BeyondFS

Financial Crime Business-Wide Risk Assessments (BWRAs):

A BeyondFS Best Practice Guide

Contents

About the author

Adrian Barnett is an established senior leader with over 20 years' experience spanning financial crime risk, operations, and regulatory consulting. As a Director at BeyondFS, Adrian's expertise covers all major financial crime domains: AML/CTF, sanctions, fraud, anti-bribery & corruption, and tax evasion.

Before joining BeyondFS, Adrian held senior roles including Head of Economic Crime Strategy and Head of CDD at Santander UK, where he shaped firm-wide responses to emerging risks and regulatory expectations. At EY, Adrian spent a decade advising global banks and financial institutions – delivering skilled person (s166) reviews, designing risk frameworks, and lecturing on risk assessment for the International Compliance Association's postgraduate diploma.

With practical insight honed through frontline and advisory positions, Adrian brings a clear, actionable perspective to the challenges of business-wide risk assessment. His credentials include the ICA Certificate in FC Crypto-Asset Risks, a Diploma in Financial Crime Prevention, and a Certificate in Anti-Money Laundering. Adrian is based in London and is a frequent contributor to thought leadership in the UK's financial crime community.

Adrian Barnett
Adrian.Barnett@beyondfs.co.uk

Introduction

To explain why I believe Business-Wide Risk Assessments (BWRA) are so critical, let me share two examples from my own experience.

In one case, I helped a client discover that they owned an entire private bank they didn't even know existed – it only came to light because of a formal BWRA. As you can imagine, with the very high net worth of private banking clients, this is typically one of the highest-risk areas for financial crime.

In another instance, I uncovered that a firm had still been paying a branch manager's salary 25 years after the branch had closed. While not a direct financial crime issue, it shows how the discipline of taking a structured look at the business and its transactions can surface risks and exposures that would otherwise remain hidden.

These examples may sound extreme – but after more than 20 years in financial crime prevention, I can tell you they're not unusual. Risks like these often hide in plain sight unless you take a structured, business-wide view.

That's why a well-run BWRA is one of the most valuable tools you can deploy in your role. Done properly, it's not just about ticking a compliance box – it's about protecting your business, improving decision-making, and making sure your team's resources are targeted at the risks that matter most.

"I've written this guide to help you - as an MLRO, Head of Financial Crime, or someone in a similar role – to improve the way you approach BWRAs, both in terms of quality (so you deliver regulator-ready assessments that genuinely protect your business) and efficiency (so the process is timely, streamlined and useful rather than a burden). My aim is to help you get more value from the effort, so the BWRA becomes a tool you can rely on, not just an obligation you have to meet."

Adrian Barnett
Director, BeyondFS
Adrian.Barnett@beyondfs.co.uk

What is the BWRA?

At its simplest, a BWRA is a risk calculation:

Inherent risk – **Effective controls** = **Residual risk**

> "In conducting a comprehensive risk assessment to evaluate [Financial Crime] risks, a bank should consider all the relevant inherent and residual risk factors at the country, sectoral, bank and business relationship level, among others, in order to determine its risk profile and the appropriate level of mitigation to be applied."
>
> **Basel Committee on Banking Supervision (Jul 2020)**

This statement is as true today as when it was originally published in 2014. (It survives in the updated 2020 guidance).

Inherent risks (a natural or underlying level of risk without any controls or mitigations in place), minus effective controls (controls which have been documented and assessed as adequately managing risk), equals your organisation's residual risk.

The real challenge lies not in the arithmetic, but in ensuring that the inputs are based on accurate, shaped insight.

Crucially, BWRAs are not optional – they are a clear regulatory expectation for every financial services firm, embedded across UK and international frameworks:

- UK Money Laundering Regulations (MLR 2017):
  - Require a business-wide assessment of financial crime risks (Article 18)
  - Mandate regular review and documentation (Articles 27 and 28)
- FCA Financial Crime Guide (FCG):
  - Sets expectations for structured, documented assessments of fraud, bribery, and other risks (sections 2.2.4, 4.2.1, 6.6.2)
- Failure to Prevent Fraud (in force September 2025):
  - Places direct accountability on firms and senior management for ensuring appropriate risk assessments are conducted and signed off each year

To meet these requirements, firms rely on established frameworks and guidance:

- JMLSG Guidance
- Wolfsberg Group
- Basel Committee on Banking Supervision (BCBS)
- As well as: FATF and U.S. FFIEC publications

Taken together, these frameworks ensure your BWRA is robust, defensible and genuinely useful.

