

Software License Audit and Security Implications



Wee Kiat Yang, Amin Hosseinian-Far , Luai Jraisat ,
and Easwaramoorthy Rangaswamy

Abstract The typical purpose of software auditing is to assess the conformance of the developed software with the original plans, procedures, relevant regulations. Every audit involves several people with various roles in the auditing processes. The audit itself entails a number of preferable characteristics. In any audit engagement, the perceptions of the audit quality are directly related to the perceived reputation, credibility and objectivity of the auditor. This paper highlights and critically reviews the research works related to quality in audit, in particular, software license audit from the perspective of internal control and security. The paper examines existing studies in the field with a view to identifying future research opportunities in relation to software license auditing. Moreover, security implications and challenges in the context of software auditing, and a set of recommendations are provided.

Keywords License audit · Software audit · Compliance · Security

1 Introduction

In every software company, survival depends on aggressive development and protection of its intellectual property [1, 2]. Other than protection from illegal installation of products, compliance is another important area of software licensing. This is especially so in relation to consumption and proper licensing of the software products and ensuring their customers software assets are managed effectively [3].

W. K. Yang · A. Hosseinian-Far (✉) · L. Jraisat
Faculty of Business & Law, University of Northampton, Northampton NN1 5PG, UK
e-mail: amin.hosseinian-far@Northampton.ac.uk

W. K. Yang
e-mail: wee.yang@Northampton.ac.uk

L. Jraisat
e-mail: luai.jraisat@Northampton.ac.uk

E. Rangaswamy
Amity Global Institute, Singapore 238466, Singapore
e-mail: moorthy@singapore.amity.edu

In an audit engagement, the perceptions of the audit quality are directly related to the perceived reputation, credibility and objectivity of the auditor; in essence, the quality and experience of an auditor [4].

Considering the plethora of software development activities in today's digital world, license auditing process entail a number of challenges. Some of these challenges are:

- Inappropriate licensing model for customer
- Ineffective software asset management process
- Ineffective users' access management
- Ineffective authorization management
- Engaging software customers in the audit process
- Third party audit firms that do not understand or abide by the licensing model and measurement methodology of software vendors
- Inaccurate information or advice provided by third party audit firms

Considering these challenges, this paper attempts to provide a concise overview of the software license auditing process. It also attempts to provide a brief discussion on security implications in the context, and offer a number of recommendations.

The rest of the paper is structured as follows. Section 2 provides a literature review on software licensing, contributing factors on audit quality, and relevant concepts within the field. Section 3 provides a brief discussion on auditing challenges and security implications. A brief discussion, the future of software license auditing, and a number of recommendations are provided in Sect. 4. The paper is concluded in Sect. 5.

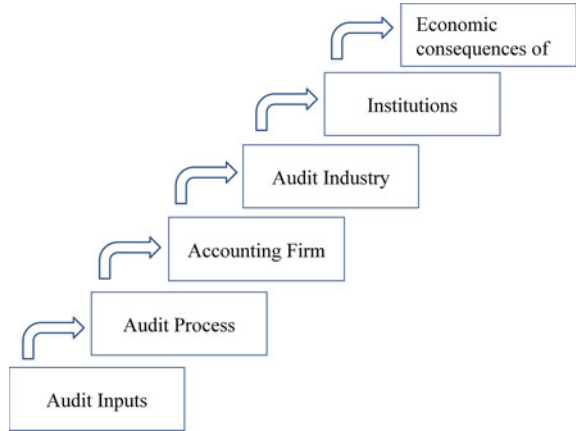
2 Literature Review

Audit is defined as "an official examination of business and financial records to see that they are true and correct" or "an official examination of the quality or standard of something" [5] and License Auditing is the official examination of the licensees' deployment and utilization of the software to ensure proper Software Asset Management (SAM). Most of the existing studies are conducted in the area of financial auditing and are focused on the financial examinations.

Other than the qualification of the auditor, audit quality is an important aspect of a successful audit. Audit quality, as defined by DeAngelo [6] "...to be the market-assessed joint probability that a given auditor will both (a) discover a breach in the client's accounting system, and (b) report the breach.". It is also determined between low-to-high quality involving various factors [7].

In the area of financial auditing, failure in an audit often occur when the auditor does not enforce the proper audit principles. This is known as the Generally Accepted Accounting Principle (GAAP) failure. Another circumstance when an audit failure can occur is when the auditor fails to produce a qualified report for the engagement known as audit report failure [8].

