Ask eRMA

ONE-PAGE BRIEF

BUSINESS CONTINUITY · RISK · COMPLIANCE

Resilience, risk and compliance belong on one platform

Three teams describe the same services, vendors and controls in three tools. Each tool is consistent. Together they rarely agree.



What goes wrong when they live apart

- **One vendor, three ratings:** critical in the BIA, moderate in the risk register, compliant in the audit file.
- **One control, three tests,** by three teams with three sets of evidence.
- **Gaps between tools:** a high risk with no plan, an obligation with no tested control.
- **Evidence by hand** for every audit and regulator request.

What "integrated" should mean

1 One set of records

Services, processes, applications, sites and vendors exist once. BIA, risk and compliance link to them.

eRMA → One connected model; Risk Assessment in core

2 Test once, use many times

One control test supports a risk treatment, several obligations and continuity assurance.

eRMA → Control tests and attestation

3 Gaps visible across teams

A high risk with no scenario or plan behind it shows as a gap, whoever owns it.

eRMA → Coverage gaps flagged

4 Shared data, own accountability

Each function keeps its own rights and decisions. Sensitive risks stay restricted.

eRMA → Rights through teams; Restricted risks

5 Traceable both ways

From a regulation to its control and evidence; from a service to all it must meet.

eRMA → Rule to control to evidence

6 Add modules, not copies

Start with continuity; add risk and compliance later, on the data already entered.

eRMA → ERM and GRC on the same records

Three questions to ask any vendor

1. **Show one vendor everywhere.**
   In the BIA, risk register and compliance view: one record or three?
2. **Show one test, many uses.**
   A single control test behind a risk treatment and several obligations.
3. **Show a gap between teams.**
   A high risk with no plan: is it flagged, and who sees it?

DOWNLOAD
The eRMA brochure
ebrp.net/brochure

JOIN
The next live showcase
ebrp.net/webinar