant security concerns, driving managers to constrain the availability of information. Such efforts have become indispensable with the recent enforcement of many government regulations, such as Sarbanes-Oxley (SOX), Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), Personal Information Protection and Electronic Documents Act (PIPEDA), and the European Union Directive on Data Privacy (EU Directive), which all include language requiring firms to maintain some level of access control. Driven by fears of data breaches, intellectual property losses, and compliance violations, firms are working to reduce information accesses through better controls and governance. Therefore, the role of access governance has become increasingly important in balancing security and availability.

Current practice of access governance focuses on the technical implementation of access management through privileges and entitlement1 coupled with auditing to detect misuse. For example, access controls dictate user privileges to view a file, execute an application, share data with other agents, and so on. Users can only use data when they have the corresponding entitlements. The key focus of this approach is to prevent misuse of data—either intentionally (such as using the data to make illegal stock trades) or unintentional (such as storing the data on device that is vulnerable to a security breach). One important criterion of access management is known as “the rule of least privilege”, i.e., each user is provided with the minimum entitlements needed to perform her/his task (Aveksa 2007). To enforce the rule of least privilege, an access control system must be customized and dynamically managed including five

1 An entitlement is a resource that a person is authorized to access in a certain way; for example, “opening case files” might be an entitlement for application X. In practice, entitlement, privilege and access permission are used interchangeably.
components—request, approve, administer, enforce and monitor. Specifically, a user requests an entitlement; the owner (typically the business owner of the data) examines the request and then approves or rejects it; the administrator modifies the user’s entitlements; the user accesses the resource and the system logs the user’s activities; and the auditor examines the logs and evaluates users’ activities. Figure 1 shows the access management system with the rule of least privilege.

To enforce the rule of least privilege, employees’ accesses must be continually updated and audited to remain in synchronization with the changing organization. In large organizations with thousands of users interacting with thousands of different applications and data sources, each having many levels of privilege, the assignment and maintenance of user access are daunting. The rule of least access is also limiting in many situations where it is difficult to foresee all information needs in advance. For example, in a hospital setting, emergencies arise where attending physicians may find themselves caring for another doctor’s patient. In the increasingly dynamic environment, organizations frequently face unanticipated situations and have to adjust their organizational structures and personnel to adapt the consumers’ needs. Rigid access control delays an organization’s response to the changing markets, resulting in missed opportunities or degraded service quality.

Figure 1. Access Management System with the Rule of Least Privilege

In current practice, flexibility of access governance is sometimes achieved by overentitlement. In a field study of an investment bank, we found that 50-90% of employees were overentitled (Sinclair et al. 2008). This outcome is rationalized by the argument that long-term employees are valuable and need quick access to information to create value for the firm. But employees that are permanently overentitled represent a large security risk to the organization because their accesses could be used maliciously or accidentally. While the malicious insiders make the headlines (Jolly 2008), in many cases, benign overentitled employees pose a much larger risk to themselves and the organization because of secondary vulnerabilities like the loss of a laptop with sensitive data or because a malicious hacker could gain access to substantial firm information through a single overentitled account.

In an increasingly dynamic world, information governance must be flexible, yet secure. In this paper, we define access governance as an integrated system including policies, controls, incentives, and processes that manage user access to information resources. The goal of such access governance is to ensure that information systems deliver the right information to the right people at the right time, while protecting the information from misuse.

To achieve flexibility, we consider a different approach where employees are allowed to escalate into controlled data and applications when needed. This allows one-time access without any time-delaying approval process. In fact, we have witnessed cases where escalation is used to solve a failure of traditional access control systems. For example, the investment banking sector refers to such an approach as “override” (Rissanen et al. 2004), and the health care sector refers to it as “break glass” (Ferreira et al. 2006). Escalation potentially breeds significant security risks since employees may abuse their ability to access information. For example, accessing information for personal benefit rather than for business need. To mitigate the associated security risks, the escalation activities are later audited, and employees found to be abusing their accesses are penalized. Auditing (or monitoring) access with violation penalties have been implemented by firms seeking to drive desired behavior from employees or partners with respect to financial reporting, contract and regulation compliance. For example, Intel issues “speeding tickets” to employees that violate information security policies (Johnson and Goetz 2007). In addition to penalties, we also consider the possibility that the firm uses rewards to motivate employees.

In this paper, we design an access governance policy with escalation options which couples escalation accesses with rewards, audit and violation penalties. We use a game-theoretic model to analyze the employees’ incentives and the firm’s policy design problem. The results show that a properly designed governance policy could provide the desired access flexibility with a significant level of control. Figure 2 shows the information governance system with escalation.
Of course, escalation must be confined to cases where the risk of failure or the cost of recovery is relatively low compared to the cost of not granting access (e.g., the potential value created through escalation). It may not be suitable for some financial or trading systems where there is significant risk of massive fraud. Rather it is useful in cases where there are small risks or where the potential value of business opportunities is high. For example, escalation is very effective in situations where emergency access may save someone’s life, or in a time-critical system where the person with the necessary privileges may be unavailable (Povey 2000).

The paper is organized as follows. In Section 2, we review the related literature. In Section 3 and Section 4, we outline the model and analyze the game. We capture the important characteristics of the optimal access governance policy with escalation options. Finally we conclude with implementation guidance in Section 5.