Fig. 1 Framework adopted from Francis’s Audit Quality Assessment Framework [7]



To date, several research works have studied audit quality and the factors that are affecting the audit quality. Some of the notable factors include: Audit firm’s reputation [9, 10], Audit firm’s size [6, 7, 11–14], Non-Audit services [15], Task complexity [16], Auditor’s rotation [16, 17] and Auditor’s independence [16, 18].

To effectively study the audit quality, Francis [7] developed a framework that assesses some of the factors that are impacting an audit quality. The framework consists of 6 levels namely Audit inputs, Audit process, Accounting firm, Audit industry, Institutions and Economic consequences of audit outcome (Fig. 1).

Audit testing procedures and team personnel are the inputs to the framework. The inputs are then transited to the next level of the framework for the decisions to be made by the engagement team through the audit process. The assumption of Francis was that auditing occurs in the context of the audit firm [7]. The audit firm is also the institution that hires, trains and develops the auditors. The audit report is also cleared and issued under the name of the firm. It is this collection of audit forms that has formed the Audit Industry and the audit market which is in turn governed by various certification bodies and institution. Therefore, these activities affect clients’ companies in terms of report outcome. It was also noted by Francis that if an audit is carried out by competent auditors, the audit result will be of a higher quality. However, there are no evidence to support this claim. On the contrary, performance can be affected by many factors [11–13]. It was also perceived that larger firms have more in-house expertise and therefore have a greater opportunity to produce higher quality audits. While there were insufficient data to link audit quality and size of audit form [7], it is somewhat true in terms of expertise. In the context of principle software vendors, the auditors, who are the employees of the principal software vendors, usually have the expertise and expert knowledge in their own software products. Additionally, they are supported by a large number of in-house resources that are experts in different dimensions of the software product. Thus, the quality of audits conducted by principle software vendors are perceived to be of a higher quality compared to external audit firms. Other factors should be considered. There

are instances that accounting audits in their audit tenure conduct non-audit services, and this may influence the level of specialty required for nonfinancial audits.

There are no firm evidence pointing to the loss of audit quality for firms registered with the Securities and Exchange Commission (SEC) when performing non-audit services. Instead, such registration is observed to be positively associated with the audit quality, and therefore it is of the opinion that it is actually the result of auditors providing higher quality audit [19]. In a separate study conducted by Boskou, Kirkos and Spathis [20], information from publicly available annual reports were used to develop a classification of audit quality. Using machine learning techniques to perform text mining from a company's annual report also yielded the conclusion that there is a positive relationship between financial, operational and strategic risks [21]. Boskou, Kirkos and Spathis used models and natural language processing to review different models and developed a classification that can be used to predict internal audit quality, by enabling the auditor to effectively assess the risks and better plan audit procedures [20].

In order to provide inputs relating to the attributes that are important to audit quality, around 4,600 audit professionals in IT and Finance were surveyed by Stoel et al. Accounting skill and Audit skills, Business process knowledge and experience were rated higher by the Financial auditors while Auditor Experience with Auditee, IT and Controls Knowledge, and Planning and Methodology were rated higher by IT [22]. This information provides greater insights to audit leads when planning for an audit that can contribute positively towards improving the quality of audit.

In a separate study conducted by Kilogre and Bennie [23] on Australian auditors, the audit quality attribute that was perceived to be the most important was reported to be 'Audit firm size' (Table 1).

"Whether or not they are IT auditor or Financial auditors, it was observed that there was a positive correlation between auditors in big-N firms and audit quality that is referred to as the "Big N effect" [14]; therefore, it seems that the higher the quality of the audit, the greater the assurance of report quality [24]. However,

Table 1 Categorization of attributes and their relative ranking, adopted from [23]

Rank	Attributes	Category
1	Audit firm size	Independence/Competence
2	Partner/Manager attention to audit	Competence/Interaction
3	Communication between audit team and client management	Interaction
4	Knowledgeable audit team	Competence
5	Audit firm industry experience	Competence
6	Partner knowledge of client industry	Competence
7	Senior manager/manager knowledgeable—client industry	Competence
8	Provision of non-audit service	Independence
9	Audit quality review	Competence
10	Audit partner tenure	Independence

it is challenging to compare the audit quality between firms that assign the audits in Big-N and non-Big-N as the audit firms choose their auditors based on firm or the characteristics of the auditor. Nevertheless, larger firms have more resources and technology support over non-Big-N firms. Moreover, Big-N auditors are known to be “generalist” [25, 26]. That being said, firms with poor performance are more likely to change auditors [27].