In my experience, a well-documented BWRA not only satisfies regulators but also gives leadership genuine visibility and control over the firm's most significant risks.

Step-by-step BWRA Process

A robust Business-Wide Risk Assessment (BWRA) doesn't have to be complicated, but it does need to be systematic. Over years of helping firms, I've found that the most successful BWRAs follow a repeatable process – thoroughly assessing where the real risks lie, which controls actually work, and where action is needed. Here's how to do it:

STEP 0

Step "0": Pre-assessment decision and governance

Governance & Reporting

A BWRA is an intrusive hard look at the structure, products and services of your firm from a financial crime threats perspective. Even though this is Business-as-Usual (BAU) activity and specifically required by law (at least in the UK), it is a good idea to have executive sponsorship to tackle likely issues of data access, issues escalation and general apathy toward the activity. Get clear on how the overall report and conclusions are going to be used: be sure that it is used in the MLRO report and discussed at Executive Committee boards as a minimum.

Timing is always hard, but try to align the anticipated completion of the exercise with the MLRO report and the change planning cycle. This will mean running the risk assessment more like a project than a BAU activity.

Structure

This guide assumes that the general nature and location of the business(es) you are about to assess will be reasonably well-known to you. But a little preparation goes a long way. For example, an updated legal entity structure diagram or document from the Company Secretariat will give a broad indication that your coverage is as expected, with no hidden or unexpected entities in scoped jurisdictions. It might also be useful to contact the finance controller for a breakdown of the firm's cost centres. The finance team will likely already have thought carefully about how the lines of business are broken down and segmented.

STEP 0

Segmentation (assessable units)

The baseline step in any BWRA is understanding – for your specific business – your geographic exposure, customers, sales channels and product lines. The preparation above will support your initial thoughts or give you an up-to-date view to adjust the previous year's coverage. Now you can decide how you are going to segment the business(es) you're going to assess.

These 'assessable units' might be by business lines, geographic regions, product lines, or functional areas / tribes – whatever best fits your firm's profile, approach to risk and operating model. The important thing is to look at the business as it is today, not as it was a year ago, or as you wish it to be. This is a vitally important step so that the baseline of your assessment translates into something that the business owners (Heads of and senior leadership) can recognise.

Invariably one view of the data will not be sufficient when it comes to reporting. Choose the most logical, consistent and balanced approach, and be aware that leadership will ask you to pivot the data from different viewpoints to test conclusion robustness or put a different communication lens on it.

The next step is to gather insights on the inherent risks for each assessable unit.

STEP 1

Step 1: Assess inherent risk

Enterprise Risk Management (ERM) – Risk Taxonomy

If your firm has a documented ERM risk taxonomy, this is a great starting point for understanding which risks have already been identified across the business in relation to financial crime prevention. If not, then start thinking about the risk areas you want to work through with your stakeholders and use broad control areas to batch inherent risks.

As an example, here's a starter on controls areas:

- Anti-Money Laundering & Terrorist Financing (and proliferation financing, if not in your TF definition)
  - CDD / KYC / KYB / KYTP
  - Name Screening
  - Payment Screening
  - Transaction Monitoring
- Fraud
  - Internal
  - External
  - Outbound (e.g. UK failure to prevent offence)
- Sanctions
- Bribery & Corruption
- Tax Evasion

There are likely to be specialist and operational processes that will be relevant to your business, for example:

- Specialist risk areas (depending on your products and services):
  - Market Abuse
  - Trade Based Money Laundering
- Operational areas – risk agnostic / multiple risk nexus:
  - Suspicious Activity Reporting
  - Exits
  - Court Orders

We call this identifying your 'inherent risks' - those that exist before you apply any controls.

STEP 1

Identifying Inherent Risks

Whether you use your firm's risk taxonomy, a pre-defined set of risks, or build a list with stakeholders, the key is to generate a clear list of risks. These should then be tested against your assessable units and either scored (preferably) or mapped against a severity-and-probability matrix.

