Campbell Rose
Tax Partner
+64 (0) 9 303 0990
camrose@deloitte.co.nz

Amy Duan
Consultant
+64 (0) 9 303 0770
amduan@deloitte.co.nz

Emails: smart ways to manage the potential minefield

Campbell Rose and Amy Duan

Some context

In our **December 2012 Tax Alert** we outlined significant changes to Inland Revenue's risk review process, which have now taken effect. The changes mean that a larger group of taxpayers must be "audit ready" sooner. Ideally, this includes preparing an "audit file" containing all advice and contractual documents, board minutes, primary email correspondence and other relevant material relevant to a transaction or tax positions generally.

The need for this readiness stems from the increasing reliance by Inland Revenue and the courts on peripheral material such as emails – particularly in an anti-avoidance context - to draw factual inferences. This is despite long-standing case law authority, and the Inland Revenue's own draft interpretation statement on section BG 1, confirming that the anti-avoidance enquiry must be objective and focussed upon the purpose or effect of the arrangement (not of the parties). Emails often form a critical part of Inland Revenue investigations because they can be a colourful – and damaging - source of evidence that is used to support the Inland Revenue's avoidance theory. In recent tax avoidance cases, emails have been relied on as evidencing relevant facts, intensely scrutinised in cross examination and fully reproduced in the courts' judgments.

Below we expand on what being "audit ready" means from a practical and technological perspective. This involves exploring some of the tools available to manage email communication and to assist in the review of voluminous email archives.

Go to the source

As the saying goes, prevention is better than cure. In our December 2012 Tax Alert Article, we outlined some basic rules of thumb which could be applied to ensure that "tax advice document" status attaches to key emails, and that unhelpful material does not come into circulation.

Of course, human behaviour is such that (even with the best of intentions, policies and procedures) potentially adverse emails may nevertheless be created. It is also apparent that, in our experience, the author of an email (particularly outside an organisation's tax function) often does not consider how the email may be interpreted by a third party such as the Inland Revenue years later.

To some extent, a solution may lie within an organisation's own IT system. The innovative leverage of existing IT infrastructure can often prevent potentially adverse emails from being produced or proliferated.

For example, email monitoring tools could be applied to automatically forward or copy to (say) the tax manager emails matching certain criteria. Better still, most large organisations already have email gateways containing filters that auto-delete or auto-block emails being sent to (or from) outside parties if particular words and/or phrases are identified in email or attachment text. This technology could be used to temporarily hold emails that contain phrases such as "tax benefit" in the organisation's email gateway, to be released to the relevant recipient(s) only after approval by particular individuals within the organisation. In a transaction context, this technology would be limited to members of the relevant project team, so that the volume of emails being forwarded/suspended did not become unwieldy.

For smaller organisations, the benefit of implementing and maintaining such gateways will obviously be weighed against the cost of doing so – but even the most elementary of IT systems may still permit some degree of filtering in this manner.

Retention obligations – the scope?

As noted above, despite the best laid plans (and monitoring/gateway tools), potentially adverse emails will inevitably slip through. This raises the issue of whether, and the extent to which, there is an obligation to retain such emails.

Section 22 of the Tax Administration Act 1994 requires any person carrying on business or other income earning activities in New Zealand to keep sufficient "records" to enable the Commissioner of Inland Revenue to readily ascertain that person's income, deductions etc. Subject to limited exceptions, those records must be kept for a minimum of 7 years. An equivalent obligation exists for GST purposes.

Clearly, an email is a "record", and a recent standard practice statement issued by Inland Revenue (SPS 13/01) confirms this. It is not so clear, however, which particular emails forming part of the general correspondence 'traffic' during the planning and implementation of a transaction fall within the section 22 obligation.

Emails circulating executed copies of transaction documents would be an obvious candidate for retention. Other emails in the formative stages of a transaction may not however provide any assistance in ascertaining a taxpayer's income or deductions – particularly if they contain subjective material which should be irrelevant to any anti-avoidance analysis. That said, there may be a desire (but not an obligation) to retain emails containing helpful material supporting the commercial rationale for a transaction or particular steps taken in the context of a transaction. Evidence of purpose or intention may be relevant to determining (say) whether assets are held on capital or revenue account, and so emails containing such evidence would appear to be within section 22's ambit.

