Security projects: how do you get a control to everyone, and into IT projects before go-live?

Before your next security rollout starts, write down its scope, a coverage target such as 98% of in-scope accounts enforced, and an end date for every exception, then run it in report-only or audit mode, a pilot and two or three rings. In the company's other IT projects, ask the security questions at kickoff and sign off before go-live, and scale the effort by protection need so only high-need projects wait for a full review.

Reviewed	Next review	Version	Written for
5 Nov 2026	**5 Dec 2026**	**1.0**	**Heads of security, IT leads who own security, and project managers in small and mid-size companies**

Latest version
sheets.einblick.dev/security-projects/

If you only do five things

1. **Define done in numbers before you start.**
   Count the scope from the inventory and set a target, such as 98% of in-scope devices in block mode by 31 March, with an exception cap. Count enforced, not deployed.
2. **Watch before you enforce.**
   Keep a new Conditional Access policy in report-only mode for at least a week[1]; it logs but blocks no one[2]. Audit ASR rules first, except the standard protection rules[3].
3. **Roll out in rings sized for your help desk.**
   Pilot with IT and a champion per business unit, then a representative ring, then everyone, in waves within support capacity[5].
4. **Give every exception an end date.**
   Exclusion lists start short and grow[11]. Give each member of a policy's exclusion group a reason, an owner and an end date.
5. **Ask security at kickoff, not at go-live.**
   The BSI requires involving the ISB early in larger projects and new IT systems[13]; Grundschutz++ requires a rule for when[14].

Roll out a security change in this order

1. **Who and what is in scope?**
   Count from the inventory, not the new tool; Defender's device discovery (Plan 2) finds devices not yet onboarded[8]. The security program sheet decides what goes first.
2. **What would break?**
   Run report-only or audit mode for one to four weeks and review the results with app owners. For segmentation, allow and log first, as the network segmentation sheet describes.
3. **Who pilots it?**
   IT and a champion per business unit[3], with a channel for problems. What they hit becomes the user message and the help desk script.
4. **When does the next ring start?**
   After a week with no open blocking tickets. Reuse your Windows update rings if you have them.
5. **When is it done?**
   When the tail is closed by name, the old path is gone, such as SMS codes, and an owner gets a monthly coverage report.

Users, help desk and rollback

- **Tell users what changes, when, and how to get help**[1], a week before their ring and on the day.
- **Brief the help desk before each ring:** the script, known errors and what to collect, including the correlation ID from **More details**[1].
- **Write the rollback first:** the trigger and the switch. Disable the CA policy or exclude a group[1]. Exclude the app from ASR or return the rule to audit[3]. Pausing Intune deployments stops only later rings; revert the policy[6].
- **Exclude Mac, iOS and Android from report-only compliance policies,** or their users may get certificate prompts[2]. Test them in an enforced pilot.
- **In Germany, ask the works council early** about EDR, DLP and logging; it co-determines systems designed to monitor behavior or performance[12].

Measure adoption against the inventory

- **Coverage is enforced over in scope,** counted weekly from the inventory by ring and business unit, with the tail named.
- **MFA and passkeys.** Entra's **Authentication methods** > **Activity** lists who is MFA or passwordless capable and counts single-factor sign-ins[9].
- **Conditional Access.** The gap analyzer workbook lists sign-ins no policy applied to (P1 and Log Analytics)[10].
- **EDR and ASR.** Compare onboarded with discovered devices[8]; the ASR report needs Plan 2 or Defender for Business, else forward event 1122[3].

Exceptions that end

- **Exclude groups, not people.** One assigned Entra group per policy shows who is excluded[11]; break-glass accounts go in every one[1].
- **Record why, what instead and until when:** a reason, a compensating control, an owner and an end date per member. Approval levels are in the risk register sheet.
- **Let reviews remove people.** Entra access reviews can ask members weekly and remove those who don't answer (Entra ID P2 or ID Governance)[11].
- **Cap them.** Our rule: at most 2% of the scope at go-live; any still open at the done date is renewed one level up, as in the risk register sheet. Report the count and the oldest monthly.

Mistakes that cost the most

- **Stopping at 80%.** The tail holds the old devices, service accounts and executives. Give it its own phase and owners.
- **Exceptions that become permanent.** Exclusions without an end date outlive their reason. Let them expire unless someone renews them.
- **No owner after go-live.** Conditional Access policies have no owner field, so Microsoft suggests putting it in the name and keeping a register[1].
- **Piloting only in IT.** IT and lab devices usually lack a representative mix of apps and drivers[4].

Security gates in IT and business projects

- **At kickoff, ask six questions:** what data, who signs in and how, internet-facing or not, which supplier, who gets admin rights, when it goes live.
- **Rate the processes the system serves: normal or high.** Grundschutz++ sets these two; on its catalog, high need adds a risk analysis[14].
- **Write requirements into the plan.** Normal: SSO with MFA, exportable logs, named admins, backups, patch deadlines. High: add a design review. Software you build: see the secure development sheet.
- **Pentest at go-live** if the system faces the internet, has high need, is custom-built or changes sign-in; ENISA advises testing at set-up[15]. Otherwise scan and check settings. See the penetration testing sheet.
- **Sign off.** Security confirms each requirement or lists open items with owners and dates; management approves the risk of unmet ones, which Grundschutz++ rules out for MUSS requirements[14].

