The Journal of Contemporary Issues in Business and Government
2010 Volume 16, Number 1, pp 1-25

Thrusters, Scoopers, Scroungers and Squirrels: A Taxonomy of Public Sector Audit and Accountability Mechanisms

Stuart Kells[1]
Monash University

Abstract

The concept of public sector accountability is attracting a great deal of attention both inside and outside the academy. Performance auditing is one of a large and growing number of mechanisms that are used to enhance accountability. Though it is an important and prominent feature of public administration in many countries, performance auditing is often said to be difficult to define. Kells and Hodge (2009) proposed a framework for defining performance auditing, which they then used to study other types of accountability and review mechanisms, including management audits, whistleblower laws, freedom of information laws, open book policies and citizen engagement models. This paper formalizes and generalizes Kells and Hodge's framework. After expressing the framework using set function notation and concepts from game theory, the paper then applies the elements of the framework to develop a general taxonomy of audit and accountability mechanisms. The taxonomy is presented graphically, and then in the form of a new terminology of mechanism types. The paper concludes with directions for future research regarding the design and evaluation of accountability mechanisms.

Introduction

The International Congress of Supreme Audit Institutions (INCOSAI) has defined *performance audit* as an 'audit which is concerned with the evaluation of economy, efficiency and effectiveness of public sector management' (INCOSAI, 1986). The US Comptroller General (1994, cited by Brooks, 1996, p. 17) has offered the alternative definition of *performance audit* as:

> *an objective and systematic examination of evidence for the purpose of providing an independent assessment of the performance of a government organization, program, activity, or function in order to provide information to improve public accountability and facilitate decision-making by parties with responsibility to oversee or initiate corrective action.*

Performance auditing is widely practiced throughout the world and it is common for public audit offices to spend the majority of their time conducting performance audits. For details of the history and global spread of performance auditing, see Dewar (1985a), Kells and Hodge (2009) and Yamamoto and Watanabe (1989).

Despite the apparently straightforward definitions provided by INCOSAI and the Comptroller General, performance auditing is often said to be a vague concept that is difficult to define. Authors have claimed that the concept of performance auditing is not well or widely understood (Barzelay, 1996), that its precise meaning is unresolved (Barzelay, 1997), that its 'nuts and bolts' are hotly debated (Power, 2000, p. 112), or that it is 'the oddball in the auditing family' (Lindeberg, 2007, p. 338). Authors have also noted that the nature of performance auditing is ambiguous (Lindeberg, 2007) or remains an open question (Keen, 1999), and that it is a 'continually unfolding drama' (Guthrie & Parker, 1999, p. 329).

A lack of clarity about the nature and definition of performance auditing is a barrier to progress in the field of performance audit research, and in the wider field of public accountability.

To help resolve some of the apparent confusion, Kells and Hodge (2009) reviewed previous definitions of performance auditing and, after adopting a heuristic approach to examine the adequacy and serviceability of those definitions, proposed a new definition of performance auditing. They then used the definition to compare various types of accountability and review mechanisms, including management audits, gateway reviews, whistleblower laws, freedom of information laws and open book policies.

This paper formalizes Kells and Hodge's definitional framework using set function notation, then applies elements of the framework to develop a general taxonomy of audit and accountability tools. The taxonomy is expressed graphically, and then in the form of a new terminology of accountability mechanism types.

Formalizing and generalizing the framework is important for two reasons. First, it will enable the framework to be further developed and more precisely tested. Secondly, and more importantly, it holds the promise of increasing clarity, and assisting innovation, in the wider field of public accountability. Contemporary interest in public accountability is intense, such that ours has been called the era of accountability. In this era, appetites for new and better ways to achieve greater accountability are insatiable. For general discussions of accountability concepts, see Hodge (2009), Bovens (2006) and Normanton (1966).

The paper is organized as follows. Section Two introduces the definitional framework, before Section Three formalizes the framework. Section Four provides a taxonomy of accountability mechanisms, and Section Five concludes the paper. The paper bridges a number of different literatures, including those of audit and accountability, electronic government, citizen engagement and investigative journalism.

The Definitional Framework

The five elements of Kells and Hodge's definitional framework for performance auditing are summarized in Table 1, and are examined in more detail in this section.

Kells and Hodge (2009) defined auditor *independence* with regard to the auditor's relationship to the auditee and the authorizer of the audit. If an auditor embarking on a performance audit of an organization requires the permission of the organization's management to conduct the audit, they concluded, then the auditor is not independent. The auditor is reporting *to* management, not *on* management (Dewar, 1985b). If the auditor is beholden to management, the decisions of management enter the *decision function* of the auditor (this is further explored below).

Table 1: A Framework of Definitional Elements for Performance Auditing

Element	Description	Relevance
Independence	The auditor is independent of the auditee. The auditor is an outsider *vis a vis* the audited organization.	Auditor's incentives.
Authorization	The auditor is authorized by an authority higher than the auditee to undertake the audit.	Auditor's incentives. Also, the authorizer may bind itself to not revoke the authorization.
Discovery	The auditor enters the auditee organization (physically or virtually) and achieves access to information that would otherwise be private.	Auditor's information sets and authorization.
Synthesis	The auditor makes findings and reaches conclusions, which may or may not involve analysis. Some or all of the discovered information is expressed in a new way.	Auditor's authorization. The scope of the findings and conclusions depends on the scope of authorization.
Publication	Some or all of the auditor's findings and conclusions are published in some form. The public achieves access to synthesized information that would otherwise be private.	Relevant to the auditee's incentives, public information sets and the auditor's authorization.

