Security, data and integration

On 19 July 2024, thousands of passengers at Palma airport queued for hours at the check-in desks. There was no attack. A faulty update of CrowdStrike Falcon, a security program, had crashed about **8.5 million Windows computers** around the world, according to Microsoft. Aena switched to manual procedures. One piece that everything depended on fell, and everything that was connected to it stopped.

Every technology you added to your plan in the last lesson brings two gifts: **new data**, which you have to manage, and **new doors**, which someone has to lock. And all of it has to be connected, so you also have to know what happens when one piece fails.

What you will learn

- Find the possible **security gaps** of each area of your plan, starting from your D5 passive audit, and give each one a measure
- Define how each new kind of data is **treated** along its lifecycle
- Give each strategic goal an **indicator** with a formula and a data source
- Draw the **integration diagram** of data, applications and platforms in diagrams.net, with the **source of truth** of each piece of data
- Avoid the trap of generic measures (“install an antivirus”) that answer no specific gap

Locks for every neighbourhood

In the city-builder, cybersecurity is the police, the walls and the locks. A new neighbourhood without them is an invitation.

> A **security gap**, in this unit, is a weak point of an area: something that could go wrong with its data or systems, by attack, by mistake or by accident.

Do not confuse it with a **personal data breach**: that is an incident that has already happened, which the RGPD (Regulation (EU) 2016/679, article 33) says must be notified to the authority “without undue delay and, where feasible, not later than 72 hours” after the company becomes aware of it. Your plan analyses the gaps so that the breaches do not happen.

For each area: **which asset or data is there, what could go wrong, what measure you put in, and which law applies.**

Area	Asset or data	Possible gap	Measure	Law
Orders	B2B portal with hotel accounts	Hotel reception staff share one password	One account per person, MFA, access log	RGPD (contact data)
Ovens	IoT meters on the bakery network	Devices with factory passwords on the same network as the office	Separate network for OT, change credentials	—

Area	Asset or data	Possible gap	Measure	Law
Quality	Temperature records	A sensor fails and nobody notices that the records stopped	Alarm when data stop arriving, daily copy	Food safety rules
All	Third-party cloud services	Dependence on the provider	Own backups, contract and data location checked	RGPD, NIS2 if it applies

The starting point for your company is the **passive audit** of D5: the security headers, cookies and privacy policy of its public website.

> **Passive only**
> Everything you say about the real company's security comes from what its website shows to any visitor: securityheaders.com, Mozilla HTTP Observatory, the browser's DevTools, the cookie banner, the privacy policy. Never scan it, never probe ports, never try a login.

> **Careful: "install an antivirus"**
> A measure that does not answer a specific gap is decoration. If you cannot say which gap a measure closes, delete it.

Data in, decisions out

Each new technology produces new data: portal orders, oven consumption, cold-room temperatures. Two things must be defined for each.

Treatment. The lifecycle you used in D5: how it is collected, where it is stored, who can access it, how long it is kept and how it is deleted. If it is personal data, the RGPD and the LOPDGDD (Ley Orgánica 3/2018) apply.

Analysis. The data must tell you whether the goals are being met.

> An **indicator** (or **KPI**, key performance indicator) is a number, calculated with a fixed formula from data you have, that shows whether a goal is being reached.

In the city-builder, indicators are the info-view overlays: traffic, pollution, happiness. Each goal of section 1 needs at least one.

Goal	Indicator and formula	Where the data come from	How often
Waste	kg rejected or unsold ÷ kg produced	ERP (production) and returns log	Weekly
Online orders	Hotel orders via the portal ÷ all hotel orders	Portal and ERP	Monthly
Energy	Oven kWh ÷ kg produced	IoT meters and ERP	Monthly

The pipes between buildings

> **Integration** is how data travel between applications, and on which platforms those applications run.