2. Related Literature

The technological aspect of implementing escalation in access control has been studied in computer science literature. Povey (2000) broadly discussed an optimistic access control scheme with escalation and developed a formal model to ensure the integrity of computer systems including accountability, auditability and recoverability. Rissanen et al. (2004) emphasized the importance of audit and manual recovery in providing overriding of access control. Ferreira et al. (2006) described the design and initial implementation of a “Break-The-Glass” policy in a virtual Electronic Medical Record system. Different from these papers that focus on the technology of implementing escalation, our paper focuses on the economic aspect of the access governance with escalation and uses a principal and agent setting to study the policy design problem.

Principle and agent models have been examined in a variety of contexts (e.g. Antle and Eppen 1985; Arrow 1985; Baiman 1990; Harris and Raviv 1979; Harris et al. 1982; Holmstrom 1979; Shavell 1979, etc.). Our paper closely relates to a large stream of literature that studies the audit policy in the principal and agent framework (Baron and Besanko 1984; Dye 1986; Harris and Raviv 1996; Kim and Suh 1992; Townsend 1979). Townsend (1979) was one of the first models to examine the costly verification. Dye (1986) showed that optimal monitoring policies are deterministic and lower-tailed. Kim and Suh (1992) also focused on the deterministic monitoring policy in which the optimal investment in audit technology is endogenously determined. They found the lower-tailed policy is one of the special cases. Baron (1984) investigated the random audit policy in a regulatory pricing problem. Firms are privately informed about their cost functions and required to report them to the regulator. Baron (1984) found that the optimal audit policy includes the possibility that firms may be penalized, even though they report their best knowledge, because of ex post uncertainty. And Harris and Raviv (1996) explored the random audit policy in the capital budgeting process and identified cases of overinvestment as well as underinvestment. We use the principle and agent framework in a novel context to better understand the value of escalation. In addition to audit with violation penalties, we also consider positive incentives. We show that an information governance policy that properly couples access, audit, violation penalties and rewards will help firms achieve a significant level of flexibility while balancing against security risks.

3. Model

We consider the case where users gain access to data and applications through a system employing access control. We focus on the firm’s optimal strategy in cases where there are only a few, discrete situations where employees may need more access—for example, when opportunities arise that require quick action or when their supervisor (who has greater access) is not available. In those situations, firms may allow employees to escalate access but then audit their actions (at a cost) afterward and penalize employees for misuse or reward for value generation.

We model the collection of applications and data as measured on a continuous scale of information, with each privilege weighted to reflect the amount and sensitivity of the data. Based on value generated by an employee and the associated information risk, the firm assigns the employee a regular access level to perform routine tasks.

Periodically, employees may face an opportunity to create more value by accessing information beyond her/his regular access. We assume that with probability
π∗ (or π∗), an employee will observe such an opportunity with high (or low) revenue potential; with probability π∗ = 1 − π∗, s/he does not observe any opportunity. We refer to these situations as the high state, denoted as θi, low state θj and regular state θh. We assume θi > θj > θh = 0. We use a to denote the access level. The firm allows employees to escalate their access levels temporarily to seize business opportunities. The net revenue from a business opportunity is determined by θ′(i = 0, l, h) and the employee’s escalated access level a, i.e., U(θ, a).

Access control, while providing a measure of security, restricts employees’ flexibility to monetize the business opportunities. Therefore the more access rights an employee has, the more likely that s/he creates value for the firm. We assume that U(θ, a) is an increasing and concave function of a (U′ > 0 and U′′ ≤ 0). This is a reasonable assumption as increased availability of information can increase revenue generating potential, but is eventually limited by the skill and knowledge of the employee. The impact of flexibility on firm revenue is more significant when the firm observes a higher revenue potential than when it observes a lower revenue potential. Therefore, we assume that the marginal revenue of the information access in a higher state is larger than that in a lower state, U′′ > 0. Figure 3 shows an example of the firm’s revenue functions from emergent opportunities in three states.

Figure 3. Firm’s Revenue Functions in Three States

The firm bears costs associated with the escalation access level of C(a) including additional security risks and routine technical support required to prudently maintain that access. C(a) is an increasing and convex function (C′ > 0 and C′′ > 0). This well-models the case where providing far too much access can eventually result in severe consequences (risks and cost to mitigate risk). To mitigate risk of unnecessary escalation, the firm controls the escalation flexibility and audits each instance of escalation. In particular, the firm offers three escalation options, {a0, a1, a2}, corresponding to the states {θ0, θ1, θ2} and motivates employees to choose the escalation access level a when the state θi arises.

Employees derive some private benefit by accessing information and data and prefer higher access levels to lower ones. Such “snooping” value is not uncommon—we have witnessed cases in health care where care providers have examined patient records for their own benefit (Grad 2008). The employee’s private benefit from escalation is u(a). u(a) is an increasing and concave function. u′ > 0 and u′′ ≤ 0. Since some employees may take advantage of the flexibility and not choose the right escalation options (choosing a, in the state θj, j ≠ i), the firm audits the instances of escalation at a cost and penalizes the escalation misuse. It is assumed that the firm can detect misuse with probability p by investing D(p) in the audit capability. The audit spending includes hiring auditors, tracking escalation instances, and verifying the business opportunities by communicating with the manager or coworkers of the employees. We refer to p as the audit precision. D(p) is an increasing and convex function (D′ > 0 and D′′ > 0). The employee will be penalized at the level of F if s/he is detected to misrepresent the state that s/he observes. We assume that the maximal violation penalty is F. Without loss of generality, we assume that if an employee choice is consistent with the state (choosing a, in the state θi), the probability of finding a violation is 0, i.e., p = 0. In addition to audit and penalties, the firm may reward employees for choosing the right escalation options. w denotes the reward for escalation option i. The audit precision, violation penalty and reward can be contingent on employees’ choices (as in related work on contingent contracts in which penalty or reward is contingent on the audit outcome, e.g., Chen, Xu and Whinston 2009).