You can do this through structured questionnaires or, if time is limited, by bringing together stakeholders for a workshop. However you do it, ask direct, challenging questions, and be ready to probe further if something doesn't look right. For example:

- Are there products, services, or locations that bring unique risks?
- Are there risks that rarely get mentioned but could be significant?

Above all, document everything:

- Why you chose your assessable units
- The method you used (workshops, questionnaires, interviews)
- The exact questions asked, and how answers were scored

This transparency is your best defence if ever challenged by a regulator – or by your own board.

STEP 2

Step 2: Map and Test Controls

Once you've identified the inherent risks, the next step is to map the controls which are already in place to mitigate them. Some firms have a formal control library or Risk & Control Self Assessment (RCSA) – if so, start there. If not, you may need to gather this information yourself via further questionnaires or workshops.

To be clear, there is no legal or regulatory requirement to map risks to controls. In fact, the Wolfsberg FAQs (2015) emphasise the holistic nature of the assessment rather than prescriptive mapping. That said, it's worth thinking beyond financial crime. Carrying out this exercise can strengthen alignment with Operational Risk and help you articulate risks at a deeper level within your firm's Enterprise Risk Management taxonomy.

Go beyond simply listing controls. Ask:

- When was each control last tested?
- Who tested it (1LOD assurance team / 2LOD / 3LOD or independent party)?
- What was the outcome of that testing?
- Was the test independent and robust?
- If the control(s) haven't been formally tested but appear in a self-identified issues log, ask: What's the problem, what's the plan to fix it, and what's the timeline?

Cross-check answers with other sources such as recent audit findings or compliance monitoring reports. This step isn't about catching people out – it's about getting an accurate picture of where your control environment is strong, and where it needs work.

STEP 3

Step 3: Scoring your Risk Exposure on a Heat Map

Once you've identified your inherent risks and assessed your controls, the next step is to consolidate everything into a meaningful analysis. This means scoring your risk exposure across the assessable units and capturing the results in either a spreadsheet or a dedicated risk assessment tool.

For consistency's sake, agree on a risk-scoring methodology up front. Whether you use simple 'High/Medium/Low' categories or a more detailed numeric scale, consistency across the business is critical.

When you have your data and scores, you can plot each assessable unit (whether that's a business line, country or product) onto a risk matrix. Most organisations use a 3x3 or 6x6 grid, with probability on the X-axis and severity on the Y-axis.

Top right is your 'danger zone': high likelihood, high impact. This exercise shows where your highest residual risks still pose a threat, after existing controls have been taken into account.

Make sure you:

- Agree scoring logic with senior stakeholders before you start
- Stick to the same scoring and mapping approach each year to track progress and spot trends
- Consider risk-assessment tools that can automate scoring, provide audit trails and produce formatted reports

STEP 4

Step 4: Develop and Deliver an Implementation Plan

For areas that fall into the 'danger zone' on your heat map, you need to dig into the root causes.

Often, it's not that controls are missing, but that they're outdated, not operating consistently, or aren't fit for the current risk.

Develop a clear, actionable remediation plan for each high-risk area:

- What needs to change (e.g. workflow, process, technology, training)?
- Who owns the action?
- What's the timeline for delivery?
- What improvement do you expect to see in risk reduction?

Once changes have been implemented, re-assess and re-score to confirm the risk has actually been reduced.

STEP 5

Step 5: Monitor, Follow Up, and Embed

The real value of an BWRA comes from what happens after the assessment is complete. Set up regular follow-ups with action owners and keep progress visible, for example through change management dashboards or governance meetings.

Importantly, don't let your BWRA become a 'tick-box' exercise that's filed away and forgotten. Treat it as a living programme – one that you revisit at least annually, or whenever a major event (like a new product launch or regulatory change) occurs.

A disciplined, transparent BWRA process isn't just about keeping the regulator happy – it's how you build true confidence that your firm knows where its risks lie and is managing them effectively.

Best practices & common pitfalls

A strong BWRA process is as much about mindset as methodology.

Over the years, I've seen that the difference between a 'tick-box' risk assessment and a genuinely valuable one comes down to a few best practices – and a handful of common traps you need to avoid.

