Information Governance: Flexibility and Control through Escalation and Incentives

Xia Zhao M. Eric Johnson

Center for Digital Strategies[*]*, Tuck School of Business, Dartmouth College*

Xia.Zhao@dartmouth.edu; M.Eric.Johnson@dartmouth.edu

April 24, 2008

Abstract

Managing information access within large enterprises 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 a governance structure based on controls and incentives, where employees' self-interested behavior can result in firm-optimal use of information. Using a game-theoretic approach, we show that an incentives-based policy with escalation can control both overentitlement and underentitlement while maintaining the flexibility needed in dynamic business environments.

1 Introduction

As the global economy evolves from the industrial age to the digital age, its focus has shifted away from the production of the physical goods towards the manipulation of information. Timely

[*]The Center for Digital Strategies at the Tuck School of Business examines the role of digital strategies in corporations and the use of technology-enabled processes to harness an organization's unique competencies, support its business strategy, and drive competitive advantage. This research was supported through the Institute for Security Technology Studies at Dartmouth College, under award Number 2006-CS-001-000001 from the U.S. Department of Homeland Security (NCSD). The statements, findings, conclusions, and recommendations are those of the authors and do not necessarily reflect the views of the Department of Homeland Security.

access to information has become a critical resource for many data-oriented organizations such as investment banks, research firms, and hospitals. Such firms have invested heavily in information technology to improve data access for employees and partners. However, in recent years, the governance of access has grown to become a significant challenge as firms struggle to balance two opposing forces.

On one hand, 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], [von Hippel, 1994], or [Tsai, 2001]). Likewise, the services and supply chain literature have also extolled the benefits of increased information availability (e.g., [Rathnam et al., 1995] or [Lee et al., 2000]). 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. On the other hand, rising security and privacy concerns are now driving managers to constrict the availability of information. Driven by fears of data breaches, intellectual property losses, and compliance violations, firms are working to reduce information access through better controls and governance [Goetz and Johnson, 2007].

Access governance includes the policies, controls, incentives, and processes that manage user access to information resources. More narrowly, access control focuses on the technical implementation of privileges. 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.[1] The goal of such access governance is to ensure the information systems deliver the right information to the right people at the right time, but also protect the information from misuse, including security and privacy violations. By far, the most common reason that firms adopt access governance 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). Recently, many firms have initiated efforts to strengthen their control systems to comply with 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

[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. Entitlement, privilege and permission are used interchangeably.

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.

One governance approach is referred to as "the rule of least access" [Aveksa, 2007]. Using that approach, each agent is provided with the minimum entitlements needed to perform his task. To ensure the rule of least access, a control system must be customized and dynamically managed including five components—request, approve, administer, enforce and monitor. Specifically a user requests an entitlement; the owner 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 control system. With this approach, employees' access 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 access are daunting.

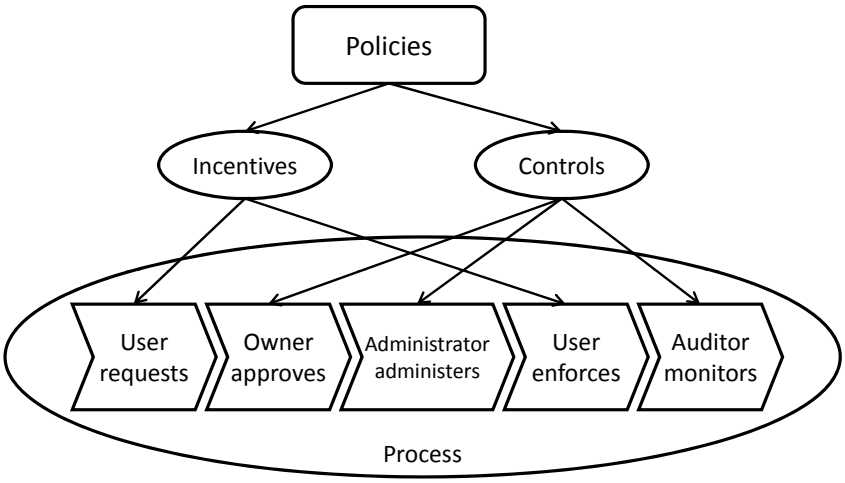


Figure 1: Information Governance System

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 orga-

nizational structures and personnel to adapt the consumers' needs. The grant of an entitlement typically requires significant interaction among the user, the owner and the administrator. This interaction delays organizations' response to the consumers' needs, resulting in missed opportunities or degraded service quality.

Rather than customizing the assignment of privileges for every employee, some organizations use a role-based approach where users are segmented into roles and given a blanket set of privileges related to that role. For example, all tellers in a bank perform roughly the same job and receive the same set of privileges. This approach works well for organizations with a few dominant roles that do not change. However, in some cases it is difficult to establish such clear roles and the information needs of those roles quickly change over time. Sinclair et al. (2007) found in their field study of an investment bank, that a business group of 3,000 people witnessed 1,000 changes to organizational structure within just a few months. Traditional access management approaches are not well suited to such a dynamic environment.

More importantly, employees often start in one role, but through promotions and transfers, require new privileges. Sinclair et al. (2007) found that privileges simply accumulate over the length of employment, leaving the employees with far more access then needed in their positions. This outcome is sometimes rationalized by the argument that long-term employees are valuable and need quick access to information to create value for the firm. But, as the employs become "overentitled", they become larger security risks 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 their accounts.

In an increasingly dynamic world, information governance must be flexible, yet secure. To achieve flexibility, we consider a different approach where employees are given a base level of access, but allowed to escalate into controlled data and applications when needed. This allows one-time access without any time-delaying approval process. We have witnessed such an approach in several settings, including investment banking (where it is sometimes referred to as "override" [Rissanen et al., 2004]) and health care (where it is called "break glass" [Ferreira et al., 2006]). In the cases we observed, escalation was used to solve a failure of traditional access control system.

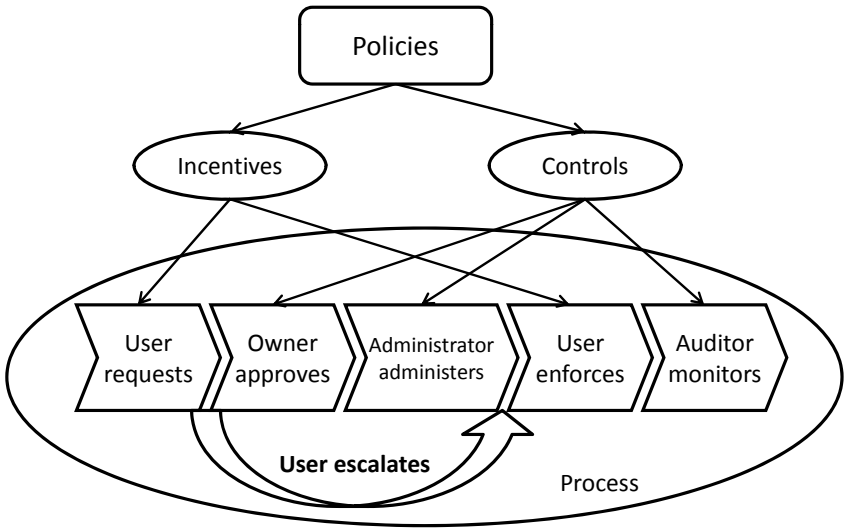


Figure 2: Information Governance System with Escalation

However, escalation potentially breeds significant security risks since employees may abuse their ability to access information. For example, accessing information not for business reasons but rather for personal benefit. 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) 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].

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 suited to some financial or trading systems where there is significant risk of massive fraud. Rather it is useful in cases where there are many small risks or where the potential value of escalation is very high. For example, escalation is very effective in situations such as access to private medical information, where emergency access may save someone's life, or in a time-critical systems where the person with the necessary privileges may be unavailable [Povey, 2000].

In this paper, we design an access governance system with flexibility. In addition to assigning

regular access to employees, the firm allows employees to escalate while detecting and penalizing abusive or malicious activities. The access management policy couples auditing with a bonus scheme to reward employees who create value for the firm through escalation. We show that combined with the proper incentives, our governance approach could provide the desired access flexibility with a significant level of control. To the best of our knowledge, ours is the first work to examine the role of incentives to drive optimal behavior within the context of information access.

The paper is organized as follows. In Section 2, we reviewed the related literature. In Section 3 and Section 4, we model the action of the firm and employees and analyze the resulting Stackelberg game to derive the equilibrium. We capture the important characteristics of the optimal information governance structure and illustrate how the model can be used to provide managerial insight. Finally we conclude with implementation guidance in Section 5.

2 Related Literature

The technological aspect of incorporating an escalation scheme into 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 (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. 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-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] or [Shavell, 1979], etc.). Our paper closely relates to a large stream of literature which studies the audit policy in a principal-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) showed that the optimal audit policy includes terms 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 and underinvestment. [2] In our paper, all escalation activities are monitored and audited for the purpose of internal control required by regulators. We focus on the firm's optimal strategy in response to the audit results, i.e. the penalty for misuse. Since a perfect audit is impossible or extremely costly to achieve, penalty by itself is incapable to eliminate misuse. We consider incorporating a reward scheme, i.e. the bonus, to alleviate the adverse consequence of imperfect monitoring. We characterize the optimal escalation scheme which helps the firm achieve a significant level of flexibility at some expense of security risks.