Source: Kells and Hodge (2009).

As a minimum, independence requires that the auditor's *authorization* is conferred by an authorizer at a higher level in the authority chain than the audited organization. The higher authorizer might be the audited organization's board or owner, the government, the legislature or the judiciary. The auditor's *decision function* would therefore be independent of the decisions of the organization's management. A particularly high level of auditor independence exists where the permission to audit is irrevocable with regard to the auditor's decisions to enter, form findings and conclusions, and publish a report. This level of independence requires a decision by the authorizer to ‘bind its own hands’ with regard to directing and terminating the auditor.

The concept of *discovery* relates to the information available to the auditor. As a consequence of discovery, the auditor achieves access to information that would normally be barred to it, and which continues to be barred to other outsiders.

The concept of *synthesis* acknowledges that performance auditing involves some form of transformation of the information discovered by the auditor. The transformation may involve analysis of the information, or selecting some information for reporting or tabulation, or otherwise using the information to form findings or express the information in a new way.

Kells and Hodge (2009) argued that *publication* of the audit results was a fundamental aspect of performance auditing. In their framework, the publication of some or all of the audit results distinguishes performance auditing from several other activities that resemble performance auditing in method, but that do not generate the accountability effects associated with publication. The publication of the auditor’s findings and conclusions changes the status of at least some of the information that the auditor discovered, and it affects the information sets of the wider audience.

Formalizing the Framework

This section presents a general, formal representation of Kells and Hodge’s (2009) definitional framework, using set function notation. The key participants in the framework are the ‘auditor’, the ‘auditee’ and the ‘authorizer’. For the purposes of the present paper, the term ‘auditor’ is used in a broad sense to mean the person, team or organization that undertakes the audit or review by gathering information from within the audited organization, analyzing the information and (using the concept of ‘synthesis’ as it was defined above) synthesizing the information in preparation for publication.

The ‘audited organization’ may be a business unit of a larger organization, or a project or program, or some other institutional form. For this paper, the critical characteristic of the organization is that its boundaries can be defined with regard to the confidentiality of information, and access to that information.

The term ‘auditee’ refers to the management of the audited organization. The ‘authorizer’ of the audit is the party who permits the auditor to undertake the audit. For much of this paper, the auditee is assumed to be in a subsidiary position to the authorizer.[2] Examples of the relationship of authorizer to auditee include that between an organization’s board and management; between the owner and the management; between a regulator and the regulatee; between the executive branch of government and a government agency; and between the legislature and a government agency.[3]

Independence

To define independence formally, it is useful to first consider a situation in which independence is absent. Such a situation is shown in equation (1), which represents the decision function of an auditor who is not independent of the auditee or the authorizer of the audit. The decision function of the auditor (D_{auditor}) refers to the actions and decisions taken by the auditor in relation to whether and how to conduct the audit, and the bases and incentives that inform and drive those decisions and actions. The auditor’s decision function can also be thought of as the ‘entry function’.

(1) Not independent:

$$D_{\text{auditor}} = f\{D_{\text{authoriser}}, D_{\text{auditee}}, [\textit{other factors – auditor}]\}$$

$$\text{where: } D_{\text{authoriser}} = f\{D_{\text{auditee}}, [\textit{other factors – authorizer}]\}$$

In equation (1), the general function $f\{\ \}$ represents how the actions and decisions of the auditor depend upon the actions and decisions of the authorizer, the auditee and other factors. For the auditor, the *other factors* include the other imperatives and motivations facing the auditor, and the auditor’s skills, knowledge, information and beliefs. The other factors do not include decisions made by the authorizer or the auditee.

Equation (1) shows that the authorizer has its own decision function, which depends on the actions and decisions of the auditee, and other factors. For the authorizer, the *other factors* again include wider imperatives and motivations, which affect the authorizer’s decisions about whether to permit the auditor to access information, the extent of the access that is permitted, and what the auditor may do after the access is granted.

In this representation, the decisions of the auditee enter the auditor's decision function in two ways: directly, and also indirectly via the authorizer's decision function. The auditee's decision to enter the organization and to access information depends on the authorizer's decision and, separately, the auditee's decision. The auditee can therefore 'block' the auditor, notwithstanding the permission from the authorizer. In situations where independence is not present, the authorizer and the auditee could coincide – that is, they could be the same person or organization.

Let us consider instead situations of auditor independence. In such situations, the auditee and the authorizer are clearly separate, and the auditee is in a subsidiary relationship to the authorizer, of the type outlined above.

First of all, the auditor may have a level of independence such that the auditee cannot block the auditor's entry into the organization and its access to information. This (low) level of independence is depicted in equation (2).