Apart from the studies involving attributes contributing to audit quality, some research works have attempted to adopt text mining to examine audit report and evaluate the quality of audits. A company’s annual report is a useful tool where the information is available publicly. This information can be analyzed textually using classification methods. Machine learning and natural language processing tools can also be used to effectively assess risks and provide recommendation to auditor to improve audit procedures [20].

Generally, in an audit practice, auditors collect artefacts and supporting documents through the use of an audit procedure to detect materials that may demonstrate misrepresentation in financial statements. When such misinterpretation is detected by auditors, such misconceptions are usually communicated to auditees’ management to adjust the misstatements. This is similar with license auditing where the license auditor communicates with customers (or management) to understand the cause of such misinterpretation. These misinterpretations, however, can also be due to the internal processes that result in certain findings. For instance, suppose a customer has User Licenses created in the System that exceeds his/her entitlement. Discussions are carried out with the customer to understand the issue, and where necessary, User number is adjusted downwards based on the assessment and feedback; Also, another underlying reason may be due to the customer’s failure to clean up or deactivate an unused User account, that was later verified using system data. In summary, the phases of determining audit quality are (i) Detecting (ii) Adjusting (iii) Reporting of misstatement/misrepresentation to achieve audit quality.

The observable audit objectives include audit adjustments, audit opinion and the quality of audited financial statements. Adjustment occurs when there is a misstatement in the pre-audit financial statements and is required by the auditor to correct the misstatement or issuing a modified audit opinion in response to the misstatement [28]. According to Xiao et al. [28], an audit adjustment appears to occur more frequently when the audit effort is greater. The increase audit effort means the auditor can perform more comprehensive audit verifications with the attainment of more artefacts to demonstrate certain system behavior or financial postings, thus improves the ability to detect misstatements. With enough artefacts and evidences, the auditor is in a better position to determine anomalies, and less likely to waive any audit adjustments proposed by the client’s management. If an adjustment is required with the support of the evidence, auditors are in a better position to ensure detected misstatements can be corrected through adjustments. Therefore, higher audit effort does not naturally means that there are more issuances of modified audit opinions [28].

2.1 Licensing

In the software market, infringement of copyright includes the reverse engineering of software codes and unauthorized duplication and use of software. The Business Software Alliance estimated that, in 2011, that the illegal software market caused about US\$63 billion in damages all over the world [29].

When we look at software licensing, the general categories are opensource, non-opensource and subscription based. There are well over 60 different types of opensource software [30] such as mSQL, Linux, opensource Office etc. In terms of non-Opensource, there are several major software vendors with products that are non-Opensource, for instance MicrosoftTM, SAPTM, OracleTM, AdobeTM etc. Subscription software examples are SalesforceTM, Workday, SAP Cloud Solutions etc.

In terms of license auditing, in particular to SAP licensing, there are different licensing models namely perpetual, subscription and consumption based. SAP software are based on two components (i) Software and (ii) SAP Named Users. There are two perpetual license models—the Classic SAP software and SAP S/4HANA-branded software. Software provides the opportunity to support business functionality and is licensed in accordance with specific metrics. SAP Named Users provide the rights for individuals to use the software. The named users are further divided into a few types, each providing specific use rights. SAP uses the analogy of a house and the key where the Software is the “house” and the Named Users are the “keys” [3].

In a subscription model, the customer does not have perpetual use rights over the software, instead pays an annual subscription fee as part of a term contract. The fee includes all the Software as a Service (SaaS) components, including product support. Under the consumption-based model, and the customers pay the dues based on actual usage. There are also various types of database licensing options that need to be considered.

Compliance is an important aspect of SAP software licensing. When it comes to the consumption and proper licensing of SAP products, SAP’s global audit and license compliance process protects SAP’s core business assets and ensures that SAP’s customers can manage their SAP assets effectively and manage any overuse of the software [3].