Security in tenders and contracts

- **Use the six NIS2 purchasing points:** security requirements, updates for the whole lifetime or replacement after support ends, component information, security functions and secure configuration, assurance, and how you validate it[15]. They bind digital providers; in Germany, BSIG § 30(2) no. 5 requires security in acquisition of all NIS2 entities[17].
- **Ask when support ends.** From 11 December 2027, the CRA requires makers of new products to state the month and year at purchase[16].
- **Require free, prompt fixes,** tested and delivered as soon as an issue is known, as ENISA advises[15].
- **Tie acceptance to evidence.** Make acceptance and the final payment depend on SSO and MFA working, logs flowing and critical pentest findings fixed. Add the third-party risk sheet's clauses.

Don't become the bottleneck

- **Publish when security joins.** Grundschutz++ doesn't need the ISB active in every security-relevant project[14]. Join the high-need ones.
- **Promise a turnaround,** such as the operating model sheet's 5 working days. If you miss it, normal-need projects go ahead and log open items.
- **Pre-approve patterns:** a SaaS requirement set, a contract annex, a reference design.
- **Put a champion in the PMO** to ask the kickoff questions and call you in for high-need projects.

What you can skip

- **A risk analysis for every project.** With the Grundschutz++ catalog, normal need requires none unless a requirement stays unmet[14].
- **A pentest at every go-live.** A standard SaaS app behind SSO needs a check of your tenant's configuration.
- **Auditing the standard ASR rules.** Microsoft says they can typically go to block or warn without testing[3].
- **Months in report-only.** Our limit: a week to a month of real sign-ins. Enforce, then fix the tail.

What changed in 2026

- **Intune stages policy rollouts.** Deployment plans, in preview since September 2026[7], push Windows policies and apps ring by ring and can be paused[6].
- **Grundschutz++ wants a project rule.** BSI-Standard 300-1 (20 October 2026) requires a security role in relevant projects and a rule for when[14].
- **CRA support periods got clearer.** The Commission's draft CRA guidance of 27 July 2026 says the five-year minimum isn't a default[16].

What this looks like at your size

Small team, no security staff

- The IT lead or provider runs rollouts; a managing director approves exceptions.
- Pilot with two or three users, then everyone.
- Check IT purchases against the six NIS2 points.

Growing, with IT or security staff

- Write one page per rollout: scope, target, rings, rollback, exceptions, owner.
- Report coverage at the program's monthly meeting.
- Ask the kickoff questions in every IT project.

Enterprise or regulated

- Ring by region or site, and hold mission-critical devices until last[4].
- Make security sign-off a gate in the project method.
- Put a security annex in every IT tender template.

Version history

5 Nov 2026, version 1.0 Published after a copy edit and a source-by-source fact check, which made the rollback steps real rollbacks, added break-glass exclusions and Defender license needs, aligned exceptions with the risk register and scoped the Grundschutz++ and CRA claims to what the sources say.

Sources

1. Plan a Conditional Access deployment. Microsoft Learn, 1 Jun 2026. learn.microsoft.com
2. Conditional Access policy insights. Microsoft Learn, 1 Jun 2026. learn.microsoft.com
3. Test your ASR rules deployment. Microsoft Learn, 2 Jul 2026. learn.microsoft.com
4. Create a deployment plan (Windows). Microsoft Learn, 31 Dec 2017. learn.microsoft.com
5. Deployment considerations for Entra MFA. Microsoft Learn, 2 Nov 2025. learn.microsoft.com
6. Create and manage an Intune deployment. Microsoft Learn, 26 Aug 2026. learn.microsoft.com
7. What's new in Microsoft Intune. Microsoft Learn, 2 Nov 2026. learn.microsoft.com
8. Defender device discovery overview. Microsoft Learn, 8 May 2025. learn.microsoft.com
9. Authentication Methods Activity. Microsoft Learn, 22 Oct 2025. learn.microsoft.com
10. Conditional Access gap analyzer workbook. Microsoft Learn, 4 Nov 2024. learn.microsoft.com
11. Manage users excluded from CA policies. Microsoft Learn, 18 Jun 2025. learn.microsoft.com
12. BetrVG, § 87. Gesetze im Internet, checked 5 Nov 2026. gesetze-im-internet.de
13. ISMS.1 Sicherheitsmanagement. BSI, Edition 2023. bsi.bund.de
14. BSI-Standard 300-1 (Grundschutz++). BSI, 20 Oct 2026. bsi.bund.de
15. NIS2 implementation guidance. ENISA, 26 Jun 2025. enisa.europa.eu
16. CRA guidance, C(2026) 5252. European Commission, 27 Jul 2026. digital-strategy.ec.europa.eu
17. BSIG, § 30. Gesetze im Internet, checked 5 Nov 2026. gesetze-im-internet.de