(2) A low level of independence:

$$D_{\text{auditor}} = f\{D_{\text{authoriser}}, [\textit{other factors – auditor}]\}$$

$$\text{where: } D_{\text{authoriser}} = f\{D_{\text{auditee}}, [\textit{other factors – authorizer}]\}$$

Note that in equation (2) the decisions of the auditee still enter the auditor's decision function, but this time only indirectly, via the authorizer.

In the framework of Kells and Hodge (2009), independence can only be present where the authorizer and the auditee do not coincide, where they are not the same person or organization. Rather, the auditee is subsidiary to the authorizer, which means that the authorizer can direct the auditee, but the auditee cannot direct the authorizer. Because of this characterization of the relationship between the authorizer and the auditee, the authorizer can choose not to act on input or requests from the auditee; the auditee may be able to influence the authorizer with regard to the scope and terms of authorization for the audit, or whether authorization is granted at all, but the auditee cannot direct that the authorization be revoked, and cannot direct the authorizer to form the authorization in any particular way. The interaction between the auditee and the auditor is mediated by the authorizer.

A still higher level of independence for the auditor is possible, and is shown in equation (3).

(3) A high level of independence:

$$D_{\text{auditor}} = f\{[\textit{other factors}] \mid \textit{authorizer establishes limits on the auditor's conduct; auditor remains within those limits}\}$$

Here, the concept of auditor independence coincides with the auditor's decision function being mathematically independent of the decision functions of the authorizer and the auditee.

In the case of this high level of independence, the authorizer binds its own hands with regard to the decisions and actions of the auditor. In other words, the authorizer unilaterally decides to limit its own ability to guide, direct or restrict the auditor. There are likely to be limits on the extent to which the authorizer's hands are tied. For example, the authorizer may only continue to tie its own hands if the auditor remains within the scope of an explicit audit mandate. Accordingly, in this representation, the *other factors* for the auditor would include the auditor's judgements about how to operate within the mandate established by the authorizer. This is shown in equation (3), where the relationship between the auditor's decision function and the other factors (which exclude $D_{\text{authoriser}}$ and D_{auditee}) is conditional upon the authorizer establishing limits on the auditor's conduct and activities, and the auditor remaining within those limits.

Because of the relationship between the authorizer and auditee, the authorizer tying its own hands is sufficient for the auditor to carry out its work without blockage from the auditee. The auditee, at a subsidiary level to the authorizer, is bound by the authorizer's decision to tie its own hands.

Authorization

The concept of authorization was shown formally above, where, in all three cases (i) not independent; (ii) low level of independence; and (iii) high level of independence) the actions and decisions of the authorizer influenced those of the auditor. Even in the third case, where the authorizer had tied its own hands with regard to whether to revoke authorization, it was still the case that the auditor's work was dependent on a decision of the authorizer. Kells and Hodge (2009) contrasted authorized audit with other types of unauthorized access to information, such as leaks and computer hackers. These are discussed further under ‘Taxonomy of Accountability Mechanisms’ below.

Discovery

The formal representation of the concept of ‘discovery’ depends on the ‘information set’ construct. From game theory, the information set is the totality of information available to a player at any point in a game. When an auditor enters an organization and achieves access to information, the auditor’s information set changes. The auditor’s information set before being given access to the audited organization differs from the auditor’s information set afterward.

The change in the auditor’s information set is a function of what was available for discovery in the organization, and the methods used by the auditor to select information (such as random sampling, or other sampling methods). The auditor will discover a subset of the available information. That subset may be a small part of the information available to be discovered in the audited organization (narrow sampling), it may approach the whole of the information available for discovery there (very wide sampling), or the subset may lie somewhere between these extremes.

$$\text{(4)} \qquad I_{\text{auditor t2}} = f\{I_{\text{auditor t1}}, I_{\text{org}}, [\textit{other discoveries}]\}$$

I_{org} is the quantum of discoverable information in the organization. It includes documentation, systems, assets, funds held, and tacit knowledge possessed by the organization’s personnel. The time period before the audit is t1, and the time period after the audit is t2. The difference between the auditor’s information set before and after the audit is $f\{I_{\text{org}}\}$, plus any other discoveries the auditor makes outside the organization between the two time periods. In this context, the function $f\{\ \}$ (the ‘discovery function’) is of a different functional form to the decision functions of the auditor, authorizer and auditee.

Synthesis

The concept of ‘synthesis’ refers to the fact that the auditor, after making discoveries, will transform the discovered information in some way. For example, the auditor might produce an audit report, which contains ‘boiled down’ findings, or which selects the most important findings for reporting. There is a very wide range of things an auditor might do with the discovered information. To represent that range, a general ‘synthesis function’ or ‘transformation function’ may be used, as follows:

$$(5) \qquad S_{\text{auditor}} = f\{I_{\text{auditor t2}}, [\textit{other input}]\}$$

$$\text{where: } I_{\text{auditor t2}} = f\{I_{\text{auditor t1}}, I_{\text{org}}, [\textit{other discoveries}]\}$$

The synthesis function shows that, in reaching findings and preparing a report, the auditor uses its existing knowledge, and information from other sources, as well as information discovered in the audited organization. The auditor’s knowledge may include generic analysis templates, performance benchmarks, and preconceptions. The auditor may also make pertinent new discoveries outside the organization, such as information from clients.