3 Modeling Access Governance with Escalation and Incentives

We consider the case where users gain access to data and applications through a system employing access control and where the users actions are monitored to support auditing. 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. The total weighted sum of information that could possibly be made available to an employee is A. Note that this does not include all firm information, as compliance and regulatory requirements make some data and applications off limits.

Information Flows. Based on value generated by an employee and the associated information risk, the firm assigns the employee a regular access level a on $[0, A]$ to perform routine tasks. However, periodically, employees face opportunities to create more value by seizing an emergent opportunity. We assume that with probability γ, an employee will observe such an opportunity and successfully create more value if they can access the requisite information. We represent the information required by the emergent task to be an random variable x, distributed $F(x)$ on $[0, A]$. If the employee's access level is lower than the information requirement, the firm's revenue from the emergent task is reduced. Therefore, the firm allows employees to escalate access levels

[2] We thank our anonymous reviewer for providing important references and helping us better position our paper.

temporarily in the emergent situations. We use e to denote the escalated access level. To mitigate risk of unnecessary escalation, the firm audits each instance of escalation. Thus employees must track their escalation activities and maintain documentation justifying their actions.

Financial Flows. The firm's net revenue from an employee's regular tasks is $U(a)$. The firm bears costs associated with the regular access level of $R(a)$, including security risks and routine technical support required to prudently maintain that access. We assume that $U(.)$ is an increasing and concave function ($U'(.) > 0$ and $U''(.) \leq 0$) and $R(a)$ is an increasing and convex function. $R'(.) > 0$ and $R''(.) > 0$. The firm's net revenue from emergent tasks is $U(\min\{a+e, x\})$.

Employees receive bonuses from the firm based on the value they create performing emergent tasks $S(U(\min\{a+e, x\}))$, where $S(.)$ is an increasing and concave function. $S'(.) > 0$ and $S''(.) \leq 0$. In addition, employees also derive some private benefit from both regular access and from escalating into information beyond their regular access levels. Such "snooping" value is not uncommon - we have witnessed such cases in health care where a provider may examine the records of a patient for their private benefit. The employee's private benefit from escalation is $u(a+e)$, which depends on both the regular access level and the escalated access level. $u(.)$ is an increasing and concave function. $u'(.) > 0$ and $u''(.) \leq 0$. The employees bear cost of $r(a, e)$ from both regular and escalated access in terms of personal risk (the personal pain of being audited or having a security breach) and in terms of the documentation required when escalating past their regular access. Higher levels of information include more risk and more complex documentation in the audit process. We assume $r(a, e)$ is an increasing and convex function of e. $r'_e > 0$ and $r''_e > 0$.

Employees escalate their access levels to meet the information requirements of the emergent tasks. Since employees are self-interested, an employee may escalate to a level that is inconsistent with the information requirement. If the employee's total access level, $a + e$, is higher than the information requirement, x, we say the employee is overentitled. In some cases, risk-averse employees may choose not to escalate to the level needed to achieve the full emergent benefit, which we refer to as underentitled. We assume that all escalation requests receive an audit and that this initial audit cost is fixed, and thus not relevant to our model. However, if overentitlement is suspected, it creates significant security risk that requires more investigation. For example, the firm would need to carefully verify the overentitlement before bringing any action. They would also need to document and evaluate the overentitlement, in compliance with SOX Section 404,

which requires firms to assess the effectiveness of the internal control structure and procedures for financial reporting. We represent this additional auditing cost related to of overentitlement with $R_o(\max\{a+e-x,0\})$. $R_o(.)$ is an increasing and convex function. $R_o'(.) \geq 0$ and $R_o''(.) \geq 0$. On the other hand, underentitlement degrades business performance as represented in the firm's revenue function. To minimize the overentitlement or underentitlement, the firm audits the escalation activities and penalizes employees who abuse their rights or fail to escalate when opportunities arise. The firm can figure out the information requirement x ex post through communicating with managers and coworkers of the employee. However it is unable to accurately measure the access level required to fulfill the information requirement and hence unable to precisely detect the difference. We assume the audit process is imperfect, so the firm does not take action unless the over- or underentitlement exceeds a threshold ε. If the employee is overentitled, the firm will penalize him at a level $n_o(a,e,x,\varepsilon)$ and $n_u(a,e,x,\varepsilon)$ for underentitlement.

The timing of events is showed in Figure 3. At stage 1, the firm announces the access management policy $\{a, S(.), n_o(.), n_u(.)\}$; At stage 2, an employee observes his information requirement, x; At stage 3, the employee escalates his access level and conducts his task; Finally, the firm investigates the escalation, rewarding and penalizing the employee according to the announced access management policy.

Figure 3: The Timing of Events

The firm's access policy will influence the employee's escalation strategies, and, by backward induction, anticipation of the latter will influence the firm's policy design. Given the policy parameters of the firm, the employee chooses e to maximize his payoff for each business task, denoted by $V_{employee}$. The employee's problem is

$$V_{employee} = \max_{e} \quad S(U(\min\{a+e,x\})) + u(a+e) - r(a,e) - n_o(a,e,x,\varepsilon) - n_u(a,e,x,\varepsilon)$$

Considering the employee's response, the firm chooses $\{a, S(.), n_o(.) n_u(.)\}$ to maximize its

profit, denoted by V_{firm}.

$$\begin{aligned} V_{firm} &= \max_{a,S(.),n_o(.),n_u(.)} U(a) - R(a) \\ &\quad +\gamma E\left[U\left(\min\left\{a+e,x\right\}\right) - S\left(U\left(\min\left\{a+e,x\right\}\right)\right) - R_o\left(\max\left\{a+e-x,0\right\}\right)\right] \end{aligned}$$

4 Analysis and Results

4.1 Employee

To gain managerial insight, we analyze the following (tractable) functional forms. We assume that the firm's revenue function is linear, $U\left(\min\left\{a+e,x\right\}\right) = B\left(\min\left\{a+e,x\right\}\right)$ where B is the firm's revenue per unit access level (we refer to B as the revenue rate hereafter) and $\min\left\{a+e,x\right\}$ implies that underentitlement degrades business performance. The employee's private benefit function is linear, $u\left(a+e\right) = b\left(a+e\right)$ where b is the private benefit per unit access level (we refer to b as the unit private benefit hereafter). The assumption of linear revenue and private benefit functions do 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 the access to a linear one. The cost functions are quadratic, $r\left(a,e\right) = \frac{1}{2}\beta e^2$, $R\left(a\right) = \frac{1}{2}sa^2$ and $R_o\left(\max\left\{a+e,x\right\}\right) = \frac{1}{2}t\left(\max\left\{a+e-x,0\right\}\right)^2$. Besides the frequent use of convex cost functions in the literature (e.g., [Kannan and Telang, 2005], [Krishnan and Zhu, 2006] and [Motta, 1993]), quadratic cost functions nicely capture higher security risks associated with higher access as well as the cost of additional IT resources for maintaining and auditing access.

We define w as the bonus rate, where employees are paid $\frac{w}{B}$ of firm revenue for value created, $S\left(U\left(\min\left\{a+e,x\right\}\right)\right) = \frac{w}{B}U\left(\min\left\{a+e,x\right\}\right)$. Additionally, for ease of communication and implementation, we assume that the firm adopts a linear penalty scheme. In particular, $n_o\left(a,e,x,\varepsilon\right) = p\left[a+e-x-\varepsilon\right]^+$ and $n_u\left(a,e,x,\varepsilon\right) = q\left[x-\left(a+e\right)-\varepsilon\right]^+$ where p and q are the penalty rates for overentitlement and underentitlement respectively.[3] The above functional forms ensure that our problems are convex and have unique solutions.

We first analyze the employee's problem. The employee's optimization problem can be repre-

[3] $[y]^+ = \max\left\{y,0\right\}$. $[y]^- = \min\left\{y,0\right\}$

sented by

$$V_{employee} = \max_{e} \quad w\left(x - [x - (a+e)]^{-}\right) + b\,(a+e) - \frac{1}{2}\beta e^2 - p\,[a+e-x-\varepsilon]^{+} - q\,[x-(a+e)-\varepsilon]^{+} \tag{1}$$

With our model fully specified, we can solve for the employees' optimal behavior. An employee's escalation strategy is as follows.

1. If $x \leq a + \frac{b-p}{\beta} - \varepsilon$, $e = \frac{b-p}{\beta}$;
2. If $a + \frac{b-p}{\beta} - \varepsilon < x \leq a + \frac{b}{\beta} - \varepsilon$, $e = x + \varepsilon - a$;
3. If $a + \frac{b}{\beta} - \varepsilon < x \leq a + \frac{b}{\beta}$, $e = \frac{b}{\beta}$;
4. If $a + \frac{b}{\beta} < x \leq a + \frac{w+b}{\beta}$, $e = x - a$;
5. If $a + \frac{w+b}{\beta} < x \leq a + \frac{w+b}{\beta} + \varepsilon$, $e = \frac{w+b}{\beta}$;
6. If $a + \frac{w+b}{\beta} + \varepsilon < x \leq a + \frac{w+b+q}{\beta} + \varepsilon$, $e = x - \varepsilon - a$;
7. If $a + \frac{w+b+q}{\beta} + \varepsilon < x \leq A$, $e = \frac{w+b+q}{\beta}$.

