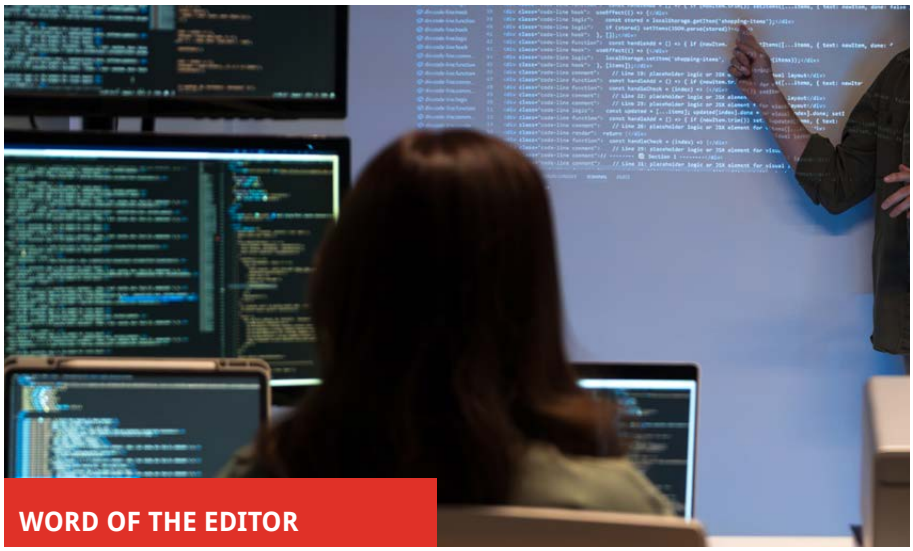
CSupMNE
Straightening Up Cybersecurity Posture of Montenegrin Higher Education system

Co-funded by the Erasmus+ Programme of the European Union

issue# 3, December 2025

newsletter



WORD OF THE EDITOR

Why every HEI needs a Dossier before rewriting policies

In this issue, we show how to assemble a lean Organizational Context (GV.OC) dossier that ties mission, stakeholders, and obligations to measurable cyber objectives.

By the end, you'll have a one-page checklist, starter templates, and a mini-case you can adapt this afternoon.

Policy rewrites often fail because they start in the document, not in the institution. The result is misaligned objectives, orphaned KPIs, and unfunded controls. HEIs feel the pain through audit pressure, grant/compliance duties, and a complex cloud and supplier stack.

- **Map mission to define what cyber objectives people can own.**
- **Register stakeholders and obligations (GDPR, grants, SLAs) with evidence sources.**
- **List critical services and dependencies to focus controls.**
- **Draft starter KPIs/KRIs the Rectorate actually reads.**
- **Create a single source of truth before touching policy text.**

Inside, you'll get a practical how-to, quick wins, and proof of impact:

- **Featured Article: step-by-step GV.OC build, with a Montenegrin HEI mini-case.**
- **Shorts: report on strengthening digital resilience through education and information of the top forgotten obligations.**
- **Project Highlights: the start of the training.**

I also want to thank all our project partners—your contributions, knowledge, and expertise shaped this issue of the CSupMNE Newsletter.

— Dr. Daniel Schönle, Furtwangen University

Editor: Dr. Daniel Schönle, Furtwangen University. **Featured**: Prof. dr Radislav Jovovic, University Mediterranean; Prof. dr Marija Jankovic, University Mediterranean. **Shorts**: Laura Horvat, University of Maribor; Dr. Daniel Schönle, Furtwangen University. Events: Dr. Daniel Schönle, Furtwangen University. **QA**: Institute of Modern Technologies Montenegro. **Coordinator**: Dr. Daniel Schönle, Furtwangen University.

Subscribe for CSupMNE newsletters: https://csupmne.me/newsletters.php

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

How to compile a GV.OC dossier: from theory to practice

Prof. dr Radislav Jovovic, University Mediterranean

Prof. dr Marija Jankovic, University Mediterranean

A GV.OC (Governance & Cybersecurity Objectives) Dossier is a structured document that acts as a single source of truth for an organization's cybersecurity program. Its purpose is to bridge the gap between high-level strategy and daily operations, providing clarity for risk management, regulatory compliance, and continuous improvement. It defines the organization's mission, strategic objectives, compliance obligations, critical services, dependencies, and performance indicators—all within a single, coherent reference point.