The firm maximizes its expected profit by designing an access governance policy with escalation options \( \{a_0, a_1, a_2, p, w, F\} \). By the revelation principle, we restrict attention to direct revelation mechanisms. We focus on constructing a policy that motivates employees to reveal their true observations.

The sequence of events is showed in Figure 4. We use one employee as an example. At stage 1, the firm announces its access governance policy with escalation options; At stage 2, an employee observes the state and then chooses an escalation option; Finally, the firm audits the escalation instance, rewarding or penalizing...
the employee according to the announced access governance policy.

Firm determines \( \{a, w_i, p,F_i\}; i = 0, l, h \)

\( \theta \) is realized and employee chooses escalation option

Firm rewards and penalizes employee

Figure 4. The Sequence of Events

The employee's expected payoff, denoted by \( \Pi_{employee} \), can be represented by

\[
\Pi_{employee} = \begin{cases} 
  w_i + u(a_i) & \text{if s/he chooses } a_i \\
  -p_i F_i + (1-p) w_i + u(a_i) & \text{if s/he chooses } a_i
\end{cases}
\]

when \( \theta = \theta_i \)

where \( i, j = 0, l, h \). The firm’s expected profit is \( E \left[ U(\theta, a) - C(a_i) - D(p) - w_i \right] \). Note that with a deterministic relationship between the firm’s profit, revenue potential and access level, it is possible to deduce employee misuse from the value created by an escalation instance. However, such an approach is impractical since the firm typically learns the value created by an employee after a significant period of time, opening the door to significant security risks. Timely audit is a security must. Let \( \Pi_{firm} \) be the maximum expected profit obtained by the following optimization problem. We do not allow the firm to profit from penalizing \( (F) \) the employee. Penalties could take many forms including nonmonetary such as required remedial training or firing the employee.

\[
\Pi_{firm} = \max_{a, w_i, p, F_i} E \left[ U(\theta, a_i) - C(a_i) - D(p) - w_i \right]
\]

s.t. \( w + u(a) \geq -p_i F_i + (1-p) w_i + u(a), j \neq i \) if \( \theta = \theta_i (IC) \)

\[
\begin{align*}
  w_i & \geq 0, a_i \geq 0, 0 \leq p_i \leq 1, 0 \leq F_i \leq \bar{F}, i = 0, l, h \\
\end{align*}
\]

(IR)

where (IC) are the employee’s incentive constraints and (IR) are the employee’s individual rationality constraints.

To gain managerial insight, we analyze the following (tractable) functional forms. We assume that the firm’s revenue function is linear, \( U(\theta, a_i) = \theta a_i \), \( i = 0, l, h \) where \( \theta_i \) represents the firm’s marginal revenue of information access. The employee’s private benefit function is also linear, \( u(a_i) = ba_i \) where \( b \) is the employee’s marginal private benefit of information access. The assumption of linear revenue and private benefit functions does not result in any loss of generality because the firm can always redefine the map between the collection of applications and data and the continuous scale of information, and transform the relationship between the benefit and information access to a linear one. We assume the cost functions are quadratic, \( C(a) = \frac{1}{2}sa_i^2, s > 0 \). Besides the frequent use of convex cost functions in the literature (e.g., Kannan and Telang 2005; Krishnan and Zhu 2006; Motta 1993), quadratic cost functions nicely capture the higher security risks associated with higher access as well as the cost of additional IT resources for maintaining access. Similarly, the audit cost function is \( D(p) = \frac{1}{2}tp^2, t > 0 \), which reflects the increasing difficulty of improving the audit precision.

4. Analysis and Results

4.1 Benchmark Case

We first consider a benchmark case where there is no information asymmetry between the firm and employees. The firm can directly observe the states (i.e. an opportunity with high revenue potential, an opportunity with low revenue potential, or no business opportunity) and assign the access levels to employees. In this case the firm does not need to implement any incentive scheme (neither reward nor penalty). The firm’s optimization problem can be represented by

\[
\Pi_{\text{optimal}} = \max_{a, i, j = 0, l, h} E \left[ \theta a_i - \frac{1}{2}sa_i^2 \right]
\]

The optimal access level is given by \( a_i^* = \frac{1}{2}\theta_i (i = 0, l, h) \). When the firm observes a business opportunity with high revenue potential, it will assign \( \frac{1}{2}\theta_i \) to the employee; when it observes an opportunity with low revenue potential, it will assign \( \frac{1}{2}\theta_i \) to the employee; otherwise, it will not assign any additional access to the employee. The firm’s optimal profit is

\[
\Pi_{\text{optimal}} = \frac{1}{2}\left( \pi_s \theta_i^2 + \pi_i \theta_i^2 \right).
\]

4.2 Asymmetric Information

When there is information asymmetry between the firm and employees (firms can not directly observe employees’ opportunities), the firm will design the escalation options in a way that the employee will choose the right option in each state, i.e. the employee will choose \( a_i \) if the state is \( \theta_i \). Therefore, the employee’s incentive constraints are as follows.