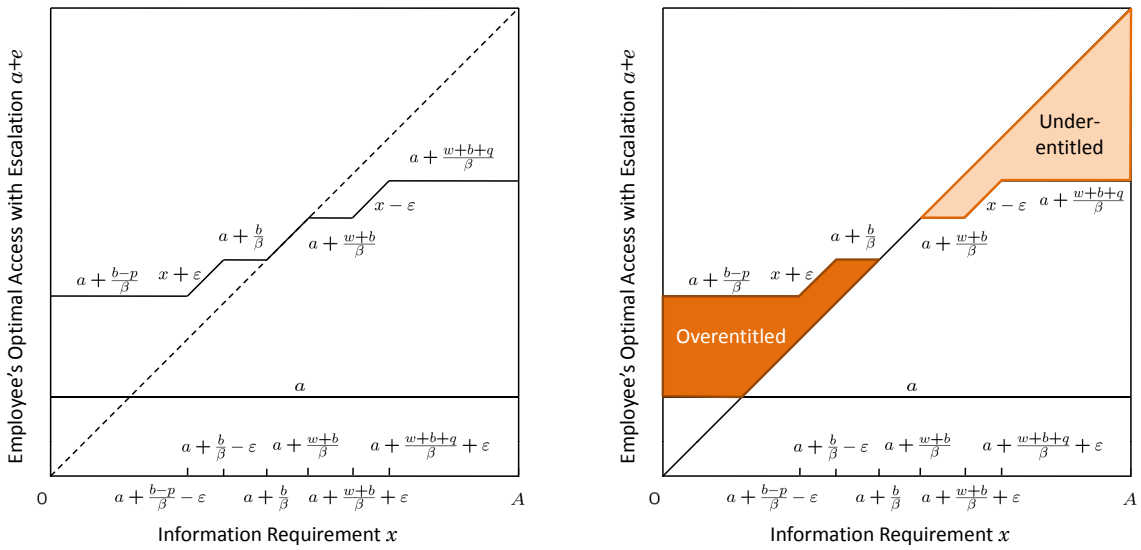
(See Proof 1.)

With the escalation strategy, we obtain Proposition 1.

Proposition 1 *The employee will be overentitled (or underentitled) if the information requirement is low (or high). i.e. if* $x \leq a + \frac{b}{\beta}$, $a + e > x$, *and if* $x > a + \frac{w+b}{\beta}$, $a + e < x$.

(See Proof 2.)

Figure 4 shows an employee's escalation strategy. The graph in Figure 4(a) represents an employee's total access level after escalation given different information requirements of the emergent task. The horizontal axis represents the level of information requirement and the vertical axis represents the employee's total access level. When the information requirement of the emergent task is lower than $a + \frac{b}{\beta}$, an employee always gains access beyond the information requirement. This "snooping" behavior is driven by the employee's private benefit from accessing extra information. The marginal benefit of the escalated access is b and the marginal cost is βe, which is proportional to the magnitude of the escalated access. Employees will escalate as much access as possible until



(a) Optimal Access with Escalation

(b) Overentitlement and Underentitlement

Figure 4: An Employee's Escalation Strategy

the cost of the incremental access exceeds the benefit. The firm can mitigate the overentitlement by auditing the escalation activities and penalizing employees who are overentitled. This penalty reduces the benefit of the incremental access from b to $b-p$ and the escalated access drops from $\frac{b}{\beta}$ to $\frac{b-p}{\beta}$. Consequently, when the information requirement is lower than $a+\frac{b-p}{\beta}-\varepsilon$, the employee will escalate to $a+\frac{b-p}{\beta}$. When the information requirement falls in the range $(a+\frac{b-p}{\beta}-\varepsilon, a+\frac{b}{\beta}]$, it is not worthwhile for the employee to escalate to a level that precipitates a penalty. Instead, the employee takes advantage of the audit imperfection and escalates to a level that is either ε higher than the information requirement or $a+\frac{b}{\beta}$, which is the optimal total access an employee would achieve without the incentive scheme. The dark-shaded area in Figure 4(b) represents all cases where the employee is overentitled.

When the information requirement of the emergent task is larger than $a+\frac{b}{\beta}$, the cost of escalating to the information requirement dominates the marginal private benefit from the escalated access. In this case, an employee tends towards underentitled if no bonus incentive w is offered. Using revenue bonuses and underentitled penalties, the firm can motivate the desired behavior. When the total access is less than the information requirement, the bonus increases the marginal benefit of the escalated access from b to $w+b$. Thus, in cases where the information requirement falls in

the range of $(a + \frac{b}{\beta}, a + \frac{w+b}{\beta}]$, the employee will escalate right to the information requirement (no over- or underentitled). When the information requirement increases beyond $a + \frac{w+b}{\beta}$, the bonus, by itself, is incapable of providing enough escalation incentive to the employee. The employee will escalate to a level that is lower than the information requirement. The penalty for underentitlement increases the marginal benefit of the escalated access to $w+b+q$ and further motivates the employee to escalate to a higher level. When the information requirement falls into $(a + \frac{w+b}{\beta}, a + \frac{w+b+q}{\beta} + \varepsilon]$, the employee will again take advantage of the audit imperfection and escalate as close to $\frac{w+b}{\beta}$ as possible. When the information requirement is greater than $a + \frac{w+b+q}{\beta} + \varepsilon$, the escalated access becomes $\frac{w+b+q}{\beta}$. The light-shaded ares in Figure 4(b) represents all cases where the employee is underentitled.

The shaded areas represent the cases that the employee's access level is inconsistent with the information requirement of the emergent task, which imposes cost to the firm. The firm can adjust its access governance policy $\{a, w, p, q\}$ to influence the employee's escalation strategy. In the next section, we will analyze the firm's optimal strategies.

4.2 Firm

The firm chooses a, w, p and q to maximize its profit. Its optimization problem is

$$V_{firm} = \max_{a,w,p,q} Ba - \frac{1}{2}sa^2 + \gamma E\left[(B-w)\left(x - [x-(a+e)]^-\right) - \frac{1}{2}t\left([(a+e)-x]^+\right)^2\right] \qquad (2)$$

Considering the employee's escalation strategy, (2) can be represented by

$$
\begin{aligned}
V_{firm} \quad = \quad & \max_{a,w,p,q} Ba - \frac{1}{2}sa^2 \qquad (3)\\
& +\gamma \int_0^{a+\frac{b-p}{\beta}-\varepsilon} \left((B-w)\, x - R_o \left(a + \frac{b-p}{\beta} - x \right) \right) f(x)\, dx \\
& +\gamma \int_{a+\frac{b-p}{\beta}-\varepsilon}^{a+\frac{b}{\beta}-\varepsilon} \left((B-w)\, x - R_o(\varepsilon) \right) f(x)\, dx \\
& +\gamma \int_{a+\frac{b}{\beta}-\varepsilon}^{a+\frac{b}{\beta}} \left((B-w)\, x - R_o \left(a + \frac{b}{\beta} - x \right) \right) f(x)\, dx \\
& +\gamma \int_{a+\frac{b}{\beta}}^{a+\frac{w+b}{\beta}} (B-w)\, x f(x)\, dx \\
& +\gamma \int_{a+\frac{w+b}{\beta}}^{a+\frac{w+b}{\beta}+\varepsilon} (B-w) \left(a + \frac{w+b}{\beta} \right) f(x)\, dx \\
& +\gamma \int_{a+\frac{w+b}{\beta}+\varepsilon}^{a+\frac{w+b+q}{\beta}+\varepsilon} (B-w)\, (x-\varepsilon)\, f(x)\, dx \\
& +\gamma \int_{a+\frac{w+b+q}{\beta}+\varepsilon}^{A} (B-w) \left(a + \frac{w+b+q}{\beta} \right) f(x)\, dx
\end{aligned}
$$

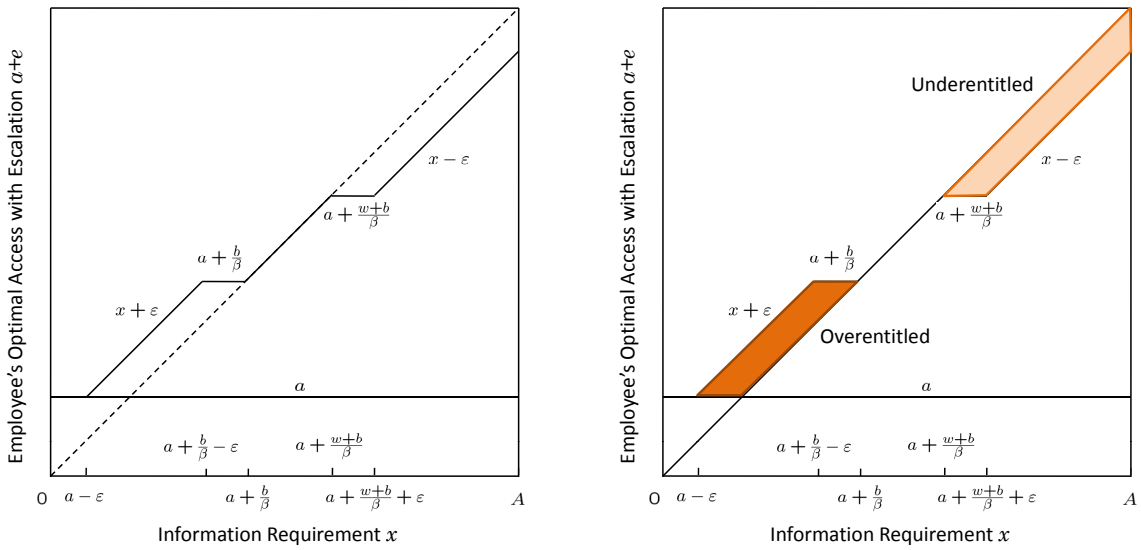
Lemma 1 gives the firm's penalty strategies.