If an audit is initiated by a software vendor, organizations should cooperate with the software vendors. There are instances where customers are evasive and purposefully delay requests, provide inaccurate or wrong information, and are non-responsive to the request of information or organization’s attempt to circumvent the software’s built in monitoring mechanisms [31]. In such cases, there will be difficult conversations with the customer with possible escalations from both sides. At times, it may involve legal interventions to enforce the contractual rights. Therefore, it is important to properly plan an audit engagement. Planning the information systems audit must include all the stages necessary for the achievement of the objectives of the audit mission, namely documentation of the audited activity, the program or system

under scrutiny, the establishment of the audit strategy, the establishment of the audit procedures and techniques, and the methods of synthesis, analysis and interpretation of the audit evidence [32].

3 Security Implications

Many software organizations are facing the situation where it is believed that their intellectual property (IP) rights are not used in a lawful manner causing revenue leakage and potential loss of control over the protection of IP rights and discouragement of infringements [33]. All usage of Intellectual Properties should be appropriately licensed depending on the usage and scenarios. In the factsheet published by the European Intellectual Property Rights (IPR) Helpdesk, license agreement is defined as “a contract under which the holder of intellectual property (licensor) grants permission for the use of its intellectual property to another person (licensee), within the limits set by the provisions of the contract” [34]. Without such an agreement, the use of the intellectual property would most likely result in an infringement.

Based on a survey conducted by Deloitte on consumer privacy, it was found that 91% of the 2,000 participants aged between 18–75 are willing to accept legal terms and conditions without reading them [35]. Not just in the consumer space, companies sometimes agree and sign the Software agreement without fully understanding the implications of the contract or the “fine prints”. While some may say that contracts of larger and younger companies tend to be “pro-seller”, there are no evidences to support that larger firms offer software terms that are worse than those that are offered to general public as compared to business and corporate users [36].

Proper software licensing and audit not just ensure company remains compliant to the agreement that they have signed with the Software vendor, but also ensure their internal control and governance are functioning properly. Internal control that we are discussing in this paper are the segregation of duties and unauthorized access. Segregation of duties is one of the fundamental elements of internal control [30]. Other than ensuring no single individual has control over the whole process, exposing the organization to risk, but also to ensure legal compliance [37]. Not just in Information Technology, this notion is also an important topic in accounting, given that the segregation of duties seeks the prevention of possible fraud through collusion, where there are conflict of interest [38]. In licensing terms, one scenario relating to the segregation of duties include sharing of User IDs within the organization. Some companies attempt to cut down the number of licensed Users by allowing Users to share a single User ID for various functions within the department. This results in the inability to identify the exact person who entered a request entry. This issue leads to the inability to identify the individual who approved the request. This also creates collusion between employees and potentially results in fraud cases within the organization.

With the sharing of User ID, an employee who is no longer with the department or organization may gain unauthorized access to the application software by using

the shared User ID. This can be done by a disgruntled employee or an attacker with the aim of stealing information, resulting in unauthorized access to the protected or sensitive information. Eventually, this compromises the data integrity and availability within the firm [39]. Software license audit can potentially expose sharing of licenses by reviewing the Usage information and User management procedures. While protecting the intellectual property of the software vendors, it can also uncover malpractices and make known to the management for corrective measures.

4 Discussion and Recommendation

In every license audit scenario, the outcome is not just ensuring the intellectual property is protected, but it also provides a significant revenue stream to the company. Several existing research studies have been conducted on audit quality. However, more remains to be done in the area software auditing, in particular, software license auditing and how it will inform information security and compliance procedures.

Some security implications relating to license management are:

- (a) The issue of unauthorized access; In addressing the issue on the sharing of User IDs, proper management of User licenses reduce sharing of User ID thus cutting down unauthorized access incidents to the system. Preventive measures include:
 - Ensuring that every individual is assigned to their own User ID; that way, any access and transactions can be traced back to the individual;
 - Ensuring User Management policy is in place. For instance, if an individual has not logged in for 30 days, the User ID should be locked and if the individual has not logged in for next 30 days, the ID will be invalidated;
 - Authorization assigned to individual IDs should have an expiry date and set access levels that should be approved periodically;
- (b) Sharing of User IDs potentially leads to the risk of segregation of duties; User ID sharing between a few individuals performing different roles leads to the User ID being authorized in excess of the requirement. For example, an individual may submit a purchase requisition and uses the same ID; the requisition can be approved by the same individual thus making unauthorised purchases through the system that are challenging to uncover by examining the existing system data.