High state:

\[
\begin{align*}
  w_i + ba_i & \geq -p_i F_i + (1-p) w_i + ba_i \quad (IC - HL) \\
  w_i + ba_i & \geq -p_i F_i + (1-p) w_i + ba_i \quad (IC - H 0)
\end{align*}
\]

Proceedings of the 43rd Hawaii International Conference on System Sciences - 2010

5
Low state:
\[
\begin{align*}
    w_i + ba_i & \geq -p_h F_h + (1 - p_h) w_h + ba_h & (IC - LH) \\
    w_i + ba_i & \geq -p_h F_h + (1 - p_h) w_h + ba_h & (IC - L0)
\end{align*}
\]

Regular state:
\[
\begin{align*}
    w_i + ba_i & \geq -p_h F_h + (1 - p_h) w_h + ba_h & (IC - LH) \\
    w_i + ba_i & \geq -p_h F_h + (1 - p_h) w_h + ba_h & (IC - L0)
\end{align*}
\]

The first (or second) group of incentive constraints is for employees who observe business opportunities with high (or low) revenue potential. The third group of incentive constraints is for employees who do not observe any business opportunity. Presumably, if employees do not observe any business opportunity, the firm should discourage escalation, i.e. \(a_g = 0\). We do not impose this constraint (allowing for the possibility of a solution with higher profit).

Properly designed escalation options will induce employees to choose the right escalation levels and hence disclose their observations. We focus on the case where \(p_h = 0\). That is, if an employee chooses the option \(a_g\) and s/he claims that s/he does not observe any business opportunity, the firm does not audit such instances. Given that escalation is used to handle unusual situations, it is reasonable that the firm does not investigate the regular states. We can substitute \(p_h = 0\) into (IC-H0) and (IC-L0) and obtain the following inequalities.
\[
\begin{align*}
    w_s + ba_s & \geq w_0 + ba_0 & (IC - H0) \\
    w_i + ba_i & \geq w_0 + ba_0 & (IC - L0)
\end{align*}
\]

It is easy to find that (IC-HL), (IC-LH) and (IR) are not binding. For example (IC-HL) is implied by (IC-H0) and (IC-OL). The firm’s optimization problem can be simplified as

\[
\Pi_{\text{firm}} = \max_{a_i, a_g, p_h} \pi_s \left( \theta_s a_s - \frac{1}{2} \sigma_l^2 - \frac{1}{2} \eta^2 - w_s \right)
\]

\[
\pi_l \left( \theta_l a_l - \frac{1}{2} \sigma_l^2 - \frac{1}{2} \eta^2 - w_l \right) + \pi_u \left( \frac{1}{2} \sigma_u^2 - w_u \right)
\]

\[
(1): \text{s.t.} \quad w_s + ba_s - w_0 - ba_0 \geq 0 & (IC-H0) \\
    w_i + ba_i - w_0 - ba_0 \geq 0 & (IC-L0) \\
    w_s + ba_s + p_h F_h - (1 - p_h) w_h - ba_h \geq 0 & (IC-0H) \\
    w_i + ba_i + p_i F_i - (1 - p_i) w_i - ba_i \geq 0 & (IC-0L) \\
    w_h, w_i, w_s, a_s, a_i, a_g \geq 0 \\
    0 \leq p_i, p_h \leq 1, 0 \leq F_i, F_h \leq \bar{F}
\]

**Proposition 1:** If the firm detects that an employee misrepresents her/his observation, the firm will penalize her/him to the maximal level. i.e., \(F_h = F_i = \bar{F}\). (See Appendix for all proofs.)

The audit and associated violation penalties deter employees from misrepresenting the business opportunities they observe. Since the firm does not incur any cost by penalizing employees after it detects misuse, it always penalizes them to the maximal level to reduce the audit spending. Proposition 2 characterizes the escalation options when the penalty can be extremely harsh, i.e. \(\bar{F} \rightarrow \infty\).

**Proposition 2:** If \(\bar{F}\) approaches infinity, the firm only offers two options, \(\{ (a_i, w_i, p_i, \bar{F}) | i = l, h \} \). In particular, \(a_i = \frac{1}{2} \theta_i\), \(a_g = \frac{1}{2} \theta_i\), \(w_i = w_s = 0\), \(p_i = p_h = \epsilon \rightarrow 0\). And the firm can achieve the optimal profit, \(\frac{1}{2} (\pi_i \theta_i^2 + \pi_u \theta_i^2)\).

If the firm can render extreme penalties for detected misuse, employees have no incentive to misrepresent their observations even though there is only a slight chance of being detected. The firm can design the escalation options with a very low probability of detection and no reward.

However, an infinite penalty is impossible to implement, e.g., the firm cannot take an employee’s life. Next we consider the situation where there is an upper bound for the penalty. To avoid trivial cases where the firm assigns the same access levels for business opportunities with different revenue potentials, we assume that the difference between \(\theta_l\) and \(\theta_i\) is greater than \(\frac{1}{2} \epsilon\), i.e. \(b < \pi_u (\theta_i - \theta_l)\) and \(\theta_i > b\). The assumption ensures that the access level for the business opportunity with higher revenue potential is higher than that with low revenue potential, i.e. \(a_s > a_i\). In addition, we assume that the audit is so

---

2 In practice, periodical entitlement reviews may be conducted to examine employees’ regular access rights and ensure that they have the adequate access rights to accomplish their tasks.
costly that it is not always optimal for the firm to invest to achieve audit precision of $p = 1$.