Lemma 1 *The penalty for overentitlement eliminates an employee's private benefit. i.e.* $p = b$ *and the penalty for the underentitlement is large enough to minimize underentitlement. i.e.* $q \geq [(A - a - \varepsilon)\beta - w - b]^+$.

(See Proof 3.)

Employee escalation beyond the information requirement is driven by their private benefit. Lemma 1 shows that the optimal penalty for overentitlement should completely eliminate the employee's private benefit from additional access. The penalty for underentitlement should be large enough to motivate the employee to escalate his access as close to the information requirement as possible. Figure 5 shows the employee's escalation strategy with the optimal penalty rates.

In Figure 5 (b), the overentitlement (the dark-shaded area) and underentitlement (the light-shaded area) still exist. With an imperfect audit instrument, the penalty scheme by itself cannot completely eliminate the overentitlement and underentitlement. Since the bonus increases the employee's benefit from the incremental access and this effect is valid only when the total access



(a) Optimal Access with Escalation

(b) Overentitlement and Underentitlement

Figure 5: An Employee's Escalation Strategy with Optimal Penalty Rates

level is less than the information requirement, firms can use bonus to reduce these underentitlement cases. Figure 5 (b) shows that a larger bonus rate, w, moves the light-shaded area upward and decreases the size of the underentitlement area.

Next we explore how the firm uses the bonus to motivate the employee. With the optimal penalty rates, the firm's optimization problem can be represented by

$$
\begin{aligned}
V_{firm} \;=\; & \max_{a,w} Ba - \frac{1}{2}sa^2 \qquad (4)\\
& +\gamma \int_0^{a-\varepsilon} \left((B-w)\, x - R_o\left(a-x\right) \right) f\left(x\right) dx \\
& +\gamma \int_{a-\varepsilon}^{a+\frac{b}{\beta}-\varepsilon} \left((B-w)\, x - R_o\left(\varepsilon\right) \right) f\left(x\right) dx \\
& +\gamma \int_{a+\frac{b}{\beta}-\varepsilon}^{a+\frac{b}{\beta}} \left((B-w)\, x - R_o\left(a+\frac{b}{\beta}-x\right) \right) f\left(x\right) dx \\
& +\gamma \int_{a+\frac{b}{\beta}}^{a+\frac{w+b}{\beta}} (B-w)\, x f\left(x\right) dx \\
& +\gamma \int_{a+\frac{w+b}{\beta}}^{a+\frac{w+b}{\beta}+\varepsilon} (B-w) \left(a+\frac{w+b}{\beta}\right) f\left(x\right) dx \\
& +\gamma \int_{a+\frac{w+b}{\beta}+\varepsilon}^{A} (B-w)\left(x-\varepsilon\right) f\left(x\right) dx
\end{aligned}
$$

Proposition 2 *If the audit is perfect, the firm only adopt the penalty scheme. i.e.* $w = 0$.

(See Proof 4.)

Implementation of the penalty scheme is based on the assumption that the firm can detect misuse through auditing. If there is no audit error, the penalty scheme can eliminate over- and underentitlement. If the audit process is imperfect, the employees will be either over- or underentitlement. The bonus rate and the penalty rates are different incentives instruments. The bonus scheme requires the firm to share revenue with employees and motivates the employees to consider the firm's loss of business. Therefore it can be used to address the underentitlement. Although this incentive is costly to the firm, the firm still have incentives to implement the bonus scheme in presence of the audit imperfection.

In this paper, we assume the audit precision is exogenous to the model. An interesting area for future research is to extend the analysis, considering the case where firms can invest to reduce audit error along with the tradeoff between audit imperfection and bonus.

When there is audit error, the optimal bonus rate w can be represented by

1. $w_1 = \left[\frac{(B-b)\varepsilon - \beta\varepsilon a - \frac{1}{2}\beta(A-\varepsilon)^2}{2\varepsilon} \right]^+$ if $a + \frac{w+b}{\beta} + \varepsilon \leq A$;
2. $w_2 = \frac{-2\beta\left(a+\frac{b}{\beta}-A-\frac{B}{2\beta}\right)+\beta\sqrt{\left(a+\frac{b}{\beta}+\frac{B}{\beta}-A\right)^2+3A^2}}{3}$ otherwise.

The benefit and cost of the bonus to the firm are shown in Figure 6. When the bonus rate is small (Figure 6(a), $a + \frac{w+b}{\beta} + \varepsilon \leq A$), the firm's total benefit from a specific bonus rate w is $(B - w)\,\varepsilon\frac{w}{\beta}$, where $\varepsilon\frac{w}{\beta}$ is proportional to the expected level of the escalated access motivated by the bonus(the dark-shaded area) and $(B - w)$ is the net unit revenue from the escalated access. The total benefit is first increasing and then decreasing as the bonus rate increases.

The bonus scheme with the bonus rate w costs the firm $w\left(\frac{1}{2}(A-\varepsilon)^2 + \varepsilon\left(a + \frac{w+b}{\beta}\right)\right)$ where $\frac{1}{2}(A-\varepsilon)^2 + \varepsilon\left(a + \frac{w+b}{\beta}\right)$ is proportional to the the revenue that the firm earns from the expected escalated access (the light-shaded area). The total bonus (or the cost of the bonus to the firm) is increasing in w. The firm will choose a bonus rate w to maximize the difference between $(B - w)\,\varepsilon\frac{w}{\beta}$ and $w\left(\frac{1}{2}(A-\varepsilon)^2 + \varepsilon\left(a + \frac{w+b}{\beta}\right)\right)$. w_1 gives the optimal bonus rate. If $a + \frac{w+b}{\beta} + \varepsilon > A$, the benefit and cost of the bonus are shown in Figure 6 (b). The expected benefit of the bonus is constrained by the maximal information access A as the dark-shaded area in Figure 6(b) shows. The optimal w is given by w_2.

Next we examine the optimal regular access assigned by the firm. The optimal regular access level is

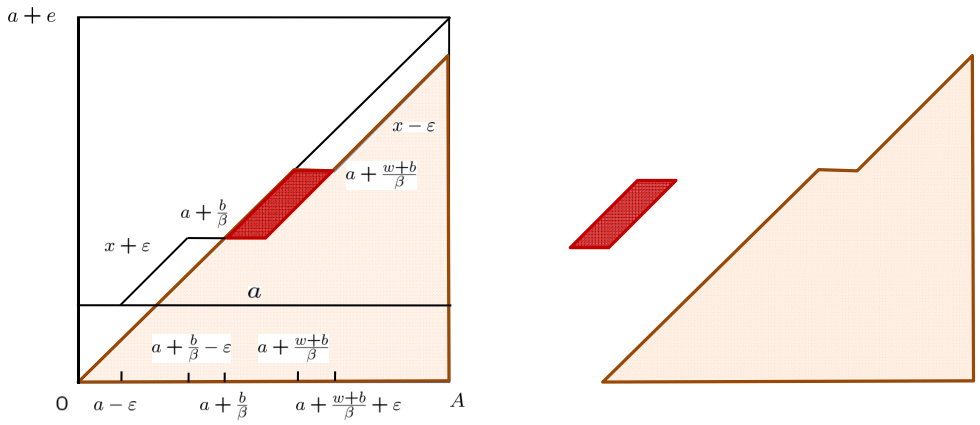
1. $a^* = \frac{-(2As-\gamma\beta\varepsilon)+\sqrt{(2As-\gamma\beta\varepsilon)^2-4\gamma t\left(-2\gamma\varepsilon B-2AB+\gamma(B-b)\varepsilon-\gamma\beta\frac{1}{2}(A-\varepsilon)^2\right)}}{2\gamma t}$ if $a^* + \frac{w^*+b}{\beta} + \varepsilon \leq A$
2. Otherwise, a^* is the solution of $a^* = \frac{-(As+\gamma(B-w^*))+\sqrt{(As+\gamma(B-w^*))^2+2\gamma t\left(\gamma(B-w^*)\left(A-\frac{w^*+b}{\beta}\right)+AB\right)}}{\gamma t}$ and $w^* = w_2$.

