

FEASIBILITY STUDY · EFESTO

Feasibility study: network analysis and penetration test

What Voltaria asks for, what can be done and under which conditions: the document that precedes the kick-off and from which the analysis and test report is born.

CLIENT

Voltaria Distribuzione S.p.A. (example)

SECTOR

Wholesale distribution of electrical materials and lighting

DATES

Request 9 March 2026 · site visit 17 March · delivery 31 March 2026

VERSION

1.0 · complete document

REFERENCES

Study SF-2026-014 · resulting mandate VD-2026-031

OUTCOME OF THE STUDY

Feasible with conditions · option C recommended

VALIDITY

60 days from delivery (until 30 May 2026)

PREPARED BY

BoNet™ — a Euro Buchberger project

Demonstration document. Company name, people, connectivity suppliers, addresses, numbers, requests and assessments described in this study are invented for illustration and do not refer to any real client. BoNet™ publishes it as an example of how, starting from a client's requests, one arrives at deciding whether and how a network analysis and penetration test engagement is feasible. The study has a companion document: the report of the analysis and tests carried out on the same network.

How to read this study

CHAPTER 1 · COLOUR AND SYMBOL CONVENTION

The colours are the same as in the analysis and test report that follows from it. Every colour is always accompanied by a text or a code, so the document stays readable in black and white.

1.1 Feasibility verdicts

Every assessment has a verdict, in the family of blues and purples (like the “strength” and “to be decided at kick-off” boxes).

Verdict	What it means
✓ FEASIBLE	It can be done as it stands, without particular conditions.
ⓘ WITH CONDITIONS	It can be done provided the listed conditions are met. Every condition becomes a point to confirm at the kick-off.
? TO BE EXPLORED	Information is missing to decide: the study says which and who can supply it.
✗ NOT FEASIBLE	As it stands it cannot be done: the study proposes an alternative.

1.2 Project risk levels

Project risks (chapter 8) use the warm colours of the report's severity scale.

Level	Meaning
CRITICAL	Can cause a total outage or data loss; the project does not start until it is governed.
HIGH	Serious impact on the service; a specific measure is needed before starting.
MEDIUM	Limited impact or particular conditions; measure provided in the plan.
LOW	Minimal impact; followed during the project.

1.3 Network zones and links

The diagram in chapter 4 colours each zone: INTERNET AND SUPPLIERS CLIENT EDGE FIREWALL DMZ CORE · CED USERS IP TELEPHONY PRINTERS CAMERAS GUEST WI-FI BONET TOOLS. Gold is reserved for BoNet™. Links are distinguished by the type of line (fibre, copper, VPN, failover, test link), not by colour.

1.4 Boxes and codes

NOTE Clarifications and definitions of technical terms.	ATTENTION A point that requires care, without being a prohibition.	STOP · LIMIT NEVER TO BE CROSSED What is never done. Bright red is reserved for this use.
TO BE DECIDED AT KICK-OFF A condition or an assumption that the client and BoNet™ confirm together.	✓ STRENGTH A successful choice in the client's infrastructure.	BONET TOOLS AND ACTIVITIES What BoNet™ installs and what it does.

Summary and recommendation

CHAPTER 2 · FOR MANAGEMENT, ON ONE PAGE

Voltaria asked us to understand **whether its network withstands a failure and an attack**, and to be able to show it to clients and the insurer. After gathering information and making a site visit, the engagement turns out to be **feasible with conditions**.

VERDICT

FEASIBLE WITH CONDITIONS

We recommend **option C**: seven-level network analysis plus a full penetration test (Efesto, Advanced level), with a test unit in the CED and six test points on the floors. It is the only option that answers all eleven of Voltaria's requests.

2.1 Why it is feasible

- The network is **well designed**: four lines on two suppliers, BGP, firewalls and cores in pairs, dual power, two REI120 risers. This makes the tests safer, because many failures are already covered.
- The **site visit of 17 March** showed that the test unit fits in the CED, that the spare routes exist (4 pairs in riser 1 and 3 in riser 2) and that 5 of the 6 candidate switches have a free fibre port.
- The **contacts** (sponsor, technical contact, privacy officer, facilities manager) have been identified and are available.