The optimal solutions of the optimization problem (1) are \:\{ (a_i, w_i, p_i, F_i) \mid i = 0, 1, b \} where

1) when $F^2 \leq \frac{\theta_\theta}{\pi_\theta \pi_\theta} (\pi_\theta + \pi_\theta b - b)$, Case I1;

2) when $\frac{\pi_\theta}{\pi_\theta} (\pi_\theta + \pi_\theta b - b) - F^2 \leq \frac{\theta_\theta}{\pi_\theta \pi_\theta} (\pi_\theta + \pi_\theta b - b)$, Case B1;

3) when $\frac{\theta_\theta}{\pi_\theta \pi_\theta} (\pi_\theta + \pi_\theta b - b) - F^2 \leq \frac{\theta_\theta}{\pi_\theta \pi_\theta} (\pi_\theta + \pi_\theta b - b)$, Case I2;

4) when $F^2 = \frac{\theta_\theta}{\pi_\theta \pi_\theta} (\pi_\theta + \pi_\theta b - b)$, Case B2.

Case I1: $a_i = \frac{1}{2} (\theta - \frac{\pi_\theta + \pi_\theta}{\pi_\theta} b)$, $a_i = \frac{1}{2} (b + \theta)$, $a_i = \frac{1}{2}$,

$p_i = \frac{1}{\pi_\theta} F$, $p_i = \frac{1}{\pi_\theta} F$, $F_i = F$, $F_i = F$, $F_i = F$, $F_i = F$,

$w_i = 0$, $w_i = 0$, $w_i = 0$, $w_i = 0$.

Case B1: $a_i = \frac{1}{2} (\theta - \frac{\pi_\theta + \pi_\theta}{\pi_\theta} b)$, $a_i = \frac{1}{2}$.

$p_i = \frac{1}{\pi_\theta} F$, $p_i = \frac{1}{\pi_\theta} F$, $F_i = F$, $F_i = F$, $F_i = F$,

$w_i = 0$, $w_i = 0$, $w_i = 0$, $w_i = 0$.

Case I2: $a_i = \frac{1}{2} (\theta - \frac{\pi_\theta + \pi_\theta}{\pi_\theta} b)$, $a_i = \frac{1}{2}$.

$p_i = \frac{1}{\pi_\theta} F$, $p_i = \frac{1}{\pi_\theta} F$, $F_i = F$, $F_i = F$, $F_i = F$,

$w_i = 0$, $w_i = 0$, $w_i = 0$, $w_i = 0$.

Case B2: $a_i = \frac{1}{2} (\theta - \frac{\pi_\theta + \pi_\theta}{\pi_\theta} b)$, $a_i = \frac{1}{2}$.

$p_i = \frac{1}{\pi_\theta} F$, $p_i = \frac{1}{\pi_\theta} F$, $F_i = F$, $F_i = F$, $F_i = F$,

$w_i = 0$, $w_i = 0$, $w_i = 0$, $w_i = 0$.

Proposition 3 characterizes the set of escalation options.

Proposition 3: When $b < \pi_\theta (\theta - \theta)$ and $\theta > b$, (1) Information access: the firm gives higher information access if the business opportunities have higher revenue potential. In addition, the access level for the business opportunity with high revenue potential is always lower than the optimal level in the benchmark case (underentitlement): The access level for the low revenue potential is higher than or equal to the optimal one (overentitlement) when $F^2 \leq \frac{\theta_\theta}{\pi_\theta \pi_\theta} (\pi_\theta + \pi_\theta b - b)$ (case I1 and B1) but lower than the optimal one (underentitlement) otherwise (case I2 and B2): The access level for no business opportunity is always higher than the optimal one (overentitlement).

2) Audit: the firm audits the escalation instances with higher precision if the employees choose a higher escalation level than it does if the employees choose a lower escalation level. In addition, the firm always audits the escalation instances associated with $a_i$ audit those associated with $a_i$ only when $F^2 > \frac{\theta_\theta}{\pi_\theta \pi_\theta} (\pi_\theta + \pi_\theta b - b)$.

3) Reward: The firm rewards more for employees who choose the lower access level. In addition, the firm rewards employees for escalation instances associated with $a_i$ only when $F^2 \leq \frac{\theta_\theta}{\pi_\theta \pi_\theta} (\pi_\theta + \pi_\theta b - b)$, for escalation instances associated with $a_i$ only when $F^2 > \frac{\theta_\theta}{\pi_\theta \pi_\theta} (\pi_\theta + \pi_\theta b - b)$, but never rewards the escalation instances associated with $a_i$.

The optimal escalation options present separating equilibria in which employees choose different escalation levels in different states.

The access levels in the asymmetric information case deviate from the optimal ones in the benchmark case ($a_i < a_i$, $a_i > a_i$, $a_i > a_i$, $a_i > a_i$) if $F^2 \leq \frac{\theta_\theta}{\pi_\theta \pi_\theta} (\pi_\theta + \pi_\theta b - b)$ but $a_i < a_i$ otherwise. It forgoes some revenue through underentitlement and voluntarily bears extra costs through overentitlement. It is counterintuitive that the firm maximizes its profit by allowing employees who do not observe any business opportunity to access extra information. It is worth remarking that designing escalation options with no escalation in the regular state is feasible (by solving the optimization problem (1) with an additional constraint that $a_i = 0$). However, such a policy results in a lower profit.