(See Proof 5.)

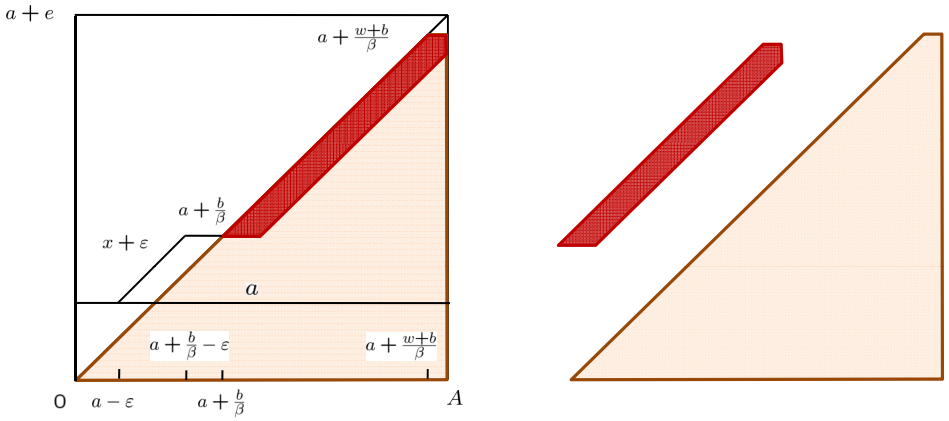
Proposition 3 *Bonus and regular access are substitutes.*

(See Proof 6.)

Proposition 3 is evident from the fact that $V''_{wa} = \frac{\partial V_{firm}}{\partial w \partial a} < 0$. The benefit of the bonus rate is decreasing when the regular access increases and vice versa. Figure 6 illustrates that both regular access and the bonus rate effect the size of the light-shaded area, and in turn the firm's profit in the same way. Therefore the regular access and the bonus potentially substitute for each other. In particular, if the regular access increases, the bonus rate decreases. When the regular access increases, the light-shaded area expands and the cost of the bonus increases. Consequently, the firm will choose a lower bonus rate.



(a) $a+\frac{w+b}{\beta}+\varepsilon \leq A$



(b) $A < a+\frac{w+b}{\beta}+\varepsilon$

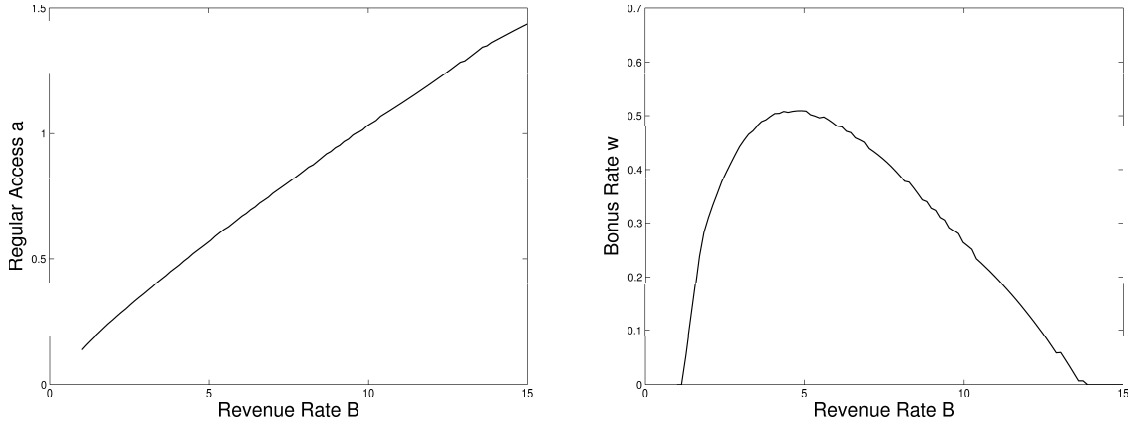
Figure 6: The Benefit and Cost of the Bonus

Corollary 1 *The bonus rate is decreasing in the regular access.*

(See Proof 7.)

We next discuss how the regular access and the bonus rate are influenced by the parameters of the model. Figure 7 illustrates how the firm assigns regular access levels a and bonus rates w for different revenue rates B. The graph in Figure 7(a) shows that the optimal regular access level increases in the revenue rate. The trend is driven by the increased marginal benefit from routine business tasks. The curve in Figure 7(b) shows that the bonus rate first increases then drops back to zero as the revenue rate increases. The revenue rate influences the firm's incentives to use the bonus in two ways. On one hand, the higher revenue rate implies that the firm benefits more from

the increased access and hence the firm has more incentives to use bonus to motivate its employees. On the other hand, the higher revenue rate results in higher regular access, which mitigates the benefit from the additional access (the dark-shaded area is constrained by the upper bound of the potential access in Figure 6(b)). Thus, the firm has less incentive to use the bonus to provide escalation incentives.



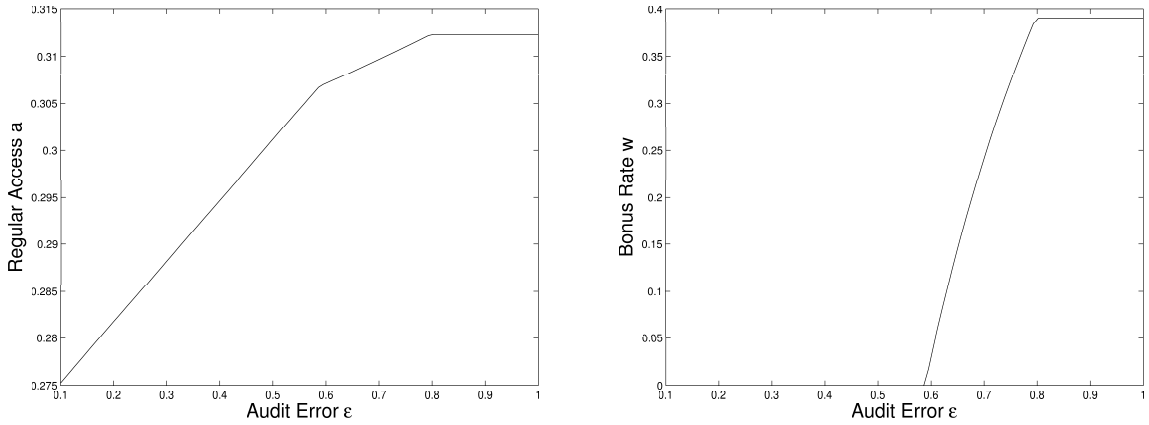
(a) The Optimal Regular Access

(b) The Optimal Bonus Rate

Figure 7: The Optimal Regular Access and Bonus Rate. $A = 2, \gamma = 0.5, t = s = 9, \beta = 1, \varepsilon = 1, b = 0.5$

Figure 8 shows the optimal regular access and the bonus rate given different audit errors. Note that the penalty scheme is ineffective in addressing the overentitlement and underentitlement caused by the audit imperfection, but the bonus can reduce the underentitlement. When the audit error increases, the firm loses more from underentitlement and hence has more incentives to increase the bonus rate. Likewise, the regular access can reduce underentitlement (the light-shaded area in Figure 5(b) shrinks). Therefore, the firm has an incentive to assign higher regular access to the employee when the audit error increases.

In contrast to the audit error, the private benefit negatively affects the optimal regular access and the bonus rate as Figure 9 illustrates. When the private benefit increases, the underentitlement situatations are less likely to occur (the dark-shaded area in Figure 6 is shifted upward.) The benefit of the bonus scheme decreases. Thus, the firm will set a lower bonus rate and a lower regular access.



(a) The Optimal Regular Access

(b) The Optimal Bonus Rate

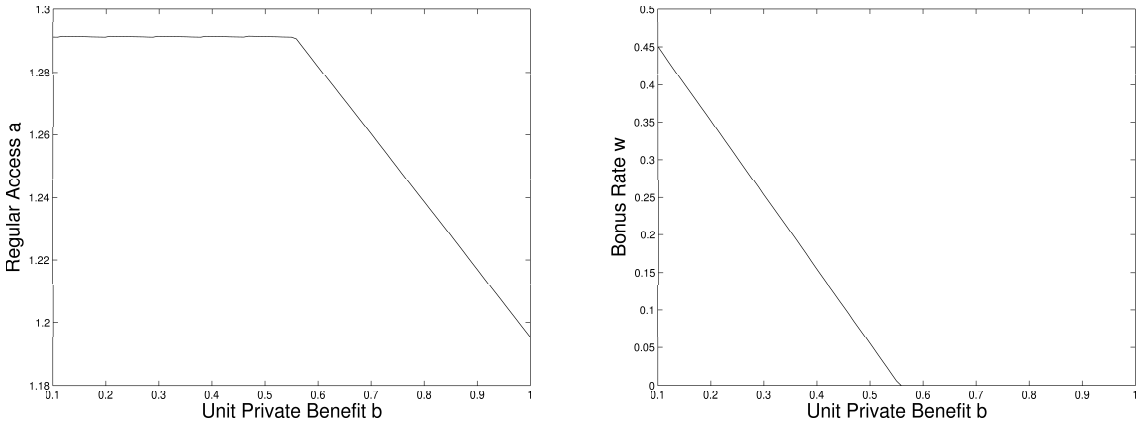
Figure 8: The Optimal Regular Access and Bonus Rate with Different Audit Errors. $A = 2, \gamma = 0.5, t = s = 9, \beta = 1, b = 0.5, B = 2.5$

5 Conclusion

Using game-theoretic analysis, we have shown how incentives can be used to encourage value creation through flexible information access schemes, while controlling information misuse. Set properly, penalties can nearly eliminate employees' propensity to access unnecessary information, reducing firm's risk. However, simple penalties are not sufficient to encourage employees to access the information required to create value. Rather, we show that bonus incentives tied to firm performance can improve outcomes for both firm and employees. We also examined how these results are linked to firm audit capability and showed that audit quality can reduce the need for incentives. The trade-off between investments to improve audit capability and the corresponding reduction in incentive payouts is an area of ongoing research.

