

---

## Revenue and Fraud Leaks: Measuring the Risks

Published by Dan Baker  
Friday, January 7<sup>th</sup> 2011

Leaks. The recent failure of the U.S. State Department to guard thousands of secret documents is a chilling reminder that leaks can do massive damage to a nation or a business.

For a telecom, a large systemic billing leak could spell a major financial loss and a public relations disaster. For a nation, intelligence leaks can weaken a security alliance, threaten the lives of diplomats, and even lead to war. Great Britain narrowly escaped complete ruin in the years before the Normandy invasion. But rising to the peril and inspiring the nation in its "finest hour" was Prime Minister Winston Churchill, who vividly explained the value of running a leak free and tight ship:

*"In times of war, the truth is so precious, it must be protected by a bodyguard of lies."*

Ironically, Churchill's comment prophesizes today's "honeypots," the cyber-defense tactic of offering up decoy computers to misdirect evil hackers and prevent leaks.

Leaks of all kinds – revenue, fraud, identity, cyber, and intelligence – are caused, of course, by a failure in upstream systems. And curing the troubles in telecom upstream systems offers great hope for the next round of RA cost savings. The mature RA organizations of the telecom world, firms like Verizon and AT&T, are reporting great success in their nascent attempts to do "preventative revenue assurance," that is, introducing controls that catch errors early enough in the upstream B/OSS systems so you can drastically reduce actual leaks.

And yet preventive RA is challenging the very way a revenue assurance team measures its success.

This subject is of great interest to Gadi Solotorevsky, CTO at cVidya, and a major contributor to the TM Forum's revenue assurance benchmarking organization. Recently, I had a chance to talk with him about it.

**Dan Baker: Gadi, preventive revenue assurance is an advanced stage in a telecom's RA maturity model. So why has it become a problem?**

**Gadi Solotorevsky:** I agree, Dan, preventive revenue assurance is a great step forward for RA because it means people are becoming more proactive. They are not just detecting leakages but stopping them from occurring in the first place.

But every organization inside a telecom needs to justify its reason for existing, and up to now, RA departments have defined themselves solely on the basis of detecting leaks and helping recover lost revenue. That's a problem because it puts the revenue-assurance manager in an awkward spot. The amount of leakage and recovery is dropping and those are precisely the parameters that dictate a RA department's budget and ability to staff the RA operation properly.

The answer, I think, is to find a new way to measure an RA department's performance in the proactive RA area. In particular, RA managers need to adopt some of the practices of Risk Management organizations.

**DB: This problem isn't limited to RA by the way. Cyber-security experts are another set of professionals who struggle to justify their existence to upper management. Because as the number of cyber-security breaches goes down, people get complacent and think the risks have gone away. But tell us, Gadi, how do you expect risk management and RA to intersect?**

**GS:** If you look at large telecoms, all of them have Risk Management (RM) experts on staff, and RM is actually the veteran discipline, with RA being a relative newcomer.

But Revenue Assurance and Risk Management speak two different languages. RA measures things in monetary terms – dollars, euros, etc. But risk management talks in terms of reducing risks.

Another contrast: Risk management takes a top down approach to measure risk, whereas revenue assurance, with our understanding of usage at a very fine grain level, can deliver a bottoms up view of revenue risks.

When you manage complex systems with lots of moving parts, it's too expensive to wrap controls around everything. So risk management is about selecting the right places to introduce controls so you have the biggest impact. Risk management is akin to insurance. So what's the risk that your office building will catch fire? Well, a risk-management specialist measures that risk and recommends smoke alarms and sprinkler systems to detect, prevent, and reduce the damage caused by building fires.

There are actually three kinds of risks that risk experts talk about: **inherent risks**, **control risks**, and **residual risks**.

In terms of a billing system, an **inherent risk** is the risk that the billing system's processes and software will not deliver accurate invoices. The **control risk**, on the other hand, is the risk that the controls (billing quality/RA people and RA software) you put in place will not be able to prevent, detect and correct those invoice errors. Finally, **residual risk** is the risk remaining after you put the controls in, and there's a formula that applies here: Residual Risk = Inherent risk x Control risk.

**DB: Governments maintains statistics on the causes and likelihood of fires to buildings. But where can you find statistics that allow you measure the risk in a billing or order management system? That information's going to be hard to come by.**

**GS:** Yes, but even if you come up with conservative estimates of risk reduction, you can show a lot of savings. You should be able to say that a certain control stops N% of leakage.

Now the telecoms who are doing preventive revenue assurance are at a mature stage, but three or four years ago they were not mature, so they must have internal benchmarks to show how valuable the risk reduction and prevention is. The question is: How much leakage did those organizations have before they put preventative controls in place? And to move the RA industry forward, we need to calculate this risk reduction and get everyone to agree on.

If you don't have a consistent way of measuring proactive controls, then each RA manager will use her own method of measuring it and it loses the authority of a standard.

**DB: Why hasn't Revenue Assurance quantified the value of risk mitigation before?**

**GS:** Well, I think in the past, leakage was so excessive that there was no need to analyze the risk side. RA was getting plenty of benefit from leak detection. If I can show I'm recovering X millions of Euros each year, what's the point? This is still the situation for many operators, especially those introducing new services and products.

But as an operator matures its RA practice, it needs to justify all the controls they have in billing and order management. So the challenge is: How do I put a number to that?

**DB: Finally, Gadi, please tell us what you're doing about this problem and how folks in the B/OSS and RA community can help.**

**GS:** cVidya and the TMForum are developing some industry standards to measure risk reduction in revenue assurance. We are eager to hear from operators willing to share their knowledge of how much RA risk mitigation and preventive revenue assurance is worth. I encourage those interested in the TMF program to contact Steve Cotton at <mailto:scotton@tmforum.org>.

We already have a first draft document at the TMForum. And I expect we'll have an approved model in 12 months time. When developed, this model will permit RA (and later, fraud management) to speak in the same language as Risk Management. I believe that in the next few years it will become just as important to report the contribution of RA to risk mitigation, as it is to report on leakage found and leakage recovered.

For the original article, please go to: <http://www.billingworld.com/blogs/baker/2011/01/revenue-and-fraud-leaks-measuring-the-risks.aspx>