The firm uses rewards, audit and violation penalties together to motivate employees to escalate information access without the long-term security risks of overentitlement. To prevent employees from misrepresenting their information needs, the firm audits with higher precision and rewards less when
employees’ choose higher information access \( w_i \leq w_i \leq w_i \) and \( p_i > p_i \geq p_i \).

**Corollary 1:** The firm rewards the employees for the escalation instances only when it does not audit them.

Corollary 1 implies that the firm does not apply two incentives simultaneously for an escalation instance, i.e., \( p_i w_i = 0 \). It is more economical to apply reward only or audit with violation penalties only.

It must be recognized that zero audit precision does not mean that the firm never audits escalation instances at all. The audit precision captures the level of additional time and effort by the firm in investigating the escalation instances compared to regular information access controls. The firm should pay additional attention to the instances of high escalation level and handle other escalation instances as the regular services such as granting regular information access.

**Corollary 2:** The firm implements underentitlement to save the audit cost, and overentitlement to save reward spending.

Proposition 3 implies that the firm rewards the employee more for choosing lower information access and audit with high precision for choosing higher information access. Instead of applying incentives to prevent an employee from misrepresenting her/his observations, the firm can achieve similar result by manipulating the information access. Underentitlement for a business opportunity mitigates an employee’s incentive to overclaim her/his observation when his/her true observation entails a lower revenue potential, saving the firm’s audit cost. Overentitlement for a business opportunity motivates an employee to tell the truth even though s/he observes a low potential or no revenue potential, saving reward spending. Therefore, information access can be considered as a substitute of the reward and a complement of the audit.

We next use numerical examples to show how the violation penalty and private benefit affect the information access level, audit precision and reward. We let \( \theta_h = 8, \theta_l = 3, b = 1, \pi_h = 0.3, \pi_l = 0.3, \pi_0 = 0.4 \). This set of parameters ensures \( b < \pi_h (\theta_h - \theta_l) \) and \( \theta_l > b \). With these specifications, \( a^*_h = 2, a^*_l = 0.75, a^*_0 = 0 \). Figure 5-7 show the information access, audit precision and reward given different marginal private benefit levels.

The audit incentive is more effective with higher penalties. When the penalty level increases, it is less necessary for the firm to manipulate the access levels. Therefore the access levels for high revenue potential and no revenue potential are closer to the optimal levels with higher penalty levels (Figure 5). However, the access level for low revenue potential is complicated. It is first approaching the optimal level from the above. The change from overentitlement to underentitlement marks the point at which the firm switches from using the audit incentive to the reward incentive for this option for low revenue potential. Corollary 2 shows that the firms use underentitlement to save the audit cost. Therefore, the access level for low revenue potential deviates from the optimal level. Nevertheless, it is ultimately gets closer to the optimal level as the penalty level further increases.

When the penalty level increases and the audit incentive becomes more effective, the firm increases audit precision to save the reward spending. The reward decreases with higher penalty levels (Figure 7). On the other hand, higher violation penalty reduces the need to audit with higher precision. Once the reward reaches zero, the firm has incentive to reduce the audit precision. This tradeoff explains the mixed trend of the audit precisions in Figure 6.

Figure 8-10 show the information access, audit precision and reward given different marginal private benefit levels. We use the same specifications of the parameters as Figure 5-7 and let \( F = 0.7 \). This violation penalty enables us to observe all four cases as the marginal private benefit changes.
The access levels deviate more from the optimal as the marginal private benefit increases. With higher marginal private benefit, employees are more likely to escalate to higher information access to obtain higher private benefit. To control employees’ incentive to over-claim access, the firm chooses to reduce the difference between the access levels for high revenue potential and low revenue potential (Figure 8). In addition, it audits with higher precision for the option with high revenue potential (Figure 9), or reward more for the option with low revenue potential (Figure 10). Figure 9 and 10 also show that when the firm starts using rewards, it keeps the audit precision for the high revenue option constant. To prevent employees from escalating access for low revenue potential case when there is no revenue potential, the firm offers higher information access and higher reward. From the employees’ perspective, the employees who observe high revenue potential obtain high information access and generate high private payoff without the risk of being penalized. They will not choose other escalation options even though they will not be rewarded by the firm. The employees who observe lower revenue potential or no business opportunity are deterred from over-claiming their observations by the audit possibility and potential violation penalties. They are also compensated by the firm through rewards for disclosing their observations.

The firm makes a positive profit by offering the escalation options in the asymmetric information case, which justifies the provision of the escalation options. With the same specifications of parameters, the optimal profit is 2.7375. Figure 11 shows the firm’s profit given different violation penalty levels and marginal private benefit. The firm’s profit in the asymmetric information case is lower than the optimal profit in the benchmark case for three reasons. First, the access levels in the escalation options deviate from the optimal access levels in the benchmark case (over-entitlement or under-entitlement); second, the firm has to invest in audit capability; finally the firm shares its profit with the employees through rewards.