2.2 The five conditions

#	Condition	Who	By
1	Backup verified before starting : a complete restore test succeeded (the last one dates back 14 months).	Voltaria's technical contact	20 April 2026
2	Written consent of the two connectivity suppliers to the checks on the external perimeter.	Voltaria, with the suppliers	21 April 2026
3	Out-of-hours windows for the risky tests: from 20:30 to 6:00, because orders close at 18:00 and shipments at 20:00.	Sponsor	Kick-off
4	Dedicated power and cooling for the test unit in the CED (about 200 W).	Facilities manager	Day G1
5	Electrician and cabler available on days G1 and G12, on call within 2 hours on the other days.	Facilities manager	Kick-off

11
VOLTARIA'S
REQUESTS

12
ON-SITE TEST DAYS

6
POINTS UNDER TEST

≈ 41
BONET™ PERSON-
DAYS

9
PROJECT RISKS

Proposed schedule: kick-off on 28 April 2026 · tests from 11 to 26 May · report on 8 June · handover on 10 June · thirty-day check on 8 July.

TO BE DECIDED · WHAT WE NEED FROM VOLTARIA

The **acceptance of option C** by 14 April 2026, the **appointment of the contacts** and the start of the two conditions with the nearest deadline (backup and supplier consents). The financial quotation is a separate document, requested following acceptance.

What Voltaria asks for

CHAPTER 3 · THE CONTEXT AND THE ELEVEN REQUESTS

On 9 March 2026 Voltaria's general manager wrote to BoNet™ to ask for a network analysis and a penetration test. It is not a theoretical exercise: it is the answer to four needs coming from the market and from management.

3.1 Why now

Reason	What happened
Clients ask for proof	Two large chains of installers and a group in specialised large-scale retail have added to the annual supplier questionnaire a section on information security, asking for evidence of an independent test .
Cyber insurance	The renewal of the cyber policy, in September, requires the declaration of a penetration test carried out in the last twelve months .
The new order portal	In July Voltaria opens a B2B ordering portal to installers: the public website and the mail become more important for revenue.
Management wants certainty	The board asks: "if a failure or an attack hit the head office, what would happen to orders?"

3.2 The requests

ID	Voltaria's request	Where it comes from	Priority
R1	To know whether the network withstands the failure of a component (a line, a core, a firewall, a floor switch) without halting orders .	Board of directors	High
R2	To understand how exposed to an attack from the Internet the network is: website, mail, branch VPNs, published services.	Insurance, clients	High
R3	To understand whether a compromised device on a floor — or a visitor connected to the Wi-Fi — could reach the critical systems .	Board of directors	High
R4	To have an up-to-date, verified inventory of devices, services and links: today the documents are not aligned with reality.	IT manager	Medium
R5	To verify that the VPNs of the 40 branches are secure and that a compromised branch does not reach the head office.	Insurance	High
R6	To verify the state of the backups and the ability to restore after a failure or an attack.	Board of directors	High
R7	To obtain a report and a summary attestation to show to clients and the insurer, with method and evidence.	Clients, insurance	High
R8	No halt to orders during working hours: orders are received from 8 to 18 and shipments close at 20.	Sales management	High
R9	A remediation plan with priorities and times, and a check after the fix.	IT manager	Medium
R10	Knowledge transfer to the two internal technicians: what emerged, what to do and how to repeat the tests.	IT manager	Medium
R11	Confidentiality and compliance with personal-data law throughout the work.	Privacy officer	High

NOTE · WHAT VOLTARIA DOES NOT ASK FOR

Not requested: phishing or social engineering simulations on staff; physical intrusion tests in the building; analysis of the code of the business applications; tests on third-party cloud services. They can be the subject of a later engagement, if management wishes.