Again, the functional form in the synthesis function differs from those in the decision functions and the discovery function above. I_{org} (the quantum of information in the organization) is not necessarily exactly the same as I_{auditee} (the information and knowledge of the auditee), though these may coincide, and it is the case that $I_{\text{auditee}} = f\{I_{\text{org}}, [\textit{other information}]\}$.

Publication

The publication of the auditor’s findings affects the ‘public information set’, which is the quantum of information available to everyone. The public information set after the audit findings are reported (in t2) is a function of: the public information set before the findings were published (t1); the synthesized discoveries of the auditor; and any other information that is published or disclosed between t1 and t2.

$$(6) \qquad I_{\text{public t2}} = f\{I_{\text{public t1}}, S_{\text{auditor}}, [\textit{other publications and disclosures}]\}$$

$$\text{where: } S_{\text{auditor}} = f\{I_{\text{auditor t1}}, I_{\text{org}}, [\textit{other discoveries}]\}$$

$I_{\text{public t2}}$ is a function of I_{org} only indirectly, via the lens of the auditor’s synthesis. With respect to the audited organization and the information therein, the information set $\{I_{\text{auditor t1}}\}$ is a subset of $\{I_{\text{public t1}}\}$.

A Taxonomy of Accountability Mechanisms

The previous section formally presented the five elements of Kells and Hodge's (2009) performance auditing definitional framework. This section uses the framework to categorize ten types of accountability mechanism. The types are described in Table 2, and relevant references are provided.

Table 2: Ten Accountability Mechanisms

Accountability Mechanism	**Description**	**Selected References**
Performance Audit	An independent public audit office is authorized to discover, synthesize and publish information that would otherwise be confidential.	Yamamoto and Watanabe (1989), Barzelay (1996), Shand and Anand (1996), Barzelay (1997), Pollitt *et al.*, (1999), Kells and Hodge (2009)
Management Audit	An auditor is engaged to provide findings, analysis and advice to an organization's management.	Adams (1986), Vinten (1996), Funnell (1998), Burrowes and Persson (2000), Flesher *et al.*, (2003)
Open Book Policies	An organization elects to make proactive disclosure of information at a level beyond standard or baseline disclosures such as those required for annual reporting.	Case (1995), Case (1998), Dunleavy and Margetts (2000), Metaxiotis and Psarras (2004)
Whistleblower Laws	In cases such as serious misconduct, an organization's staff are authorized to disclose information that would ordinarily be confidential.	Brewer and Selden (1998), Jubb (1999)
Freedom of Information Laws	Members of the public are authorized to seek disclosure of information from government agencies,	Piotrowski and Rosenbloom (2002), Hazell (2007)

	who have an obligation to disclose except in defined circumstances (such as threats to the public interest or commercial in confidence obligations).	
Investigative Journalism	Media organisations and media professionals use a combination of authorized and unauthorized means to uncover and publicize fraud, misconduct or other forms of gross underperformance.	Ettema and Glasser (1998), McMillan and Zoido (2004)
Citizen Engagement Models	Citizens and local resident groups audit government programs and performance either officially or based on documents obtained informally from officials.	Goetz and Jenkins (2001), Government 2.0 Taskforce (2009)
Leaks from Organisations	A person within an organization makes an unauthorized disclosure of information to a third party, or to the public at large.	Katz (1976), Tant (2005)
Hackers[4]	External parties achieve unauthorized access to an organization’s confidential information, such as by exploiting weaknesses in computer system security.	Government 2.0 Taskforce (2009), websites and blogs such as hackernews.com and hackingcongress.org
Bounty Hunters	Parties who specialize in identifying, primarily for private reward, instances of fraud, criminal conduct or gross underperformance. Bounty hunters develop expertise to synthesize	Toma (1989), Frey (1994), Braithwaite (2007)

	information and identify fraud etc.	

Source: Original table

These ten mechanisms are all ‘accountability mechanisms’ because they all relate in one way or another to ‘answering for one’s actions’ (Ott & Russell, 2001, cited by Hodge, 2009). All ten involve some form of shining a light on activities that otherwise would be secret or only partially known. Each of them involves either the provision of information and analysis to owners, boards or management, who are in a position to act on the information to address shortcomings or improve performance, or the (potential) provision of information to the wider community, members of which are in a position to pressure organisations to make meritorious changes.

Graphical Representation of the Taxonomy

Depicting concepts and activities graphically can facilitate the identification of patterns, differences and commonalities that may not be apparent from other forms of representation. There are a number of ways in which the analysis in Section Three can be shown graphically. One approach is to conceive of elements of the definitional framework as ‘spaces’ that coincide with particular information sets, or spaces in which particular activities occur or particular participants dwell. Different types of accountability mechanism, including performance auditing, can then be mapped across the conceptual spaces.

For example, it is possible to conceive of a space that coincides with the information set I_{org}. The people who have access to the information in I_{org} as part of their everyday work can be thought of as ‘insiders’ in this space. In contrast, there are ‘outsiders’ who, in their everyday work, do not have access to I_{org}, and therefore do not dwell in the corresponding space. For these people to have access to the confidential information in I_{org}, something particular must happen. For the present purposes, that ‘something’ is the activation of some form of accountability mechanism that gives the outsider access to the information in I_{org}.