Best practices

Adopt a risk-based approach:

Tailor your BWRA process to your firm's size, complexity and risk profile. For smaller or less complex businesses, a simple, targeted assessment may be enough. For larger, multinational groups, you'll need something far more detailed, likely with regional or business-line granularity.

Fully document your methodology:

Record not just the results, but how you reached them. This includes your choice of assessable units, your scoring approach and the rationale for any changes year on year.

Blend quantitative and qualitative input:

Use both hard data (e.g. loss events, volumes, audit findings) and softer, expert judgment from across the business. This gives a truer picture than relying on numbers alone.

Get control mapping right:

Control mapping is often treated as an afterthought, but it's essential. Map controls to risks clearly and keep the map up to date. Evidence operational effectiveness by maintaining audit trails, tracking testing outcomes and being ready to answer the question, "How do we know these controls work in practice?".

Involve the right people:

Engage stakeholders who genuinely know the risks in their area – not just those with the most senior job title. This often means including operations, technology, and even front-line teams.

Challenge and review:

Don't simply accept the first answer. Healthy challenge – both within the team running the BWRA and from independent oversight (e.g. Internal Audit) – keeps the process honest and robust.

Common Pitfalls to Avoid

Treating BWRAs as a compliance tick-box:

Rushing through the process to meet a deadline, with minimal documentation and no meaningful review, is a wasted opportunity – and a red flag for regulators.

Manual, fragmented processes:

Spreadsheets and email chains create data gaps, conflicting narratives, and inconsistencies across the assessment cycle. BWRA digitisation can help – but only if the underlying processes are sound.

Ignoring emerging risks:

It's easy to focus on known risks and miss new or evolving threats – like cryptoassets, digital ID fraud, or geopolitical sanctions. Build in a mechanism to scan for emerging risks.

Lack of clear accountability:

Action plans that are too vague, or have no clear owner, almost always stall. Make sure every change initiative is assigned and tracked.

Letting the BWRA gather dust:

The process shouldn't end once the document is filed. If you're not using your BWRA to drive decision-making, you're missing its real value.

Summary & next steps

A well-run BWRA should be a cornerstone of your financial crime risk management, not just a regulatory chore. It gives you the insight to allocate resources where they matter most and the confidence to defend your approach to both your board and your regulators.

Remember:

- An BWRA is a process, not a one-off project. Keep your methodology transparent, your results clearly documented, and your action plans live and accountable.
- Prioritise clear documentation, strong data and regular evidence of improvement – especially around control effectiveness.
- Use your BWRA to challenge assumptions, surface hidden risks, and drive continuous improvement – not just to satisfy the regulator, but to give your board and stakeholders genuine confidence in your control environment.

Next steps:

- Benchmark your current BWRA approach against the steps and best practices in this guide.
- Identify your main gaps – whether in scope, documentation, stakeholder involvement or follow-up.
- Involve the right people early for your next BWRA cycle, including from business, risk, audit, operations and technology teams.
- Set clear ownership for remediation, and establish a process for tracking progress throughout the year.

If you want independent support – whether it's a fresh look at your existing approach, a new methodology, or simply an expert sounding board – we're here to help.