The primary purpose of the GV.OC Dossier is to translate cybersecurity strategy into actionable governance. It enables decision-makers to understand where the organization stands, what it must comply with, and how progress and risks are measured. By integrating governance, risk management, and compliance (GRC) principles, the Dossier ensures transparency, accountability, and continuous improvement in cybersecurity operations.

1. From Mission to Concrete Cyber Objectives

The mission statement provides the "why" for the cybersecurity program. The objectives translate this vision into actionable, strategic goals. This step ensures that every security control implement directly supports the organization's core mission.

Mission:

To ensure secure, resilient, and compliant digital operations that protect sensitive data, support critical services, and enable organizational growth. Example cyber objectives derived from the mission:

- *Data protection:* Safeguard personal and institutional data against unauthorized access and leaks. This objective directly addresses the "protect sensitive data" part of the mission.
- *Service Continuity:* Ensure uninterrupted delivery of essential academic and administrative services. This supports the "resilient digital operations" and "support critical services" aspects, focusing on availability and reliability.
- *Regulatory Compliance:* Maintain compliance with national and international cybersecurity and privacy standards. This makes the "compliant digital operations" part of the mission measurable and manageable.

2. Stakeholder register: Who is involved?

Cybersecurity is not just IT's responsibility. This register identifies all key individuals and entities (internal and external) who have a role or are impacted by cybersecurity decisions. Defining their responsibilities prevents gaps in accountability and ensures effective communication, especially during an incident.

Stakeholder	Role	Contact	Cyber Responsibility
IT Director	Decision-maker	itdir@hei.edu.me	Approves cybersecurity policies, allocates budget, oversees incident response.
Data Protection Officer	Compliance	dpo@hei.edu.me	Oversees GDPR/ADPD compliance, conducts audits, manages data breach reporting.
Faculties	Users	faculty@hei.edu.me	Responsible for secure handling of research and student data on their devices.
Students	Users	student@hei.edu.me	Expected to adhere to acceptable use policies for university systems.
External Providers	Service Providers	prov@vendor.com	Contractually obligated to provide security controls and adhere to SLAs.

3. Obligation register: what must comply with?

This is "compliance checklist." It maps all legal, contractual, and regulatory requirements which organization must follow. Crucially, it also documents where to find proof of compliance. This turns abstract rules into manageable tasks and provides rady evidence for auditors.

Obligation	Source	Evidence Location
GDPR / APDP Compliance	EU GDPR / Montenegro APDP	Data protection policies, DPO audit reports, consent forms.
Research grants	Ministry of science, Erasmus+, Horizon	Signed grant agreements, data management plans, reporting templates.
Service level agreements	IT contracts	Signed SLA documents, monthly performance and uptime reports.
ISO/IEC 27001	Internal certification	Audit reports, certification certificates, ISMS documentation.

Where to find evidence: Internal audit reports, contract repositories, organizational policy portals, regulatory authority websites (e.g., APDP Montenegro), and grant management systems.

4. Critical services & dpendencies: What must be protect?

This step forces organisation identify the "crown jewels"—the services whose failure would severely impact the organization. Documenting their dependencies reveals the underlying infrastructure and systems that need to be secured to ensure service continuity. Top 5 critical services for a higher education institution (HEI):

1. Student information system (SIS):
– Dependencies: Cloud provider availability, internal network stability, identity management system.
2. Learning management system (LMS):
– Dependencies: Internet connectivity, LMS server health, faculty and staff authentication.
3. Research data repositories:
– Dependencies: Secure storage infrastructure, reliable backup systems, granular access controls.
4. Email & collaboration Tools:
– Dependencies: Provider SLAs (e.g., Microsoft 365), network infrastructure, multi-factor authentication.
5. Financial Management & Payroll:
– Dependencies: Internal finance servers, ERP system integrity, secure bank communication interfaces.

5. Initial KPIs and KRIs: How Do We Measure Success and Risk?

This is how track progress and spot trouble. Key performance indicators (KPIs) measure the effectiveness of security processes. KRIs act as an early warning system, measuring exposure to potential threats. Together, they move cybersecurity from an opinion-based discussion to a data-driven one.