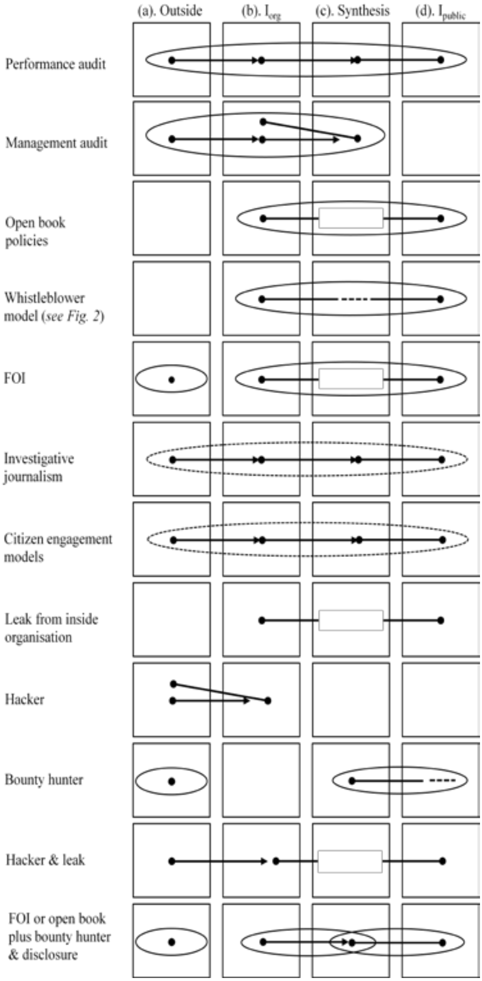
Staff within the organization have access to the information therein (I_{org}), but are bound by confidentiality obligations. These confidentiality obligations can be overridden by whistleblower laws, freedom of information laws, or decisions by managers or owners to unilaterally disclose information via an 'open book policy' or a similar mechanism.

Conceptually, another 'space' is the public domain that corresponds with the public information set, I_{public}. This is the destination for information that is published as a consequence of the activation of an accountability mechanism that involves publication. Recalling the idea of 'synthesis' of audit findings, it is also possible to conceive of a space in which, having entered I_{org}, an auditor or reviewer then undertakes the task of synthesizing its findings and conclusions.

Using this approach, four spaces have been defined. The four spaces correspond approximately to four parts of the definitional framework, namely independence (which is related to the 'outside' space), discovery (the I_{org} space), synthesis (the space in which synthesis occurs) and publication (the I_{public} space). Figure 1 shows the four spaces, and maps the ten accountability mechanisms from Table 2 across the spaces. The representation of accountability mechanisms in this way makes use of the fact that the different mechanisms share common elements, such as relationships with otherwise secret information within organisations, and relationships with the wider set of public information.[5]

As an example of the mapping method, consider the first row in the figure, which is performance auditing. Different aspects of performance auditing occupy all four spaces: the auditor comes from outside the organization (so it dwells initially in the 'outside' space); the auditor then achieves access to I_{org}; subsequently the auditor synthesizes the discovered information (in the 'synthesis' space); and finally the resulting findings and conclusions are published, entering I_{public}. The auditor's authorization to take these actions is shown in Figure 2 by the unbroken line that surrounds the actions taken by the auditor in each space.

Figure 1: Graphical Representation of Different Accountability Mechanisms



Source: Original figure

Figure 1 shows that a management audit by an independent auditor does not (typically) involve publication. Rather, after the findings and conclusions are synthesized, these are provided to the auditee (within I_{org})

for consideration and action. In contrast, a number of other mechanisms in Figure 1, such as open book policies, whistleblower models and freedom of information laws, result in changes to I_{public} as a result of transmitting information (in a synthesized or unsynthesised form) into the public domain.

Open book policies typically do not involve synthesis; rather, the information is released in an untransformed state. Accordingly, in Figure 1, open book policies are shown as not occupying the synthesis space. (Exceptions to this are possible, such as where only selected data are released.) In the case of whistleblower models, some involve synthesis, while others do not. This is shown in Figure 2, which depicts five different whistleblower models:

1. Disclosure directly to the public, without synthesis

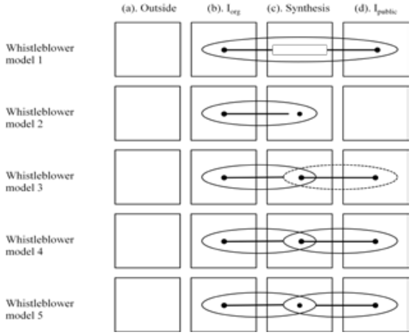
2. Disclosure to another party (eg. an Ombudsman), who synthesizes information but does not disclose it publicly

3. Disclosure to another party, who synthesizes information and has limited authorization to publish

4. Disclosure to another party, who synthesizes the information and has full authorization to publish

5. Disclosure to another party, who synthesizes the information, and then a third party is authorized to publicly disclose it (eg. a legislature).