Our analysis provides many interesting insights into the implementation challenges of access governance with escalation.

1. Audit quality is an important element of our governance scheme. Without the ability to catch cheaters, firms are better-off moving towards a more traditional 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 not



(a) The Optimal Regular Access

(b) The Optimal Bonus Rate

Figure 9: The Optimal Regular Access and Bonus Rate with Different Private Benefit. $A = 2, \gamma = 0.5, t = s = 9, \beta = 1, \varepsilon = 1, B = 13$

technologically or financially feasible in most cases. Our work shows that bonus schemes can counteract audit imperfection, making the escalation strategy desirable even in cases with significant audit error.

2. 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 [Johnson and Goetz, 2007].

3. Escalation must be done within the allowable zone dictated by regulatory requirements. Some data or applications cannot be made available through an escalation scheme.

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

5. The value of the information governance system with escalation also includes the possibility that the firm learns the dynamics of the business environment from employees. Sometime the firm is unaware of potential business opportunities simply because employees forwent

them. The escalation scheme creates an implicit communicate 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.

References

[Antle and Eppen, 1985] Antle, R. and Eppen, G. D. (1985). Capital rationing and organizational slack in capital budgeting. Management Science, 31(2):163–174.

[Arrow, 1985] Arrow, K. J. (1985). Principals and Agents: The Structure of Business, chapter The Economics of Agency, pages 37–53. Harward Business School Press, Boston, MA.

[Aveksa, 2007] Aveksa (2007). Enterprise roles-based access governance. Technical report, White Paper.

[Baiman, 1990] Baiman, S. (1990). Agency research in managerial accounting: A second look. Accounting Organizations and Society, 15(4):341–371.

[Baker and Freeland, 1972] Baker, N. R. and Freeland, J. R. (1972). Structuring information flow to enhance innovation. Management Science, 19(1):Theory Series, 105–116.

[Baron and Besanko, 1984] Baron, D. P. and Besanko, D. (1984). Regulation, asymmetric information, and auditing. The RAND Journal of Economics, 15(4):447–470.

[Dye, 1986] Dye, R. A. (1986). Optimal monitoring policies in agencies. The RAND Journal of Economics, 17(3):339–350.

[Ferreira et al., 2006] Ferreira, A., Cruz-Correia, R., Antunes, L., Farinha, P., Oliveira-Palhares, E., Chadwick, D., and Costa-Pereira, A. (2006). How to break access control in a controlled manner. In Proceedings of the 19th IEEE Symposium on Computer-Based Medical Systems (CBMS'06), pages 847–854.

[Goetz and Johnson, 2007] Goetz, E. and Johnson, M. E. (2007). Security through information risk management. I3P Technical Report. Dartmouth College, http://mba.tuck.dartmouth.edu/digital/Programs/CorporateEvents/CISO2007/Overview.pdf.

[Harris et al., 1982] Harris, M., Kriebel, C., and Raviv, A. (1982). Asymmetric information, incentives and intrafirm resource allocation. Management Science, 28(6):604–620.

[Harris and Raviv, 1979] Harris, M. and Raviv, A. (1979). Optimal incentive contracts with imperfect information. Journal of Economic Theory, 20:231–259.

[Harris and Raviv, 1996] Harris, M. and Raviv, A. (1996). The capital budgeting process: Incentives and information. Journal of Finance, 51(4):1139–1174.

[Holmstrom, 1979] Holmstrom, B. (1979). Moral hazard and observability. Bell Journal of Economics, 10(1):74–91.

[Johnson and Goetz, 2007] Johnson, M. E. and Goetz, E. (2007). Embedding information security risk management into the extended enterprise. IEEE Security and Privacy, 5(3):16–24.

[Jolly, 2008] Jolly, D. (2008). Fraud costs french bank $7.1 billion. New York Times.

[Kannan and Telang, 2005] Kannan, K. and Telang, R. (2005). Market for software vulnerabilities? think again. Management Science, 51(5):726–740.

[Kim and Suh, 1992] Kim, S. K. and Suh, Y. S. (1992). Conditional monitoring policy under moral hazard. Management Science, 38(8):1106–1120.

[Krishnan and Zhu, 2006] Krishnan, V. and Zhu, W. (2006). Designing a family of development-intensive products. Management Science, 52(6):813–825.

[Lee et al., 2000] Lee, H. L., So, K. C., and Tang, C. S. (2000). The value of information sharing in a two-level supply chain. Management Science, 46(5):626–643.

[Motta, 1993] Motta, M. (1993). Endogenous quality choice: Price vs. quantity competition. Journal of Industry Economics, 41(2):113–131.

[Povey, 2000] Povey, D. (2000). Optimistic security: a new access control paradigm. In Proceedings of the 1999 Workshop on New Security Paradigms, pages 40–45. ACM Press.

[Rathnam et al., 1995] Rathnam, S., Mahajan, V., and Whinston, A. B. (1995). Facilitating coordination in customer support teams: A framework and its implications for the design of information technology. Management Science, 41(12):1900–1922.

[Rissanen et al., 2004] Rissanen, E., Firozabadi, S. B., and Sergot, M. (2004). Towards a mechanism for discretionary overriding of access control. In Proceedings of the 12th International Workshop on Security Protocols, Cambridge.

[Shavell, 1979] Shavell, S. (1979). Risk sharing and incentives in the principal and agent relationship. Bell Journal of Economics, 10.

[Townsend, 1979] Townsend, R. M. (1979). Optimal contracts and competitive markets with costly state verification. Journal of Economy Theory, 21.

[Tsai, 2001] Tsai, W. (2001). Knowledge transfer in intraorganizational networks: Effects of network position and absorptive capacity on business unit innovation and performance. The Academy of Management Journal, 44(5):996–1004.

[von Hippel, 1994] von Hippel, E. (1994). Sticky information and the locus of problem solving: Implications for innovation. Management Science, 40(4):429–439.

6 Appendix

Proof 1 *If $x \leq a + e - \varepsilon$, the first-order-condition (FOC) of (1) w.r.t. e is $b - \beta e - p = 0$. The escalated access level is given by $e = \frac{b-p}{\beta}$. The condition can be rewritten as $x \leq a + \frac{b-p}{\beta} - \varepsilon$.*

If $a + e - \varepsilon < x \leq a + e$, the FOC of (1) w.r.t. e is $b - \beta e = 0$. The escalated access level is given by $e = \frac{b}{\beta}$. The condition can be rewritten as $a + \frac{b}{\beta} - \varepsilon < x \leq a + \frac{b}{\beta}$.

If $a + e < x \leq a + e + \varepsilon$, the FOC of (1) w.r.t. e is $w + b - \beta e = 0$. The escalated access level is given by $e = \frac{w+b}{\beta}$. The condition can be rewritten as $\frac{w+b}{\beta} < x \leq a + \frac{w+b}{\beta} + \varepsilon$.

If $A \geq x > a + e + \varepsilon$, the FOC of (1) w.r.t. e is $w + b - \beta e + q = 0$. The escalated access level is given by $e = \frac{w+b+q}{\beta}$. The condition can be rewritten as $x > a + \frac{w+b+q}{\beta} + \varepsilon$.

Next we consider three ranges which are missing from the previous analysis: $a + \frac{b-p}{\beta} - \varepsilon < x \leq a + \frac{b}{\beta} - \varepsilon$, $a + \frac{w+b}{\beta} + \varepsilon < x \leq a + \frac{w+b+q}{\beta} + \varepsilon$ and $a + \frac{b}{\beta} < x \leq a + \frac{w+b}{\beta}$.