Voltaria's network

CHAPTER 4 · THE STARTING POINT OF THE STUDY

The study starts from the network as Voltaria described it to us and as we observed it during the site visit. The network does not change in the engagement: the aim is to analyse and test it, not to modify it. The diagram on the next page is the same one you will find in the report.

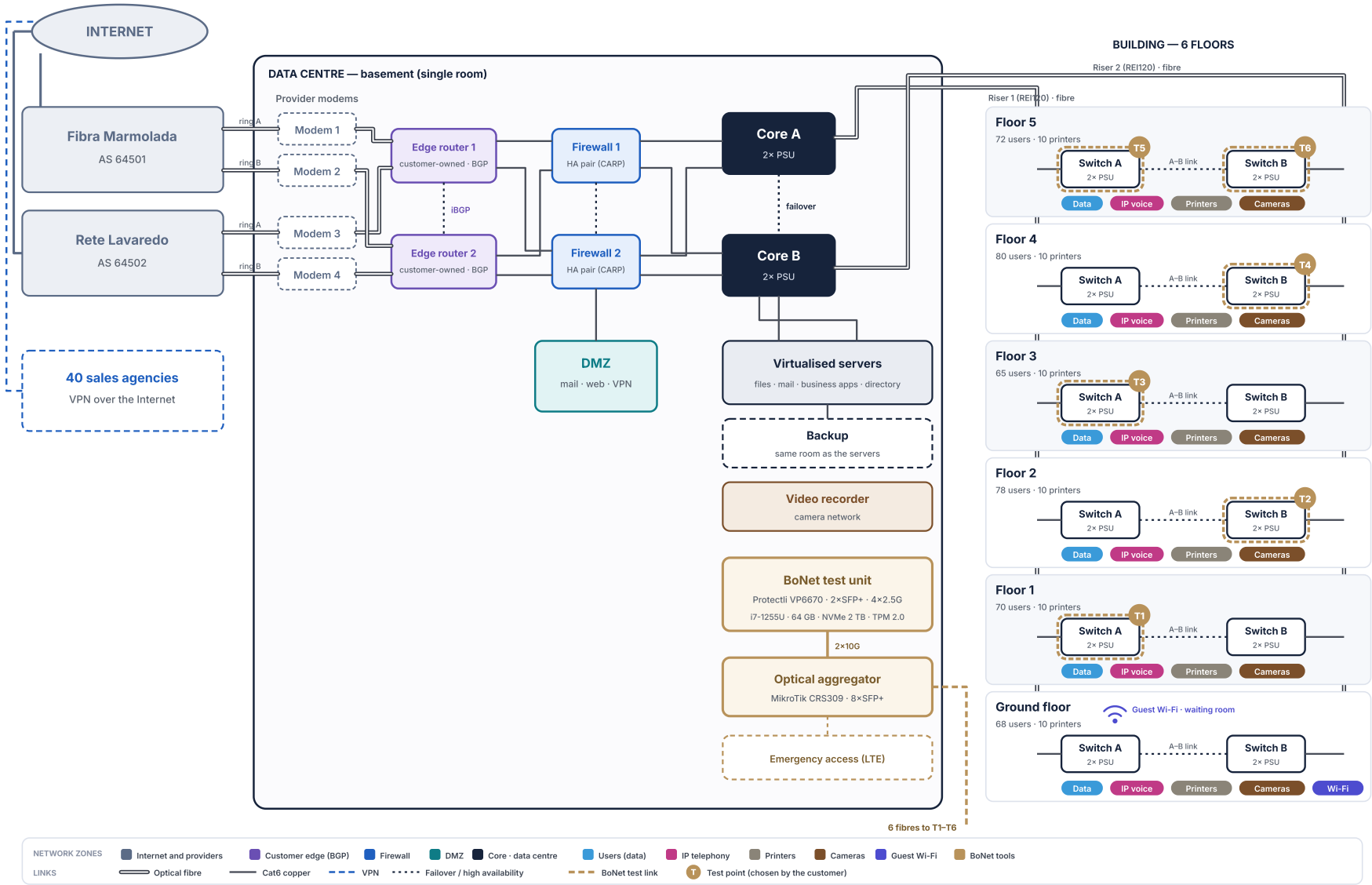
Element	Description
Internet access	4 fibre lines at 1 Gbit/s: 2 for each of the two suppliers (Fibra Marmolada and Rete Lavaredo), on two different terrestrial rings per supplier; 4 supplier modems.
Edge and security	2 client edge routers as a pair (outside the DMZ), BGP with the suppliers (AS 64500; block 203.0.113.0/24, documentation numbers); 2 firewalls in high availability; DMZ; 40 VPNs to the branches.
Data centre	A single room on the basement floor: 2 cores in failover, 3 virtualisation servers (14 virtual machines: files, mail, business applications, directory), backup system and video recorder. Dual power supply on all devices.
Building	6 floors (ground floor and 1–5), 2 switches per floor on different cores and linked to each other; 433 users (65–80 per floor), 433 IP phones, 60 printers, 56 cameras on dedicated networks. Fibre on two REI120 risers; horizontal Cat6 copper.
Wi-Fi	Guests only, in the ground-floor waiting room, on an isolated network.