Figure 2: Graphical Representation of Different Whistleblower Models



Source: Original figure

In Figure 1, investigative journalism and citizen engagement models occupy all the spaces that are occupied by performance auditing. The difference is that investigative journalists and participants in citizen engagement models use a variety of formal and informal, and lawful and unlawful, methods. As defined here, their activities are only partially authorized, and so are shown surrounded by a broken line in Figure 1. This indicates that the access achieved by these parties, and their actions to synthesize and publish information, may be open to legal or administrative challenge in a number of ways in which the analogous activities of an authorized performance auditor would not be.

The next types of parties shown in Figure 1, leakers and hackers, operate further outside the law than investigative journalists and participants in citizen engagement models. Leakers and hackers are shown as lacking both authorization and synthesis. As shown in the figure, the hacker enters the organization from the outside, then retreats once the information is obtained. In this representation, the hacker does not synthesize or publish the information discovered. In contrast, the leaker causes information to enter the public domain. Different combinations and permutations of these activities are of course possible, such as where hackers publish the information that they access. The penultimate row of Figure 1 shows a leaker and a hacker in combination, which results in information moving from I_{org} to I_{public}.

Another party shown in Figure 1 is the bounty hunter. As defined here, the bounty hunter is an outsider who does not achieve direct access to I_{org}. Rather, the bounty hunter gathers information from others in order to perform its synthesis function. Accordingly, the bounty hunter can have a complementary relationship with other accountability mechanisms. Figure 1 gives an example of this. The last row shows a combination of a bounty hunter and a party who is authorized to obtain information via FOI or due to an open book policy.

A New Vocabulary of Accountability Mechanisms

There are a number of recurring patterns in Figures 1 and 2. These indicate that it is possible to divide the various accountability mechanisms into various types and sub-groupings. One way of distinguishing types is to have regard for whether the ‘outside’ element (as defined here) is present. That element is not present in open book policies, whistleblower models, or in the case of a leak from within the organization. In these three instances, the information is ‘thrust outward’ from the organization. In contrast, other mechanisms, such as performance auditing, freedom of information, investigative journalism and citizen engagement models, begin with a party who is outside the organization, who then achieves access, and brings some of the discovered information into the light of day. A third mechanism, that of the bounty hunter, is different again. As defined here, the bounty hunter does not itself achieve access to the organization, but relies on others to provide the information that the bounty hunter can then synthesize, and perhaps publish.

On this dimension of categorization, therefore, the various mechanisms can be sorted into ‘thrusters’, ‘scoopers’ and ‘scroungers’, with the meanings as defined in Table 3. (The ‘squirrel’ type is discussed later in this section.)

Table 3: A Verbal Taxonomy of Accountability Mechanisms

Type	**Description**	**Examples**
Thrusters	Release of information is initiated from within the organization.	Whistleblower; open book policy; leak
Scoopers	A party comes from outside the organization, achieves access to information, and brings some of that information (possibly in synthesized form) into the public domain.	Performance auditing; investigative journalism; citizen engagement model
Scroungers	A party obtains (and possibly synthesizes) information from another party. The synthesizing party does not directly achieve access to the organization.	Bounty hunter
Squirrels	A party comes from outside the organization, achieves access to information, removes some of that information (possibly in synthesized form) but does not take the information into the public domain.	Management audit; hacker

Source: Original table

Another distinction that may be made is whether the mechanism involves authorization and, if so, the level of authorization. Performance auditors are 'authorized scoopers', in that their activities are fully authorized by the relevant legislature or audit mandate, whereas investigative journalists and citizen engagement models involve scooping with potentially less authorization. The combination of a hacker and a leaker is a fully unauthorized scooper. Likewise, there are authorized and unauthorized thrusters. Some types of whistleblowers are authorized to thrust information into the public domain (see Figure 2), whereas the internal staff member who leaks secrets is an unauthorized thruster. In principle, there are also unauthorized and authorized scroungers.

Figures 1 and 2 also suggest another distinction between mechanism types. Most of the mechanisms in the table involve publication, whereby information from I_{org} finds its way into I_{public}, in a synthesized or unsynthesized form. However, in some of the mechanisms, the information is discovered, and then squirreled away. The non-leaking hacker is an example, as is the model in Figure 2 in which whistleblowers make disclosures to a body that is not authorized to publish them, or a synthesized version of them. Another example is the management auditor which squirrels away its findings within the organization itself, in the form of unpublished reports to the auditee. Accordingly, another sub-category of accountability mechanism is the 'squirrel', as defined in Table 3. All other things equal, squirrels have a weaker impact on accountability than do non-squirrels, because the squirrel hides his nuts, rather than expose them to public scrutiny.

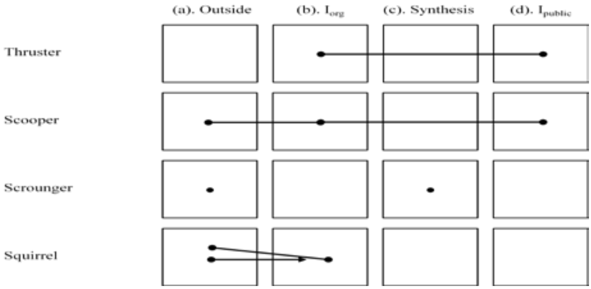
From this discussion, and Figures 1 and 2, it is possible to represent graphically what might be 'typical' or 'standard' types of the thruster, the scooper, the scrounger and the squirrel. These are shown in Figure 3.