First we check the range $a+\frac{b-p}{\beta}-\varepsilon<x\leq a+\frac{b}{\beta}-\varepsilon$. *Suppose an employee claims the escalated access level as* $x+\varepsilon+e_1-a$ *instead of* $x+\varepsilon-a$. *The employee will choose* $x+\varepsilon-a+e_1$ *if* $w(x)+b(x+\varepsilon-a)-R(x+\varepsilon-a)<w(x)+b(x+\varepsilon-a+e_1)-R(x+\varepsilon-a+e_1)-p(e_1)$. *We then obtain* $x<a+\frac{b-p}{\beta}-\varepsilon-\frac{e_1}{2}$, *which is lower than the lower bound of the range. Thus,* $e\leq x+\varepsilon-a$. *Suppose an emplyee claims the escalated access level as* $x+\varepsilon-a-e_2$ *instead of* $x+\varepsilon-a$. *The employee will choose* $x+\varepsilon-a-e_2$ *if* $w(x)+b(x+\varepsilon-a)-R(x+\varepsilon-a)<w(x)+b(x+\varepsilon-e_2-a)-R(x+\varepsilon-e_2-a)$. *We then obtain* $x>a+\frac{b}{\beta}-\varepsilon+\frac{e_2}{2}$, *which is higher than the upper bound of the range. Thus,* $e\geq x+\varepsilon-a$. *Overall, we conclude* $e=x+\varepsilon-a$.

Second, we then check the range $a+\frac{w+b}{\beta}+\varepsilon<x\leq a+\frac{w+b+q}{\beta}+\varepsilon$. *Suppose an employeeclaims the escalated access level as* $x-\varepsilon-a-e_3$ *instead of* $x-a-\varepsilon$. *The employee will choose* $x-\varepsilon-a-e_3$ *if* $w(x-\varepsilon)+b(x-a-\varepsilon)-R(x-a-\varepsilon)<w(x-\varepsilon-e_3)+b(x-\varepsilon-a-e_3)-R(x-\varepsilon-a-e_3)-q(e_3)$. *We can obtain* $x>a+\frac{w+b+q}{\beta}+\varepsilon+\frac{e_3}{2}$, *which is higher than the upper bound of the range. Thus,* $e\geq x-a-\varepsilon$ *Suppose an emplyee claims the escalated access level as* $x-\varepsilon-a+e_4$ *instead of* $x-\varepsilon-a$. *The employee will choose* $x-\varepsilon-a+e_4$ *if* $w(x-\varepsilon)+b(x-\varepsilon-a)-R(x-\varepsilon-a)<w(x-\varepsilon+e_4)+b(x-\varepsilon+e_4-a)-R(x-\varepsilon+e_4-a)$. *We then obtain* $x<a+\frac{w+b}{\beta}+\varepsilon-\frac{e_4}{2}$, *which is lower than the lower bound of the range. Thus,* $e\leq x-\varepsilon-a$. *Overall, we conclude* $e=x-\varepsilon-a$.

Finally we consider the range $a+\frac{b}{\beta}<x\leq a+\frac{w+b}{\beta}$. *Suppose an employee claims the escalated access level as* $x+e_5-a$ *instead of* $x-a$. *The employee will choose* $x+e_5-a$ *if* $w(x)+b(x-a)-R(x-a)<w(x)+b(x+e_5-a)-R(x+e_5-a)$. *We then obtain* $x<a+\frac{b}{\beta}-\frac{e_5}{2}$, *which is lower than the lower bound of the range. Thus,* $e\leq x-a$. *Suppose an employee claims the escalated access level as* $x-e_6-a$ *instead of* $x-a$. *The employee will choose* $x-e_6-a$ *if* $w(x)+b(x-a)-R(x-a)<w(x-e_6)+b(x-e_6-a)-R(x-e_6-a)$. *We then obtain* $x>a+\frac{w+b}{\beta}+\frac{e_6}{2}$, *which is higher than the upper bound of the range. Thus,* $e\geq x-a$. *Overall, we conclude* $e=x-a$.

Proof 2 *Given the employee's escalation strategy, we can verify that when* $x\leq a+\frac{b}{\beta}$,$a+e>x$; *when* $a+\frac{b}{\beta}<x\leq a+\frac{w+b}{\beta}$, $a+e=x$ *and when* $a+\frac{w+b}{\beta}<x\leq A$, $a+e<x$.

Proof 3 *Differentiate (3) w.r.t. p is*

$$\begin{aligned} V_p' &= \gamma\left((B-w)\left(a+\frac{b-p}{\beta}-\varepsilon\right)-R_o(\varepsilon)\right)\frac{-1}{\beta}f(x)+\gamma\int_0^{a+\frac{b-p}{\beta}-\varepsilon}-t\left(a+\frac{b-p}{\beta}-x\right)\frac{-1}{\beta}f(x)\,dx \\ &\quad -\gamma\left((B-w)\left(a+\frac{b-p}{\beta}-\varepsilon\right)-R_o(\varepsilon)\right)\frac{-1}{\beta}f(x) \\ = &\quad \gamma\int_0^{a+\frac{b-p}{\beta}-\varepsilon} t\left(a+\frac{b-p}{\beta}-x\right)\frac{1}{\beta}f(x)\,dx \end{aligned}$$

Since $V_p' > 0$, the optimal p is given by

$$p = b \tag{5}$$

Differentiate (3) w.r.t. q is

$$\begin{aligned} V_q' &= (B-w)\left(a+\frac{w+b+q}{\beta}+\varepsilon-\varepsilon\right)\frac{1}{\beta}\frac{1}{A}-(B-w)\left(a+\frac{w+b+q}{\beta}\right)\frac{1}{\beta}\frac{1}{A} \\ &\quad +\int_{a+\frac{w+b+q}{\beta}+\varepsilon}^{A}\left((B-w)\frac{1}{\beta}\right)\frac{1}{A}dx \\ &= (B-w)\frac{1}{A\beta}\left(A-a-\frac{w+b+q}{\beta}-\varepsilon\right) \end{aligned}$$

Let $V_q' = 0$, we obtain $q = (A-a-\varepsilon)\beta - w - b$.

If $a+\frac{w+b}{\beta}+\varepsilon \le A$, the optimal q satisfies $q = (A-a-\varepsilon)\beta - w - b$. Otherwise, $q = 0$.

$$q = [(A-a-\varepsilon)\beta - w - b]^+ \tag{6}$$

Proof 4 *If $\varepsilon = 0$,*

$$
\begin{aligned}
V_{firm} &= \max_{a,w,p,q} Ba - \frac{1}{2}sa^2 \\
&\quad +\gamma \int_0^{a+\frac{b-p}{\beta}} \left((B-w)\, x - R_o \left(a + \frac{b-p}{\beta} - x \right) \right) f(x)\, dx \\
&\quad +\gamma \int_{a+\frac{b-p}{\beta}}^{a+\frac{b}{\beta}} (B-w)\, x f(x)\, dx \\
&\quad +\gamma \int_{a+\frac{b}{\beta}}^{a+\frac{b}{\beta}} \left((B-w)\, x - R_o \left(a + \frac{b}{\beta} - x \right) \right) f(x)\, dx \\
&\quad +\gamma \int_{a+\frac{b}{\beta}}^{a+\frac{w+b}{\beta}} (B-w)\, x f(x)\, dx \\
&\quad +\gamma \int_{a+\frac{w+b}{\beta}}^{a+\frac{w+b}{\beta}} (B-w) \left(a + \frac{w+b}{\beta} \right) f(x)\, dx \\
&\quad +\gamma \int_{a+\frac{w+b}{\beta}}^{a+\frac{w+b+q}{\beta}} (B-w)\, x f(x)\, dx \\
&\quad +\gamma \int_{a+\frac{w+b+q}{\beta}}^{A} (B-w) \left(a + \frac{w+b+q}{\beta} \right) f(x)\, dx \\
&\qquad\qquad w = 0
\end{aligned}
$$

The FOC of (4) w.r.t. w

$$
\begin{aligned}
V'_w &= \gamma \int_0^{a-\varepsilon} (-x) f(x)\, dx + \gamma \int_{a-\varepsilon}^{a+\frac{b}{\beta}-\varepsilon} (-x) f(x)\, dx + \gamma \int_{a+\frac{b}{\beta}-\varepsilon}^{a+\frac{b}{\beta}} (-x) f(x)\, dx \\
&\quad +\gamma \left((B-w) \left(a + \frac{w+b}{\beta} \right) \right) \frac{1}{\beta} f(x) + \gamma \int_{a+\frac{b}{\beta}}^{a+\frac{w+b}{\beta}} (-x) f(x)\, dx \\
&\quad +\gamma \left((B-w) \left(a + \frac{w+b}{\beta} \right) \right) \frac{1}{\beta} f(x) - \gamma \left((B-w) \left(a + \frac{w+b}{\beta} \right) \right) \frac{1}{\beta} f(x) \\
&\quad +\gamma \int_{a+\frac{w+b}{\beta}}^{a+\frac{w+b}{\beta}+\varepsilon} \left(- \left(a + \frac{w+b}{\beta} \right) + (B-w) \frac{1}{\beta} \right) f(x)\, dx \\
&\quad -\gamma \left((B-w) \left(a + \frac{w+b}{\beta} + \varepsilon - \varepsilon \right) \right) \frac{1}{\beta} f(x) + \gamma \int_{a+\frac{w+b}{\beta}+\varepsilon}^{A} (-(x-\varepsilon)) f(x)\, dx \\
&= 0
\end{aligned}
$$

The SOC of (4) satisfies $-\frac{2\gamma\varepsilon}{\beta} < 0$. The optimal rate is given by.

$$
w = \left[\frac{\frac{1}{\beta}(B-b)\varepsilon - \varepsilon a - \frac{1}{2}(A-\varepsilon)^2}{2\varepsilon\frac{1}{\beta}} \right]^+ \tag{7}
$$

The condition is $a+\frac{w+b}{\beta}+\varepsilon \leq A$.