4.1 What we know and what remains to be verified

Information	Source and reliability	Status
Logical network diagram	Voltaria's document, updated two years ago; confirmed by sampling at the site visit.	🕒 TO BE UPDATED
Spare routes in the risers	Site visit of 17 March: 4 pairs in riser 1 and 3 in riser 2, labelled.	✓ VERIFIED
Free fibre ports on the switches	Checked on 6 candidate switches: 5 have a free SFP+ port; one (floor 3) does not.	🕒 TO BE SOLVED
CED power	Electrical diagram supplied; the two power supplies of the cores appear to be on the same UPS (to be confirmed).	? TO BE EXPLORED
Last trial restore of the backups	Technical contact's statement: 14 months ago.	🕒 TO BE REDONE
Configuration of firewalls and edge routers	Not yet examined: it will be the subject of day G2.	? TO BE EXPLORED

CHAPTER 4 · NETWORK DIAGRAM

From the four lines to the twelve floor switches



The diagram shows Voltaria's network and, in gold, the BoNet™ tools **foreseen** by option C: the test unit in the CED, the optical aggregator with six fibres to the points under test T1-T6 (one on floors 1-4, two on floor 5) and the emergency access. Colours follow the convention of chapter 1.

Objectives and scope

CHAPTER 5 · WHAT WE WANT TO ACHIEVE, AND WHERE WE STOP

From the eleven requests we derived five measurable objectives, a precise scope and a list of assumptions. The assumptions are what we took as true in order to conclude that the engagement is feasible: **at the kick-off they are verified one by one.**

5.1 Objectives and success criteria

#	Objective	How we will know we have achieved it	Requests
O1	Know the network as it is	Inventory and diagram verified in the field, with the differences from Voltaria's documents listed and corrected.	R4
O2	Measure fault tolerance	For every duplicated component (line, router, firewall, core, switch) we know what happens if it stops, with a switchover test in a protected window.	R1, R6
O3	Test the exposure to attacks	From outside (Internet, VPN) and from inside (six points on the floors, guest Wi-Fi): every weakness has severity, evidence and impact documented.	R2, R3, R5
O4	Be able to demonstrate it	Complete report, evidence log and summary attestation ready for clients and the insurer.	R7, R11
O5	Remediate and hand over	Remediation plan with priorities and times, handover to the internal technicians, check after the fix.	R9, R10

Request R8 (no halt to orders) is not an objective but a **constraint** that governs the whole project: see 5.3.

5.2 Scope

Inside the scope

- The head-office network: from the edge to the six floors.
- The four lines, the edge routers and the firewalls (read-only checks on BGP).
- The DMZ and the published services (website, mail, VPN concentrator).
- The VPNs to the 40 branches, from the head-office side.
- The CED: cores, servers, backup, video recorder.
- Six floor switches chosen by the client (T1–T6).
- Guest Wi-Fi, the camera, printer and phone networks.