As Figure 3 shows, the relationship between thrusters and scroungers is a symbiotic one. Thrusters are rich when it comes to access to information, but they are light on synthesis. Scroungers are the reverse; waiting patiently in the 'outside' space, they rely on others for information, and develop expertise in synthesis.

This representation offers potentially important insights into the design and evaluation of accountability mechanisms. With respect to design, for example, Figure 1 shows that several mechanisms and combinations of mechanisms share some substantive similarities.

Notwithstanding differences in authorization, it is clear that performance auditors, investigative journalists and citizen engagement models occupy the same accountability niche, and could be expected to have similar effects on the performance and accountability of the organisations they scrutinize.

Figure 3: ‘Standard’ Types of Thrusters, Scoopers, Scroungers and Squirrels



Source: Original figure

The last row in Figure 1 (the combination of a bounty hunter and an authorization to obtain information via FOI or an open book policy) has all the elements of a performance audit: independence, authorization, discovery, synthesis and publication. The difference between performance auditing and this combination of elements is that performance auditing is ‘vertically integrated’: the same person, team or organization undertakes the tasks of discovery, synthesis and publication. Despite this difference of integration, it is plausible that, because performance auditing and the combination of elements share all five substantive components in the definitional framework, these two alternatives would have the same impact on the accountability and performance of public organisations. This is an important conclusion with regard to assigning audit mandates, funding public audit offices, and making changes to other accountability and transparency mechanisms such as open book policies and freedom of information laws.

More generally, the visual tools presented here could be used to conceive of new accountability mechanisms that involve different combinations of the four spaces, and variations on the elements and activities in Figure 3. The tools could also be used to study other accountability mechanisms, such as Qui Tam laws.

Conclusion

This paper began with a discussion of definitions of performance auditing, and concluded with a taxonomy that has potentially much wider application in the analysis of accountability mechanisms. A method of graphically representing different accountability mechanisms was presented, and a new terminology of accountability mechanism types – thrusters, scoopers scroungers and squirrels – was proposed.

Most jurisdictions feature a mixture of thrusters and scoopers in their accountability arrangements. Scroungers are also emerging as an important part of the accountability mix. It is conceivable that further research could articulate a set of desirable combinations of scoopers, scroungers, thrusters and squirrels for a given jurisdiction or institutional framework. The goals of such a combination would be to maximize the accountability dividend while minimizing the investment in what can be costly review and oversight activities.

References

Adams, N. (1986) 'Efficiency Auditing in the Australian Audit Office', *Australian Journal of Public Administration*, 45(3), pp. 189–200.

Barzelay, M. (1996) 'Performance Auditing and the New Public Management: Changing Roles and Strategies of Central Audit Institutions', in: OECD (1996), *Performance Auditing and the Modernization of Government*, Paris: OECD.

Barzelay, M. (1997) 'Central Audit Institutions and Performance Auditing: A Comparative Analysis of Organizational Strategies in the OECD', *Governance*, 10(3), July 1997, pp. 235–60.

Bovens, M. (2006) Analysing and Assessing Public Accountability: A Conceptual Framework, European Governance Papers (EUROGOV), no C-06-01, accessed 15 February 2009 at http://www.connex-network.org/eurogov/pdf/egp-connex-C-06-01.pdf

Braithwaite, J. (2007) *Regulatory Capitalism: How it Works*. Edward Elgar. Cheltenham.

Brewer, G. A. and S. C. Selden (1998) ‘Whistle Blowers in the Federal Civil Service: New Evidence of the Public Service Ethic’, *Journal of Public Administration Research and Theory*, 8(3), pp. 413–40.

Burrowes, A. and M. Persson (2000) ‘The Swedish Management Audit: A Precedent for Performance and Value for Money Audits’, *Managerial Auditing Journal*, 15(3), pp. 85–97.

Case, J. (1995) *Open-Book Management: The Coming Business Revolution*, New York: Harper Business.

Case, J. (1998) *The open-book experience: Lessons from over 100 companies who successfully transformed themselves*, Reading: Addison Wesley.

Dewar, D. (1985a) ‘Value for money audit: the first 800 years’, *Public Finance and Accountancy*, August 30, pp. 10–12.

Dewar, D. (1985b) ‘Cutting through the blurred distinctions of what is VFM’, *Accountancy Age*, April 11, 1985.

Dunleavy, P. and H. Margetts (2000) ‘The advent of digital government: Public bureaucracies and the state in the internet age’, Paper delivered to the Annual Conference of the American Political Science Association, Omni Shoreham Hotel, Washington, 4 September 2000.

Ettema, J. S. and T. L. Glasser (1998) *Custodians of Conscience: Investigative Journalism and Public Virtue*, New York: Columbia University Press.

Flesher, D. L., W. D. Samson and G. J. Previts (2003) ‘The origins of value-for-money auditing: the Baltimore and Ohio Railroad: 1827–1830’, *Managerial Auditing Journal*, 18(5), pp. 374–86.