Addressing such licensing concerns, provides the opportunity to organizations to minimize risks related to internal controls.

5 Conclusion and Future Work

License auditing entails a number of processes and a good quality audit is typically defined by several characteristics. There are security implications in the software license auditing sector. This paper highlighted the importance of audit quality, and discussed some of the security implications within the context.

Moreover, the paper explored other research opportunities. One of the future areas of research is to assess and identify further factors that affect the quality of an audit. This could be achieved, for instance, by the application of information seeking behavior and foraging theories and practices, which may also inform other security implications specific to license auditing. In this context, various categories of information, i.e. information as process, information as knowledge and information as thing will need to be analyzed considered, and ‘information as thing’ as a notion will need to be used to assess data in the license auditing process [40]. Data in the context of future research refers to the facts and statistical representation residing in the information system that can be downloaded for analysis.

References

1. Bader MA (2006) Intellectual property management in R&D collaborations: the case of the service industry sector. Physic-Verlag-A Springer Company
2. Perleberg GB (2015) Technology licensing, pp 27–30
3. SAP (2018) SAP licensing guide.pdf
4. Soobaroyen T, Chengabroyan C (2006) Auditors’ perceptions of time budget pressure, premature sign offs and under-reporting of chargeable time, vol 218, pp 201–218
5. Oxford Learners D (2020) Definition of audit. https://www.oxfordlearnersdictionaries.com/definition/english/audit_1?q=audit. Accessed 26 June 2020
6. DeAngelo LE (1981) Auditor size and audit fees. *J Acc Econ* 3(May):183–199
7. Francis JR (2011) A framework for understanding and researching audit quality. *Auditing* 30(2):125–152. <https://doi.org/10.2308/ajpt-50006>
8. Francis JR (2004) What do we know about audit quality? *Br Acc Rev* 36(4):345–368. <https://doi.org/10.1016/j.bar.2004.09.003>
9. Skinner DJ, Srinivasan S (2012) Audit quality and auditor reputation: evidence from Japan. *Acc Rev* 87(5):1737–1765. <https://doi.org/10.2308/accr-50198>
10. Aronmwan EJ, Ashafoke TO, Mgbame CO (2013) Audit firm reputation and audit quality. *Eur J Bus Manag* 5(7):2222–2839
11. Castka P, Bamber CJ, Sharp JM (2001) Factors affecting successful implementation of high performance teams. *Team Perform Manag Int J* 7(7–8):123–134. <https://doi.org/10.1108/13527590110411037>
12. Caillier JG (2010) Factors affecting job performance in public agencies. *Public Perform Manag Rev* 34(2):139–165. <https://doi.org/10.2753/pmr1530-9576340201>
13. Ariffin ZZ (2012) Do industry affiliations affecting corporate tax avoidance. In: International conference on management, economics and finance (Icmef 2012) proceeding, no October, pp 784–796
14. DeFond M, Erkens DH, Zhang J (2015) Do client characteristics really drive the Big N audit quality effect? *Manag Sci*
15. Beck PJ, Wu MGH (2006) Learning by doing and audit quality. *Contemp Acc Res* 23(1):1–30. <https://doi.org/10.1506/axu4-q7q9-3yab-4qe0>