The firm’s profit is higher when it is less costly for the firm to motivate employees to disclose their observations. Higher marginal private benefits of access increase the employees’ incentive to cheat. The firm must further distort the escalation access and offer higher rewards to drive employees to report the truth, resulting in higher costs. Even though penalties are never applied in the equilibrium, they are an effective instrument to motivate employees to tell the truth. The firm’s profits increase when the penalty level increases.

5. Conclusion

Using game-theoretic analysis, we have shown how the firm can encourage value creation through flexible access governance, while controlling information misuse. By properly designing the access governance with escalation options, the firm seizes every business opportunity without bearing significant security risks. Rewards, audit and violation penalties together provide employees with incentives to escalate to the appropriate level of information access. Our analysis provides many interesting insights into the implementation challenges of access governance with escalation.

1. The firm should consider providing employees with more information access in escalation options than strictly needed because of information asymmetry. Such a strategy is optimal in that the firm can take advantage of the employees’ private benefit to save audit expenditure and rewards. The proposed scheme does not imply that the firm should offer three escalation options, with employees escalating no matter whether there is a business opportunity or not. The firm can set two options instead of three, assigning the escalation level with additional access in place of the regular level (and thus freeing them from escalating from time to time when there is no business opportunity).

2. Escalation must be done within the allowable zone dictated by regulatory requirements. Some data or applications cannot be made available through an escalation scheme. By providing options with
predefined access levels, the firm controls the limit for escalation.

3. Audit quality is an important element of our governance scheme. Without the ability to catch cheaters (i.e., the audit cost is extremely high), firms are better-off moving towards a more traditional rigid role-based access approach. Escalation must be done in a way that provides an audit trail, including records of who requested it, when, what data was accessed, and what value was created (e.g., the type of transaction being performed) (Rissanen et al., 2004). Nevertheless, perfect monitoring is technologically challenging or financially undesirable in most cases. This study provides managers guidance on saving audit expenditures using rewards and balancing the incentive spending and the security risks.

4. Penalty instruments need not be monetary or be directly levied against the employees. For example, operational penalties could be very effective, such as mandatory attendance at compliance training for violators or requiring employees to file reports for the illegitimate escalation. We have also observed cases where the security fines were levied against the employees’ manager, highlighting the manager’s responsibility for training.

5. The firm needs to know employees’ private benefit to properly design the escalation options. It is important for the firm to learn employees’ characteristics over time or through other approaches, and only grant escalation flexibility to known employees.

6. The value of the access governance system with escalation options also includes the possibility that the firm learns the dynamics of the business environment from employees. Sometimes the firm is unaware of potential business opportunities simply because employees forwent them. The escalation scheme creates an implicit communication channel between the firm and employees. It is also possible for the firm to spot trends that could identify a potentially malicious insider. Finally, it can be very helpful in establishing regular access levels and understanding how employees’ roles change over time (sometimes referred to as role drift). By observing employees’ needs over time, the firm can adjust their regular accesses accordingly.
Proof of Proposition 1

Proof: Since larger $F_i$ and $F_j$ make (IC-H0) and (IC-L0) easier to hold and $F_h$ and $F_i$ do not appear in the firm’s expected profit function, the firm maximizes its profit by imposing the maximal level of penalty.

Proof of Proposition 2

Proof: If $\overline{F} \to \infty$, (IC-H0) and (IC-L0) are not binding if $p_h > p_i > 0$. The optimization problem can be simplified as

$$L = \pi_h (\theta_h a_h - \frac{1}{2} sa_b^2 - \frac{1}{2} tp_b^2 - w_b)$$

$$+ \pi_i (\theta_i a_i - \frac{1}{2} sa_i^2 - \frac{1}{2} tp_i^2 - w_i)$$

$$+ \pi_h (\theta_h a_h - \frac{1}{2} sa_b^2 - \frac{1}{2} tp_b^2 - w_b)$$

$$+ \lambda_i (w_i + ba_i - w_i - ba_i)$$

$$+ \lambda_i (w_i + ba_i - w_i - ba_i)$$

$$+ \lambda_i (w_i + ba_i - w_i - ba_i)$$

$$+ \lambda_i (w_i + ba_i - w_i - ba_i)$$

FOC w.r.t. $a_h$: $\pi_h (\theta_h - s_b a_h) - \lambda_h b - \lambda_i b = 0$

FOC w.r.t. $p_h$: $\pi_h (-tp_h) + \lambda_i (\overline{F} + w_h) = 0$

FOC w.r.t. $w_h$: $\pi_h (-1) + \lambda_i - \lambda_i (1 - p_h) = 0$

FOC w.r.t. $a_i$: $\pi_i (\theta_i - s_a a_i) + \lambda_i - \lambda_i b b = 0$

FOC w.r.t. $p_i$: $\pi_i (-tp_i) + \lambda_i (\overline{F} + w_i) = 0$

FOC w.r.t. $w_i$: $\pi_i (-1) + \lambda_i - \lambda_i (1 - p_i) = 0$

FOC w.r.t. $a_h$: $\pi_h (-s) - \lambda_i b - \lambda_i b + \lambda_i b = 0$

FOC w.r.t. $w_h$: $\pi_h (-1) - \lambda_i - \lambda_i b + \lambda_i b = 0$

$\lambda_i (w_i + ba_i - w_i - ba_i) = 0$

$\lambda_i (w_i + ba_i - w_i - ba_i) = 0$

$\lambda_i (w_i + ba_i - w_i - ba_i) = 0$

$\lambda_i (w_i + ba_i - w_i - ba_i) = 0$

$\lambda_i (w_i + ba_i - w_i - ba_i) = 0$

We obtain $a_h = \frac{1}{2} \theta_h$, $a_i = \frac{1}{2} \theta_i$, $w_h = w_i = 0$. Since the penalty is effective only if misuse can be detected, the firm has to audit escalation instances. $p_h = p_i = \epsilon \to 0$. The firm’s profit approaches $\frac{1}{2} \pi_h (\theta_h a_h^2 + \pi_h \theta_i^2)$. 