Outside the scope

- The internal networks of the 40 branches.
- Third-party systems (connectivity suppliers, cloud services).
- Staff: no phishing simulation.
- The building: no physical intrusion tests.
- The code of the business applications.
- Tests that saturate lines or systems (denial of service).
- Changes to production configurations.

5.3 Constraints

Constraint	What it entails
Working hours (R8)	Orders from 8 to 18, shipments until 20: risky tests are done from 20:30 to 6:00 or on quieter days.
Single CED	One room for cores, firewalls, servers and backup: an event in the CED stops everything, so tests in the CED have the recovery plan already open .
REI120 risers	Fire compartments are not opened: only existing passages are used, and only the cabler touches the openings.
Third parties	The written consents of the connectivity suppliers are needed; the building owner must be informed.
Personal data (R11)	Tests are carried out without reading or copying data: evidence is reduced to a minimum and kept encrypted.

5.4 Assumptions to confirm at the kick-off

TO BE DECIDED AT KICK-OFF · THE STUDY'S ASSUMPTIONS

1. The spare routes in the risers (4 pairs + 3) are **free and usable** without reducing the spare capacity below the agreed limit.
2. For the floor 3 switch an **adapter** on an access port is enough, at a lower speed.
3. The **backup** can be restored: the restore test will be redone by 20 April.
4. The **two suppliers** give written consent by 21 April.
5. The CED can host the test unit with a **dedicated power supply** (about 200 W) and without exceeding the agreed temperature.
6. Electrician and cabler are **available** on days G1 and G12.

The intervention options

CHAPTER 6 · THREE WAYS OF ANSWERING THE REQUESTS

To answer Voltaria's requests we evaluated three options, from the lightest to the most complete. There is no "right" option in absolute terms: it depends on how many requests one wants to meet and how much effort the site can sustain.

A · Network analysis	B · Analysis + external test	C · Analysis + full test recommended
What. The seven analyses, desk-based and from the CED: inventory, topology, performance, security and segmentation, configuration, reliability, intervention plan. What it does not do. No attack tests and no switchover tests. On site. 4 days, all during working hours. Operational risk. LOW	What. Option A plus the external penetration test (Standard level): perimeter, DMZ, branch VPNs, guest Wi-Fi. What it does not do. It does not test what a device already inside the network could do, nor the floors. On site. 6 days, some outside office hours. Operational risk. MEDIUM	What. Option A plus the full penetration test, Advanced level: from outside and from inside, with the test unit in the CED and six test points on the floors, failover test and check after the fix. What it requires. Hardware in the CED, routes to the floors, out-of-hours windows, kick-off and recovery plan. On site. 12 full days. Operational risk. HIGH (only G8 and G11, controlled)

6.1 Which requests each option meets

Request	A	B	C
R1 · Fault tolerance	●	●	✓
R2 · Exposure from the Internet	—	✓	✓
R3 · Compromised device on the floors	—	●	✓
R4 · Verified inventory	✓	✓	✓
R5 · Branch VPNs	●	✓	✓
R6 · Backup and restoration	●	●	✓
R7 · Report and attestation	●	●	✓
R8 · No halt to orders	✓	✓	✓ (with kick-off and recovery)
R9 · Remediation plan and check	●	●	✓
R10 · Knowledge transfer	✓	✓	✓
R11 · Confidentiality and personal data	✓	✓	✓
Requests met	4 of 11 (+5 in part)	6 of 11 (+5 in part)	11 of 11

✓ met · ● partly met · — not met.

✓ **RECOMMENDATION**

We recommend **option C**: it is the only one that answers all the requests, and the two riskiest days (G8 and G11) are governed with the measures of chapter 8. If management prefers a smaller commitment, option B is the second choice: it leaves uncovered attacks from the inside and failover tests (R1, R3, R6).