Think in three layers:

Layer	What it holds	In the example bakery
Data	Customers, orders, consumption, temperatures	Each piece of data has **one source of truth**: the customer "lives" in the ERP
Applications	The programs that use the data	Portal, ERP, dashboard, forecasting model. They talk through **APIs**; manual exports are the last resort
Platforms	Where the applications run	Cloud services from D3, an edge device at the bakery for the sensors

> The **source of truth** of a piece of data is the one system where it is created and corrected; every other system copies it from there.

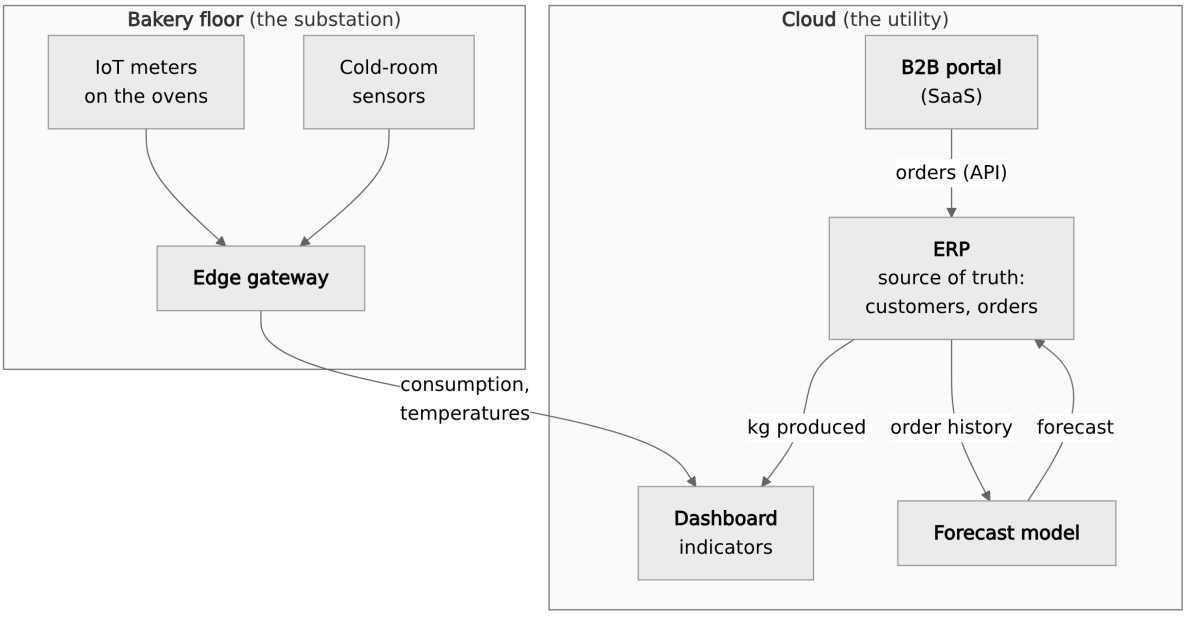
> An **API** (application programming interface) is a door that one program opens so another program can ask it for data or send it data, without a person in between.

Here is the example bakery's integration diagram, the same kind you will draw:

Check every diagram with three questions: **where is the source of truth? how does the data travel? what happens if one piece falls?** The Palma airport story is the answer to the third question when nobody asked it.

In class: diagram, gaps and indicators

Step	Do this	You should see
1 · group	The Technician opens app.diagrams.net, chooses **Device** (save to this computer) and creates a blank diagram. The others dictate from D3 and section 2	An empty canvas
2 · group	One box per application, grouped by platform (cloud, edge, local); arrows labelled with **what** travels and **how** (API, file, by hand); the source of truth of each piece of data marked	A diagram someone outside the group could read
3 · group	**File › Export as › PNG**, and also save the `.drawio` file	Two files: the picture and the editable diagram



Step	Do this	You should see
4 · alone	Take **one area** of the plan and write two possible gaps, the asset affected, one measure for each and the law involved. At least one must come from your D5 passive audit	Two rows in the shared gaps table
5 · alone	Write the indicator of **one** goal: name, formula, where the data come from in the diagram, how often	One indicator you could actually calculate

Hand in on Classroom (individual class activity): your two gap rows and your indicator, with the group's diagram as PNG attached. Passive only, and no generative AI.