It therefore seems difficult to formulate any "one size fits all" rule, in terms of which emails can be permanently deleted from an organisation's server and when: although, even then, such emails may still be stored in the sender's "sent items" folder or in other electronic locations. Perhaps the best that can be done, in addition to the measures discussed above, is to undertake some 'housekeeping' post-completion, to determine which categories of emails (for example, by sender/recipient) do not need to be retained – some tools in this regard are discussed further below. The question also arises as to whether an email that has been held in a gateway and not ultimately received by its intended recipient (i.e. not released) is still a "record" for section 22 purposes.

Finally, the Inland Revenue's published guidance does confirm that taxpayers must retain information that can identify the origin, destination and time when an email was sent; and such information must be kept in readily accessible form (SPS 13/01 at [37] and [39]). We note that the Commissioner may apply to extend the 7 year retention period for a further 3 years if a taxpayer is under (or intended to be under, or the Commissioner is "actively considering") an audit or investigation. For completeness, taxpayers also have a duty to preserve relevant evidence under rule 8.3 of the High Court Rules, if litigation is "reasonably contemplated". This includes

preserving potentially relevant emails in readily retrievable form, even if they would otherwise be deleted in the ordinary course of business.

Credibility and consistency – filtering tools can help

It can be tempting to be drawn into providing explanations to Inland Revenue during the early phase of an audit. However, there is considerable risk in doing so without first reviewing relevant emails and other electronic material that may be uncovered in the course of the audit. This need for establishing a clear and credible position at the outset of the audit/dispute process, and consistency with that position as the audit/dispute progresses, has recently been illustrated in the Court of Appeal's judgment in Alesco. An explanation given, or position taken, which is inconsistent or at odds with material uncovered at a later stage, can quickly erode credibility and – if settlement is being pursued – bargaining position.

In our experience, "internal discovery" exercises are becoming more common at relevant stages of an audit or dispute. This involves reviewing all emails and other relevant electronic material (including, if needed, text messages and instant messages), before providing explanations to Inland Revenue and in order to fully assess the merits and weaknesses of a tax position. The main challenges in practice are:

- Volume of emails - it is reasonably common in a transaction to have "starting" email sets of 20,000 to 200,000 emails;
- Duplicate emails - in most email datasets there is often a high level of duplicates caused by emails being sent to multiple recipients, and the same email being stored in multiple locations (e.g. laptop, email server and back-up tapes);
- Review of emails - the needs of someone reviewing emails for audit/dispute purposes are different from someone reviewing emails for general business related purposes. The person reviewing must also have the requisite knowledge to tag certain emails as being relevant, discoverable, privileged, tax advice document, etc.

We have technology available that makes light(er) work of email review. The level of streamlining achievable by using specialised tools can be illustrated by a recent real example:

- We started with 450,000 emails;
- We reduced these by approximately 15% by removing duplicates (the reduction from duplicates is often closer to 50%);
- We further reduced this to approximately 4,000 emails by using a variety of keywords, date ranges and other filters.

By doing this, we were able to generate vast savings in terms of the cost and time required to review the emails. The client was able to review the 4,000 emails and attachments in less than a day, "tagging" documents as relevant, not relevant, etc. It meant that multiple layers of review could be applied to the final dataset (i.e. more than one set of eyes), in a cost efficient manner. In a section 17 notice context, it could also make what appear to be challenging deadlines both for responding and making tax advice document claims eminently achievable.

Concluding remarks

It is certainly true that email technology can contribute to a taxpayer's downfall, be it in a black letter or avoidance-related tax dispute.

However, it is equally clear that IT technology can feasibly be employed to:

- prevent the creation (or stem the proliferation) of adverse material;
- formulate policies around what electronic material can be deleted whilst maintaining compliance with record retention obligations and duties of preservation; and
- rationalise/review masses of electronic material with a view to ensuring that a credible and consistent position is taken, and that the strength and weaknesses of a position are most easily capable of assessment if settlement is plausible.

If you have any questions regarding anything discussed in this article, please contact your usual Deloitte advisor.