Proof of Proposition 3

Proof: The Lagrangian of the firm’s optimization problem can be represented as

$$\text{FOC w.r.t. } \theta_h: \frac{1}{\pi} (\theta_h - \frac{1}{1-\pi} b)$$

$$\text{FOC w.r.t. } \theta_i: \frac{1}{\pi} (\theta_i - \frac{1}{1-\pi} b)$$

$$\text{FOC w.r.t. } p_h: \pi_h (\theta_h - \theta_i) - \frac{1}{1-\pi} b$$

$$\text{FOC w.r.t. } w_h: \pi_h (\theta_h - \theta_i) - \frac{1}{1-\pi} b$$

If $\overline{F}^2 \leq \frac{1}{\pi} (\theta_h - \theta_i) - \frac{1}{1-\pi} b$, we have $w_h \geq 0$. If $\theta_h - \theta_i > \frac{1}{1-\pi} b$, we have $a_h > a_i$. 

Case B1: When $\{\lambda_i = 0, \lambda_i > 0, \lambda_i > 0, \lambda_i = 0\}$ and $\overline{F}^2 > \frac{1}{\pi} (\theta_h - \theta_i) - \frac{1}{1-\pi} b$, we have $a_h = \frac{1}{2} (\theta_h - \theta_i - \frac{1}{\pi} b, \lambda_i + \frac{1}{\pi} (\theta_h - \theta_i) - \frac{1}{1-\pi} b)$.
\[ a_i = \frac{1}{\Delta} \left( \theta_i - \frac{\pi_i (\pi_i + \pi_i \theta_i)}{(\pi_i F + \pi_i b)^2} + \lambda_i \right), \quad a_0 = \frac{\theta_0}{b} \]

\[ p_b = \frac{\pi_b (\pi_b + \pi_b \theta_b)}{(\pi_b F + \pi_b b)^2} F, \quad p_i = p_0 = 0, \quad F_i = F = F, \]

\[ F_i, F_0 \in [0, F], \quad w_i = w_0 = 0, \]

\[ w_0 = \frac{1}{\Delta} \left( \theta_0 - \frac{\pi_0 (\pi_0 + \pi_0 \theta_0)}{(\pi_0 F + \pi_0 b)^2} + \lambda_0 \right), \quad \lambda_i = \lambda_0 = 0, \quad \lambda_2 = \frac{\pi_2 (\pi_2 + \pi_2 \theta_2)}{(\pi_2 F + \pi_2 b)^2} \]

\[ \lambda_3 = \frac{\pi_3 (\pi_3 + \pi_3 \theta_3)}{(\pi_3 F + \pi_3 b)^2} \]

\[ \lambda_4 = \frac{\pi_4 (\pi_4 + \pi_4 \theta_4)}{(\pi_4 F + \pi_4 b)^2} \]

\[ F_0 = F_i = F \]

\[ F_0 \in [0, F], \quad w_i = w_0 = w_0 = 0 \]

It is easy to verify that \( a_i^a > a_i^b \) and \( p_i^a > p_i^b \) always hold. If \( F^2 > \frac{\Delta}{\pi_0 (\pi_0 + \pi_0 \theta_0)} (\pi_0 F + \pi_0 b) \), we have \( a_i^a > a_i^b \) and \( a_i^b < a_i^b \) and \( a_i^b < a_i^b \). Compare the firm’s profits in Case I1, I2, B1 and B2, we can conclude that given \( \pi_0 (\pi_0 + \pi_0 \theta_0) > \theta_0 \), the optimal solution is

5) When \( F^2 \leq \frac{\Delta}{\pi_0 (\pi_0 + \pi_0 \theta_0)} (\pi_0 F + \pi_0 b) \), Case I1;

6) When \( \frac{\Delta}{\pi_0 (\pi_0 + \pi_0 \theta_0)} (\pi_0 F + \pi_0 b) \leq \frac{\Delta}{\pi_0 (\pi_0 + \pi_0 \theta_0)} (\pi_0 F + \pi_0 \theta_0 F) \), Case B1;

7) When \( \frac{\Delta}{\pi_0 (\pi_0 + \pi_0 \theta_0)} (\pi_0 F + \pi_0 \theta_0 F) < \frac{\Delta}{\pi_0 (\pi_0 + \pi_0 \theta_0)} (\pi_0 F + \pi_0 \theta_0 F) \), Case I2;

8) When \( F^2 > \frac{\Delta}{\pi_0 (\pi_0 + \pi_0 \theta_0)} (\pi_0 F + \pi_0 \theta_0 F) \), Case B2.

7. References


Ferreira, A., Cruz-Correia, R., Antunes, L., Farinha, P., Oliveira-Palhares, E., Chadwick, D., and Costa-Pereira, A. “How to Break Access Control in a Controlled Manner,” in