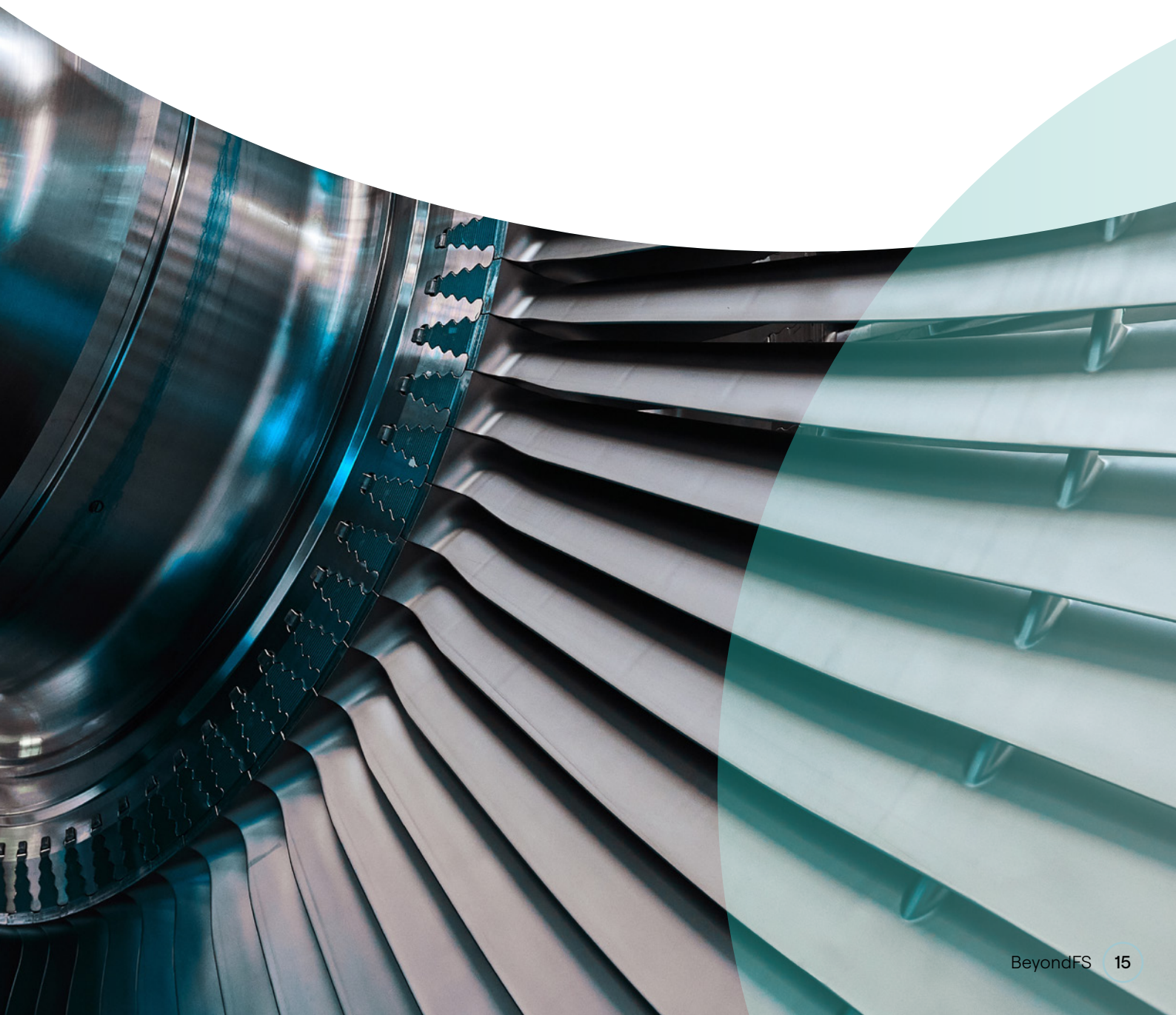
Ultimately, a strong BWRA is how you turn regulatory obligation into strategic advantage. Make it count.

About BeyondFS

At BeyondFS, we help banks build Financial Crime programmes that reduce risk, satisfy regulators, and restore confidence.

We don't just advise - we deliver. Our senior teams bring clarity, focus and momentum when programmes are under pressure, turning strategy into results that stand up to scrutiny.

A core part of our work is Advisory & Regulatory Response - helping clients stay ahead of regulatory demands while building stronger, more resilient frameworks.



Our Advisory & Regulatory Response Services

Regulatory Response

- Inspection and review preparation
- Mock interviews, training and briefings
- Support with regulator scope (e.g. VREQs, s166)
- Regulator-ready documentation

Horizon Preparation

- 3-year Regulatory Radar to anticipate change
- Map new rules to your controls
- Translate policy shifts into practical steps

Risk Assessment (CRA & BWRA)

- Proven methodology and scoring approach
- Build or calibrate risk frameworks regulators trust
- Simplify models for sustainability

Gap & Control Reviews

- Independent gap and model reviews
- Actionable roadmaps for remediation
- Strong foundations for long-term compliance

BeyondFS

Contact

BeyondFS
Dawson House, 5 Jewry St, London
EC3N 2EX, United Kingdom

+44 (0)203 637 4117
info@beyondfs.co.uk
beyondfs.co.uk