Frey, B. S. (1994) ‘Supreme Auditing Institutions: A Politico-Economic Analysis’, *European Journal of Law and Economics*, 1, pp. 169–76.

Funnell, W. (1998) ‘Executive coercion and state audit, A processual analysis of the responses of the Australian audit office to the dilemmas of efficiency auditing 1978–84’, *Accounting Auditing and Accountability Journal*, 11(4), pp. 436–58.

Funnell, W. (2001) *Government by Fiat*, UNSW Press, Sydney.

Goetz, A. M. and R. Jenkins (2001) ‘Hybrid Forms of Accountability: Citizen Engagement in Institutions of Public-sector Oversight in India’, *Public Management Review*, 3(3), pp. 363–83.

Government 2.0 Taskforce (2009) ‘Engage: Getting on with Government 2.0’, Draft Report of the Government 2.0 Taskforce, Canberra: Government 2.0 Taskforce.

Guthrie, J. and Parker, L. D. (1999) ‘A Quarter Century of Performance Auditing in the Australian Federal Public Sector: A Malleable Masque’, *Abacus*, 35(3), pp. 302–32.

Hazell, R. (2007) ‘Freedom of Information in Australia, Canada and New Zealand’, *Public Administration*, 67(2), pp. 189–210.

Hodge, G. (2009) ‘Accountability’, in: P. A. O’Hara (ed.) *International Encyclopedia of Public Policy*, Volume 3: Public Policy and Political Economy, Perth: Global Political Economy Research Unit, .] pp. 1–17.

INCOSAI [International Congress of Supreme Audit Institutions] (1986) *General Statement on Performance Audit of Public Enterprises and Audit Quality*, International Congress of Supreme Audit Institutions, Sydney, 7–16 April, 1986, Canberra: AGPS.

Jubb, P. B. (1999) ‘Whistleblowing: A Restrictive Definition and Interpretation’, *Journal of Business Ethics*, 21(1), pp. 77–94.

Katz, A. M. (1976) ‘Government information leaks and the First Amendment’, *California Law Review*, 64(1), pp. 108–45.

Kells, S. and G. Hodge (2009) ‘Performance auditing in the public sector: Reconceptualising the task’, in *Journal of Contemporary Issues in Business and Government*, 15(2).

Lindeberg, T. (2007) ‘The Ambiguous Identity of Auditing’, Financial Accountability and Management, Vol. 23, No. 3, pp. 337–50.

Lonsdale, J. (2000) ‘Developments in value-for-money audit methods: impacts and Implications’, *International Review of Administrative Sciences*, 66(1), pp. 73–89.

McMillan, J. and P. Zoido (2004) ‘How to Subvert Democracy: Montesinos in Peru’, Centre for Economic Policy Research, Discussion Paper 4361, 21 April 2004.

Metaxiotis, K. and J. Psarras (2004) ‘E-government: new concept, big challenge, success stories’, *Electronic Government,* 1(2), pp. 141–51.

Normanton, E. L. (1966) *The Accountability and Audit of Governments*, Manchester: Manchester University Press.

Ott, S. J. and E.W. Russell (2001) ‘Leadership and Accountability’, in: *Introduction to Public Administration: A Book of Readings*, Melbourne.

Piotrowski, S. J. and D. H. Rosenbloom (2002) ‘Nonmission-Based Values in Results-Oriented Public Management: The Case of Freedom of Information’, *Public Administration Review*, 62(6), pp. 643–57.

Pollitt, C., X. Girre, J. Lonsdale, R. Mul, H. Summa and M. Waerness (1999) *Performance or Compliance? Performance Audit and Public Management in Five Countries*, Oxford: Oxford University Press.

Power, M. (2000) ‘The Audit Society – Second Thoughts’, *International Journal of Auditing*, 4(1), pp. 111–19.

Shand, D. and P. Anand (1996) ‘Performance auditing in the public sector: Approaches and issues in OECD member countries’, in: OECD (1996), *Performance Auditing and the Modernisation of Government*, Paris: OECD.

Tant, A. P. (2005) ‘“Leaks” and the nature of British Government’, *Political Quarterly*, 66(2), pp. 197–209.

Toma, M. (1989) ‘Will bounty-hunting revenue agents increase enforcement?’ *Public Choice* 61, pp. 247–60.

Vinten, G. (1996) *Internal Audit Research: The First Half Century*, London: The Chartered Association of Certified Accountants.

Yamamoto, K. and Watanabe, M. (1989) ‘Performance auditing in the Central Government of Japan’, *Financial Accountability and Management*, 5(4).

Notes

[1] The author is grateful to Professor Graeme Hodge for valuable discussions about the concepts and tools presented in this paper. Any remaining errors are the author’s.

[2] In one instance, the authoriser and the auditee may coincide.

[3] In some respects, the relationship being described is analogous to that between principal and agent.

[4] According to the Australian Government 2.0 Taskforce, ‘hacking’ is ‘Not necessarily a negative term...hacking can refer to the act of building new applications or modifying existing ones with the goal of encouraging openness, sharing and collaboration’ (p. 103).

[5] Another way to represent the different mechanisms graphically is to plot them against the relevant dimensions such as outside/inside (I_{org}), authorised/unauthorised, and publication/no publication.