For your project

This lesson builds **section 3 · Security and data** of D6 · Transformation plan (criteria g and h) and the integration diagram of **section 4** (criterion i). The gaps start from your D5 audit; the platforms come from your D3 architecture. If D3 no longer fits the technologies of section 2, update it and write the change in the change log.

Key takeaways

- A **security gap** is a weak point of an area; a **personal data breach** is an incident that already happened, notifiable within 72 hours under the RGPD. Plans analyse gaps to prevent breaches.
- For each area: asset, possible gap, a specific measure, the law involved. Start from your **passive** D5 audit.
- Every new kind of data needs its **treatment** defined along its lifecycle.
- Every goal needs an **indicator** (KPI) with a formula and a data source you actually have.
- **Integration** has three layers: data, applications, platforms. Each piece of data has one **source of truth**, and applications talk through **APIs**.
- Always ask what happens if one piece falls: on 19 July 2024, one faulty update stopped check-in at Palma airport.

Quick check

1 What is the difference between a security gap and a personal data breach?

- **A** None: they are two names for the same thing
- **B** A gap is a weak point that could be exploited; a breach is an incident that has already happened
- **C** A gap only affects OT and a breach only affects IT
- **D** A breach is always caused by an external attacker

2 Which of these measures is well matched to a specific gap?

- **A** "Install an antivirus on every computer", for every area
- **B** "One account per person and MFA", for a portal where hotel staff share one password
- **C** "Buy a faster router", for paper temperature logs
- **D** "Hire a lawyer", for IoT devices with factory passwords

3 For your company's real website, which of these is allowed in the course project?

- **A** Scanning its open ports to find vulnerable services
- **B** Trying common passwords on its login page
- **C** Reading its security headers in securityheaders.com and its cookie banner
- **D** Sending it a test phishing email

4 What makes an indicator usable in the plan?

- **A** It sounds impressive in the presentation
- **B** It measures something unrelated to the goals, so it is objective
- **C** It has a fixed formula and can be calculated with data the plan actually collects
- **D** It is calculated only once, at the end of the project

5 What is the source of truth of a piece of data?

- **A** The most expensive application in the company
- **B** The one system where that data is created and corrected; the others copy it from there
- **C** The backup copy in the cloud
- **D** Any spreadsheet where the data appears

6 In an integration diagram, what should each arrow say?

- **A** Nothing: arrows only show that two boxes are related
- **B** What travels and how: for example "orders, via API"
- **C** The price of each application
- **D** The name of the person who installed it

7 A hotel uses a cloud booking system connected to its door-key system. Which two questions should its integration diagram help answer?

- **A** If the booking system is down, can guests still open their rooms?
- **B** What colour should the boxes of the diagram be?
- **C** Which system holds the correct guest list, and how does the key system get it?
- **D** How many floors does the hotel have?

Data, doors and pipes are in place. The last pieces are the people who will run the new city, and the written plan of what changes and when: People and documentation.

Solutions

1. B · The plan analyses **gaps** to prevent **breaches**. And a breach can be caused by a mistake too, such as an email sent to the wrong person.

2. B · A measure must **close a specific gap**. Shared passwords are closed with personal accounts and multi-factor authentication.

3. C · Only **passive** observation: what the website already shows to any visitor. Never scan, probe or try logins on a real company.

4. C · An **indicator** turns data into a check on a goal. If the data are not in your diagram, you cannot calculate it.

5. B · With one **source of truth**, the customer's address is corrected in one place and every other system gets the right one. With several, they contradict each other.

6. B · An arrow without content hides the important part. Label **what** travels and **how** (API, file, by hand), so you can see the frictions.

7. A, C · The control questions of every diagram: **what happens if one piece falls**, and **where is the source of truth and how does the data travel**.