6.2 How we reach the six points under test

Option C requires reaching six floor switches chosen by Voltaria (T1–T6: one on floors 1–4, two on floor 5). At the site visit we found the conditions for the **main approach**: using the spare routes that Voltaria has already set up. If at the kick-off they turned out not to be usable, we move to dedicated runs or to the mobile unit (described in the report, chapter 7). For the floor 3 switch, which has no free fibre port, an adapter on an access port is used.

Feasibility assessment

CHAPTER 7 · OPTION C, DIMENSION BY DIMENSION

We evaluated option C from ten points of view. The overall result is **🔦 FEASIBLE WITH CONDITIONS**: no dimension is “not feasible”, seven require conditions, two are feasible as they stand and one is to be explored. The conditions are those of chapter 2 and become points to confirm at the kick-off.

Dimension	Verdict	Rationale	Condition / what is needed
Technical · installation in the CED	🔦 WITH CONDITIONS	The test unit (Protectli VP6670, up to 100 W) and the optical aggregator fit in the rack indicated at the site visit.	Dedicated power (about 200 W with the UPS) and temperature reading before and after.
Technical · links to the floors	🔦 WITH CONDITIONS	Existing spare routes (4 + 3 pairs); 5 switches out of 6 with a free fibre port.	Authorisation to use the spare; adapter for the floor 3 switch.
Operational · time windows	🔦 WITH CONDITIONS	Orders until 18:00 and shipments until 20:00: risky tests are possible only at night.	Windows from 20:30 to 6:00 for G6–G8 and G11; BoNet™ on site.
Organisational	✓ FEASIBLE	Sponsor, technical contact, privacy officer and facilities manager are identified and available.	Formal appointment at the kick-off.
Legal and contractual	🔦 WITH CONDITIONS	The tests on the external perimeter involve third-party lines.	Written consent of the two suppliers; non-disclosure agreement; signed mandate; insurance at Voltaria's expense, as per the mandate; Voltaria informs its insurer in writing of the testing activity.
Personal data	🔦 WITH CONDITIONS	The networks and systems contain data of employees, clients and agents.	Assessment by the privacy officer; tests without reading data; evidence encrypted and kept for a defined time.
Service continuity	🔦 WITH CONDITIONS	The risk of an interruption exists, but it is manageable: the network is already redundant and there is a recovery plan.	Backup restore test successful before G1; recovery plan signed.
Timing	✓ FEASIBLE	Calendar compatible with Voltaria's activities: tests end before the order portal opens (July).	Avoid the quarter-end closing days.
Third-party dependencies	🔦 WITH CONDITIONS	Connectivity suppliers, electrician and cabler must be reachable.	Dedicated support numbers; on call within 2 hours.
Economic	? TO BE EXPLORED	The effort (about 41 person-days) is proportionate to the value to be protected; the amount depends on choices on cabling and licences.	Separate quotation after acceptance of the option.

NOTE · WHY THE CONDITIONS ARE GOOD NEWS

The conditions are not obstacles: they are what makes the test **safe**. The same list that we call “conditions” here becomes, at the kick-off, the list of decisions and prerequisites signed by the two parties.

Project risks

CHAPTER 8 · WHAT CAN GO WRONG, AND WHAT WE DO

An invasive engagement has risks of its own, different from those of the network. We have listed them with the risk level, the planned measure and the owner. The measures are the same ones found in the kick-off and in the recovery plan of the report: this chapter is the **risk register they start from**.