16. Agus Wijaya I, Yulyona MT (2017) Does complexity audit task, time deadline pressure, obedience pressure, and information system expertise improve audit quality? *Int J Econ Financ Iss* 7(3):398–403 [Online]. <http://www.econjournals.com>
17. Knechel WR, Vanstraelen A (2007) The relationship between auditor tenure and audit quality implied by going concern opinions. *Auditing* 26(1):113–131. <https://doi.org/10.2308/aud.2007.26.1.113>
18. Tepalagul N, Lin L (2015) Auditor independence and audit quality: a literature review. *J Acc Audit Financ* 30(1):101–121. <https://doi.org/10.1177/0148558x14544505>
19. Bell TB, Causholli M, Knechel WR (2015) Audit firm tenure, non-audit services, and internal assessments of audit quality. *J Acc Res* 53(3):461–509. <https://doi.org/10.1111/1475-679X.12078>
20. Boskou G, Kirkos E, Spathis C (2019) Classifying internal audit quality using textual analysis: the case of auditor selection. *Manag Audit J* 34(8):924–950. <https://doi.org/10.1108/MAJ-01-2018-1785>
21. Yang R, Yu Y, Liu M, Wu K (2018) Corporate risk disclosure and audit fee: a text mining approach. *Eur Acc Rev* 27(3):583–594. <https://doi.org/10.1080/09638180.2017.1329660>
22. Stoel D, Havelka D, Merhout JW (2012) An analysis of attributes that impact information technology audit quality: a study of IT and financial audit practitioners. *Int J Acc Inf Syst* 13(1):60–79. <https://doi.org/10.1016/j.accinf.2011.11.001>
23. Kilgore A, Bennie NM (2014) The drivers of audit quality: auditors' perceptions. *Assoc Chart Certif Acc* 3–15
24. DeFond M, Zhang J (2014) A review of archival auditing research. *J Acc Econ* 58(2–3):275–326. <https://doi.org/10.1016/j.jacceco.2014.09.002>
25. Sirois L-P, Simunic DA (2012) Auditor size and audit quality revisited: the importance of audit technology. *SSRN Electron J*. <https://doi.org/10.2139/ssrn.1694613>
26. Jiang J, Wang IY, Philip Wang K (2019) Big N auditors and audit quality: new evidence from quasi-experiments. *Acc Rev* 94(1):205–227. <https://doi.org/10.2308/accr-52106>
27. Landsman WR, Nelson KK, Rountree BR (2009) Auditor switches in the pre- and post-enron eras: risk or realignment? *Acc Rev* 84(2):531–558. <https://doi.org/10.2308/accr.2009.84.2.531>
28. Xiao T, Geng C, Yuan C (2020) How audit effort affects audit quality: an audit process and audit output perspective. *China J Acc Res* 13(1):109–127. <https://doi.org/10.1016/j.cjar.2020.02.002>
29. Arai Y (2018) Intellectual property right protection in the software market. *Econ Innov New Technol* 27(1):13. <https://doi.org/10.1080/10438599.2017.1286734>
30. Peng G, Di Benedetto CA (2013) Learning and open source software, vol 44, no 4, pp 619–643
31. Bigler M (2003) The high cost of software piracy. *Intern Audit*
32. Lenghel RD, Vlad MP (2017) Information systems auditing. *Quaestus Multidiscip Res J* 11:178–182. [https://doi.org/10.1016/0378-7206\(84\)90006-5](https://doi.org/10.1016/0378-7206(84)90006-5)
33. European IPR Helpdesk (2015) Fact sheet defending and enforcing IP. European IP Helpdesk. <http://www.iprhelpdesk.eu/sites/default/files/newsdocuments/Fact-Sheet-Defending-and-Enforcing-IP.pdf>. Accessed 29 July 2020
34. European IPR Helpdesk (2015) Commercialising intellectual property : license agreements. European Intellectual Property Rights. <https://www.iprhelpdesk.eu/sites/default/files/newsdocuments/Fact-Sheet-Commercialising-IP-Licence-Agreements.pdf>. Accessed 29 July 2020
35. Deloitte (2017) Global mobile consumer survey: US results
36. Marotta-Wurgler F (2007) What's in a standard form contract? An empirical analysis of software license agreements. *J Empir Leg Stud* 4(4):677–713. <https://doi.org/10.1111/j.1740-1461.2007.00104.x>
37. Ferroni S (2016) Implementing segregation of duties. A practical experience based on best practices. *ISACA J* 3:1–9 [Online]. www.isaca.org
38. Kim R, Gangolly J, Ravi SS, Rosenkrantz DJ (2020) Formal analysis of segregation of duties (SoD) in accounting: a computational approach. *Abacus* 56(2):165–212. <https://doi.org/10.1111/abac.12190>

39. Sen R, Borle S (2015) Estimating the contextual risk of data breach: an empirical approach. *J Manag Inf Syst* 32(2):314–341. <https://doi.org/10.1080/07421222.2015.1063315>
40. Buckland MK (1991) Information as thing. *J Am Soc Inf Sci* 42(10):758–758. [https://doi.org/10.1002/\(SICI\)1097-4571\(199112\)42:10%3c758:AID-ASII1%3e3.0.CO;2-4](https://doi.org/10.1002/(SICI)1097-4571(199112)42:10%3c758:AID-ASII1%3e3.0.CO;2-4)