If $a+\frac{w+b}{\beta}+\varepsilon > A$, *The optimization problem becomes*

$$\begin{aligned} V_{firm} &= \max_{a,w} Ba - R_s(a) \\ &+\gamma \int_0^{a-\varepsilon} ((B-w)x - R_o(a-x)) f(x)\,dx + \gamma \int_{a-\varepsilon}^{a+\frac{b}{\beta}-\varepsilon} (B-w)x - R_o(\varepsilon) f(x)\,dx \\ &+\gamma \int_{a+\frac{b}{\beta}-\varepsilon}^{a+\frac{b}{\beta}} \left((B-w)x - R_o\left(a+\frac{b}{\beta}-x\right)\right) f(x)\,dx + \gamma \int_{a+\frac{b}{\beta}}^{a+\frac{w+b}{\beta}} (B-w)xf(x)\,dx \\ &+\gamma \int_{a+\frac{w+b}{\beta}}^{A} \left((B-w)\left(a+\frac{w+b}{\beta}\right)\right) f(x)\,dx \end{aligned} \tag{8}$$

Differentiate (8) w.r.t. w

$$\begin{aligned} V'_w &= \gamma \int_0^{a-\varepsilon} (-x) f(x)\,dx + \gamma \int_{a-\varepsilon}^{a+\frac{b}{\beta}-\varepsilon} (-x) f(x)\,dx + \gamma \int_{a+\frac{b}{\beta}-\varepsilon}^{a+\frac{b}{\beta}} (-x) f(x)\,dx \\ &+\gamma \left((B-w)\left(a+\frac{w+b}{\beta}\right)\right)\frac{1}{\beta} f(x) + \gamma \int_{a+\frac{b}{\beta}}^{a+\frac{w+b}{\beta}} (-x) f(x)\,dx \\ &-\gamma \left((B-w)\left(a+\frac{w+b}{\beta}\right)\right)\frac{1}{\beta} f(x) \\ &+\gamma \int_{a+\frac{w+b}{\beta}}^{A} \left(-\left(a+\frac{w+b}{\beta}\right) + (B-w)\frac{1}{\beta}\right) f(x)\,dx \end{aligned}$$

$$w = -\frac{2\beta}{3}\left(a+\frac{b}{\beta}-A-\frac{B}{2\beta}\right) + \frac{\beta}{3}\sqrt{\left(a+\frac{b}{\beta}-A+\frac{B}{\beta}\right)^2 + 3A^2} \tag{9}$$

The SOC of (8) w.r.t. w *is* $2\left(a+\frac{w+b}{\beta}-A\right)-\frac{B-w}{\beta} < 0$. *(9) gives the maximal value.*

Proof 5 *The FOC of (4) w.r.t. a*

$$\begin{aligned}
V_a' &= B - sa \\
&\quad +\gamma\left((B-w)(a-\varepsilon) - R_o(a-(a-\varepsilon))\right) f(x) + \gamma\int_0^{a-\varepsilon} -t(a-x) f(x)\,dx \\
&\quad +\gamma\left((B-w)\left(a+\frac{b}{\beta}-\varepsilon\right) - R_o(\varepsilon)\right) f(x) - \gamma\left((B-w)(a-\varepsilon) - R_o(\varepsilon)\right) f(x) \\
&\quad +\gamma\left((B-w)\left(a+\frac{b}{\beta}\right) - R_o\left(a+\frac{b}{\beta}-\left(a+\frac{b}{\beta}\right)\right)\right) f(x) \\
&\quad -\gamma\left((B-w)\left(a+\frac{b}{\beta}-\varepsilon\right) - R_o\left(a+\frac{b}{\beta}-\left(a+\frac{b}{\beta}-\varepsilon\right)\right)\right) f(x) \\
&\quad +\gamma\int_{a+\frac{b}{\beta}-\varepsilon}^{a+\frac{b}{\beta}} -t\left(a+\frac{b}{\beta}-x\right) f(x)\,dx + \gamma(B-w)\left(a+\frac{w+b}{\beta}\right) f(x) - \gamma(B-w)\left(a+\frac{b}{\beta}\right) f(x) \\
&\quad +\gamma\left((B-w)\left(a+\frac{w+b}{\beta}\right)\right) f(x) - \gamma(B-w)\left(a+\frac{w+b}{\beta}\right) f(x) + \gamma\int_{a+\frac{w+b}{\beta}}^{a+\frac{w+b}{\beta}+\varepsilon} (B-w) f(x)\,dx \\
&\quad -\gamma\left((B-w)\left(a+\frac{w+b}{\beta}+\varepsilon-\varepsilon\right)\right) f(x) \\
&= 0
\end{aligned}$$

$$a = \frac{A}{\gamma t}\left(-s + \sqrt{s^2 + \frac{2}{A}\gamma t\left(B + (B-w)\gamma\frac{\varepsilon}{A}\right)}\right) \tag{10}$$

$$a = -\frac{\gamma\varepsilon}{A\sqrt{s^2 + \frac{2}{A}\gamma t\left(B + (B-w)\gamma\frac{\varepsilon}{A}\right)}} \tag{11}$$

The SOC of (4) w.r.t a is $-s - \frac{1}{A}\gamma t a < 0$. *Thus, the access level is given by (10).*

Solve (7) into (10), we obtain the close form solution of the regular access level,

$$a_1^* = \frac{-(2As - \gamma\beta\varepsilon) + \sqrt{(2As-\gamma\beta\varepsilon)^2 - 4\gamma t\left(-2\gamma\varepsilon B - 2AB + \gamma(B-b)\varepsilon - \gamma\beta\frac{1}{2}(A-\varepsilon)^2\right)}}{2\gamma t} \tag{12}$$

Substitute (12) into (7) and (6), we can obtain the optimal bonus rate and the penalty for underentitlement.

If $a^* + \frac{w^*+b}{\beta} + \varepsilon > A$, *The optimization problem is represented by (8)*

The FOC of (8) w.r.t. a

$$\begin{aligned}
V_a' &= B - sa \\
&\quad +\gamma\left((B-w)(a-\varepsilon) - R_o(a-(a-\varepsilon))\right) f(x) + \gamma\int_0^{a-\varepsilon}(-t(a-x))\, f(x)\, dx \\
&\quad +\gamma\left((B-w)\left(a+\frac{b}{\beta}-\varepsilon\right) - R_o(\varepsilon)\right) f(x) - \gamma\left((B-w)(a-\varepsilon) - R_o(\varepsilon)\right) f(x) \\
&\quad +\gamma\left((B-w)\left(a+\frac{b}{\beta}\right) - R_o\left(a+\frac{b}{\beta}-\left(a+\frac{b}{\beta}\right)\right)\right) f(x) \\
&\quad -\gamma\left((B-w)\left(a+\frac{b}{\beta}-\varepsilon\right) - R_o\left(a+\frac{b}{\beta}-\left(a+\frac{b}{\beta}-\varepsilon\right)\right)\right) f(x) \\
&\quad +\gamma\int_{a+\frac{b}{\beta}-\varepsilon}^{a+\frac{b}{\beta}}\left(-t\left(a+\frac{b}{\beta}-x\right)\right) f(x)\, dx \\
&\quad +\gamma(B-w)\left(a+\frac{w+b}{\beta}\right) f(x) - \gamma\left((B-w)\left(a+\frac{b}{\beta}\right)\right) f(x) \\
&\quad -\gamma(B-w)\left(a+\frac{w+b}{\beta}\right) f(x) + \gamma\int_{a+\frac{w+b}{\beta}}^{A}(B-w)\, f(x)\, dx \\
&= 0
\end{aligned}$$

$$a_2 = \frac{-(As+\gamma(B-w)) + \sqrt{(As+\gamma(B-w))^2 + 2\gamma t\left(\gamma(B-w)\left(A-\frac{w+b}{\beta}\right)+AB\right)}}{\gamma t} \tag{13}$$

The SOC of (8) w.r.t. a, $-As-\gamma ta-\gamma(B-w)<0$. (13) is the unique solution. Solve (9) and (13) together, we can get the optimal solutions.

Proof 6 *Differentiate (4) w.r.t. w and a*

$$V_{wa}'' = -\frac{1}{A}\varepsilon < 0$$

Differentiate (8) w.r.t. w and a

$$V_{wa}'' = -\frac{1}{A}\left(A-a-\frac{w+b}{\beta}\right) - \frac{1}{A\beta}(B-w) < 0$$

Thus, w and a are substitutes.

Proof 7 *Differentiate w w.r.t. a*

$$w_a' = -\frac{\beta}{2}$$

$$w_a' = \frac{\beta}{3}\left(-2 + \frac{\left(a+\frac{b}{\beta}-A+\frac{B}{\beta}\right)}{\sqrt{\left(a+\frac{b}{\beta}-A+\frac{B}{\beta}\right)^2+3A^2}}\right) < 0$$