ID	Risk	Probability · impact	Level	Planned measure	Owner
RP-01	Service interruption during an invasive test (G8, G11).	Low · High	MEDIUM	Night windows, recovery plan open, BoNet™ on site, immediate stop.	BoNet™ + technical contact
RP-02	Backup that cannot be restored , discovered during a recovery itself.	Medium · High	HIGH	Complete restore test successful before G1 (condition 1). Without it, the project does not start.	Technical contact
RP-03	Overheating or electrical overload in the CED from the test hardware.	Low · High	MEDIUM	Dedicated power, UPS, temperature threshold, shutdown of the unit (also remotely with the LTE access).	Facilities manager + BoNet™
RP-04	A supplier does not give consent to the checks on the external perimeter.	Medium · Medium	MEDIUM	Early request (by 21 April); otherwise the tests on that line are excluded and this is declared in the report.	Sponsor
RP-05	Spare routes not usable or not sufficient.	Medium · Low	LOW	We move to dedicated runs or to the mobile unit (report, chapter 7).	Cabler + BoNet™
RP-06	Exposure of personal data during the tests.	Low · High	MEDIUM	Tests without reading data, encrypted evidence, restricted access, opinion of the privacy officer.	Privacy officer
RP-07	A security incident already in progress is discovered .	Low · High	MEDIUM	Stop; immediate information to sponsor and privacy officer; the notifications required by law are the controller's responsibility.	Sponsor + BoNet™
RP-08	Delays : late authorisations, electrician or cabler not available.	Medium · Low	LOW	On call within 2 hours; calendar with spare days; second date for G1 and G12.	Facilities manager
RP-09	Voltaria's cyber policy does not cover the damage of a test not declared to the insurer.	Medium · High	HIGH	Insurance is at Voltaria's expense, as per the mandate. Before G1 Voltaria informs its insurer in writing of the testing activity and keeps the reply.	Sponsor

RULE OF ENGAGEMENT · THE PROJECT DOES NOT START IF

the backup restore test has not succeeded (RP-02), the written consents of the suppliers have not arrived (RP-04), Voltaria's insurer has not been informed (RP-09) or the recovery plan has not been signed by the sponsor and the technical contact.

8.1 How the risk level is read

The level is the result of two assessments: **how likely** it is that the event happens (low, medium, high) and **how much it would weigh** on Voltaria (low, medium, high). Low probability and high impact give a **MEDIUM** risk; medium probability and high impact give a **HIGH** risk, which requires a specific measure **before** starting. None of the nine risks is **CRITICAL** once the measures are applied.

Outline plan and effort

CHAPTER 9 · WHEN, WITH WHOM AND HOW MUCH WORK

The plan that follows is **an outline**: dates are confirmed at the kick-off, when the assumptions of chapter 5 are verified. It runs from the study to the check after thirty days.

STUDY 9–31 March Request, site visit, feasibility study	AGREEMENT 14 April Acceptance of the option and signing of the mandate	PREREQUISITES 20–21 April Backup restore test; supplier consents	KICK-OFF 28 April Assumptions confirmed, limits and recovery signed	TESTS 11–26 May 12 days (G1–G12)	DELIVERY 8–10 June Report and handover	CHECK 8 July Tests repeated after the fix
---	--	--	---	--	--	---

9.1 Milestones and documents

When	Milestone	Document or result
9 March 2026	Request from Voltaria's general manager; first meeting on 12 March; information-gathering questionnaire.	Written request; completed questionnaire (24 March)
17 March 2026	One-day site visit: CED, risers, three floors.	Minutes and photos of the site visit
31 March 2026	Delivery of this study.	Feasibility study SF-2026-014
14 April 2026	Acceptance of option C and signing of the mandate.	Mandate VD-2026-031
20–21 April 2026	Backup restore test; written consents of the suppliers.	Restore minutes; two consent letters
28 April 2026	Project kick-off : confirmation of the study's assumptions, roles, limits, stop, recovery.	Signed kick-off minutes
11–26 May 2026	Twelve test days (G1–G12), with the BoNet™ project manager on site for every recovery or emergency.	Evidence log
8 June 2026	Delivery of the analysis and test report.	Complete report (Italian and English)
10 June 2026	Handover : delivery and transfer to the IT team (half-day workshop).	Delivery minutes; traceability matrix
8 July 2026	Follow-up check after thirty days.	Update of the report

9.2 Estimated effort

Activity	BoNet™ days	Effort required from Voltaria
Feasibility study (meeting, site visit, drafting)	3	Technical contact: 1 day
Kick-off	2 (2 people × 1 day)	Sponsor, technical contact, privacy officer, facilities manager: half a day

Activity	BoNet™ days	Effort required from Voltaria
On-site tests (G1-G12)	24 (2 people × 12 days)	Technical contact: present or on call; facilities manager: G1 and G12; electrician and cabler: G1 and G12 on site
Analysis, drafting and report	8	Clarifications, review of the draft
Handover	2 (2 people × 1 day)	Sponsor, IT team, privacy officer: half a day
30-day check	2	Technical contact: 1 day
Total	≈ 41 person-days	—

The financial commitment is defined in a separate quotation, after acceptance of the option.

From the study to the kick-off and the handover

CHAPTER 10 · THE THREAD THAT TIES THE THREE DOCUMENTS TOGETHER

The feasibility study is not an isolated document: it is the **first link** in a chain of three. What is promised here is verified at the kick-off and accounted for at the handover. This chapter shows where.

1 · FEASIBILITY STUDY 31 March Requests R1-R11, assumptions, conditions, risks, options	2 · KICK-OFF 28 April Assumptions and conditions are verified; limits, stop and recovery are signed	3 · HANDOVER 10 June Every request is accounted for with the traceability matrix
---	---	--

10.1 What passes from the study to the kick-off

At the kick-off of 28 April the study is the **first item on the agenda**. We proceed as follows:

From the study...	...to the kick-off
The requests R1-R11 (ch. 3)	They are confirmed or corrected, one by one. Those confirmed become the scope and objectives of the mandate.
The assumptions (ch. 5.4)	They are verified on site: spare routes, free fibre ports, CED power, availability of electrician and cabler.
The five conditions (ch. 2)	They become the signed prerequisites : backup restore test, supplier consents, night windows, dedicated power, on-call availability.
The risk register (ch. 8)	It feeds the operating limits, stop conditions and recovery plan of chapter 4 of the report.
The option chosen (ch. 6)	The days, the six points under test and the choice of cabling to the floors are fixed.

10.2 What passes from the study to the handover

At the delivery of 10 June every request of the study receives an **outcome**, reported in a traceability matrix: from the request to the chapter of the report that covers it, down to the result. Requests not fully met, or that depend on a fix still to be made, are declared and deferred to the follow-up check after thirty days.

BONET™ TOOLS AND ACTIVITIES · WHO SIGNS WHAT

The feasibility study is signed for acceptance by Voltaria's sponsor. The kick-off minutes are signed by the sponsor and the technical contact. The delivery minutes (handover) are signed by the sponsor and the BoNet™ project manager. Each document refers to the previous one by its number.

10.3 Acceptance of the study

With the signature below Voltaria accepts **option C** described in this study, under the conditions listed in chapter 2, and requests the issue of the quotation and the mandate. Acceptance does not yet authorise any activity in the field: these start only after the kick-off and the signed minutes.

For Voltaria Distribuzione S.p.A. — General manager
Date and signature

For BoNet™ — Project manager
Date and signature

Appendix A · Glossary

Term	Meaning
Codes	R1-R11: Voltaria's requests · RP-01... : project risks · G1-G12: test days · T1-T6: points under test · SF-2026-014: this study · VD-2026-031: the resulting mandate.
BGP	The system by which a company tells its connectivity suppliers its public addresses: if one line drops, traffic goes over the other without changing addresses.
CED	Data centre (centro elaborazione dati): the room that hosts cores, servers and backup.
DMZ	An intermediate zone between the Internet and the internal network, with the services reachable from outside.
Failover	Automatic switch to a spare device or line when the one in use fails.
Handover	Delivery and transfer: the moment when BoNet™ returns everything to Voltaria and passes the knowledge to the internal team.
Kick-off	Initial meeting, and signed minutes, in which roles, limits, stop conditions and recovery are set.
Penetration test	An authorised and controlled test in which an attempt is made to exploit weaknesses to show their real effect.
REI120	A compartment fire-resistant for 120 minutes: it is neither opened nor drilled.
SFP+	A module that, inserted in a port of a switch or a unit, makes it a 10 Gbit/s fibre port.
VPN	An encrypted link across the Internet, used here between the branches and the head office.