Metric	Type	Definition	Target / Threshold
% of systems with up-to-date patches	KPI	Proportion of servers/workstations fully patched against known vulnerabilities.	≥ 95%
Mean time to incident detection (MTTD)	KRI	Average time from a security event occurring to its discovery. A rising MTTD indicates increased risk.	< 4 hours
% of staff completing cybersecurity training	KPI	Proportion of employees who have completed mandatory annual security awareness training.	≥ 90%
Number of GDPR breaches	KRI	Count of reported incidents affecting personal data. This directly measures compliance risk.	0
Critical system downtime	KRI	Total hours of unplanned downtime per month for services defined in Section 4.	≤ 2 hours

6. Mini case: The impact on a montenegrin HEI

Before the GV.OC Dossier:

– *Unstructured Tracking:* Cybersecurity efforts were reactive and disorganized.
– *Obligation Blind Spots:* Limited awareness of all legal and contractual requirements.
– *Unmeasured Performance:* Ad-hoc KPIs without clear risk context made improvement impossible.

After Implementing the GV.OC Dossier:

– *Clarity and alignment:* Mission and objectives were formalized, aligning security with institutional goals.
– *Clear accountability:* All stakeholders were identified with defined responsibilities.
– *Audit-ready compliance:* Obligations were mapped with direct links to evidence sources.
– *Focused investment:* Understanding critical dependencies allowed for targeted spending on resilience.
– *Data-driven management:* Established KPIs/KRIs enabled measurable tracking and improvement.

Tangible Impact:

– Reduced downtime of the student information system (SIS) and learning management system (LMS) by 30%.
– Identified and closed GDPR compliance gaps before the annual audit.
– Improved staff awareness of their cybersecurity obligations through targeted training.

Project Highlights: Govern Training Program for Montenegrin Higher Education Institutions

Our online training series brought together ≈20 participants per session, with trainers from all European project partners delivering the modules. Participants didn't just listen, they built: the core governance artefacts were successfully elaborated during the workshops and then peer-reviewed for immediate reuse in Rectorate/Senate contexts. The program followed a sequenced Govern (GV) pathway: organizational context, risk strategy, supply-chain assurance, roles & authorities, and policy lifecycle, so that each artefact reinforced the next and culminated in a governance-ready strategy pack.

Training snapshot

• **Format:** Online, instructor-led delivery blended with hands-on labs and a capstone peer review to transform templates into institution-ready drafts.

• **Participation:** ~20 attendees per session from leadership, DPO, IT, QA, and faculty administration, ensuring decisions and evidence lines could be tested live.

• **Trainers:** Cross-partner faculty from all European project partners (AGH, HFU, UM, UBG, UDG, UoM, UNIM, AUB, MEDU, IMTM, PKCG, ACQAHE), guaranteeing coverage from governance, legal, and operational angles.

• **Modules covered:** GV.OC (Organizational Context), GV.RM (Risk Strategy), GV.SC (Supply Chain), GV.RR (Roles & Authorities), GV.PO (Policy System), each mapped to tangible outputs and adoption steps.

• **Method mix:** Mini-lectures (~20–25%) for framing, hands-on labs (~50%) to populate registers/matrices, cases & simulations (15–20%) for realism, and a capstone (~10%) to consolidate and peer-review.

What we produced (artefacts)

• **GV.OC Dossier.** Each HEI assembled a concise dossier linking mission → cyber objectives, with a Stakeholder Register (Ministry, APDP, EU funders, faculties, SaaS vendors), an Obligation Register (GDPR/APDP, grants, SLAs), a Critical Services & Dependencies catalog (LMS, SIS, IdP, campus network, eduroam/MREN), and a starter set of KPIs/KRIs (e.g., exam availability, breach reporting ≤72h). The result is a single source of truth to guide risk, policy, and investment.

• **Risk Strategy Pack (GV.RM).** Teams drafted risk objectives, appetite/tolerance statements, and a standardized 5×5 scoring method; they populated a Risk Register with a working heatmap, mapped risk →control →budget, and added an Opportunity Register for positive risks (e.g., shared services, EU funding). This converts scattered assessments into a governance-approved, budget-linked strategy.

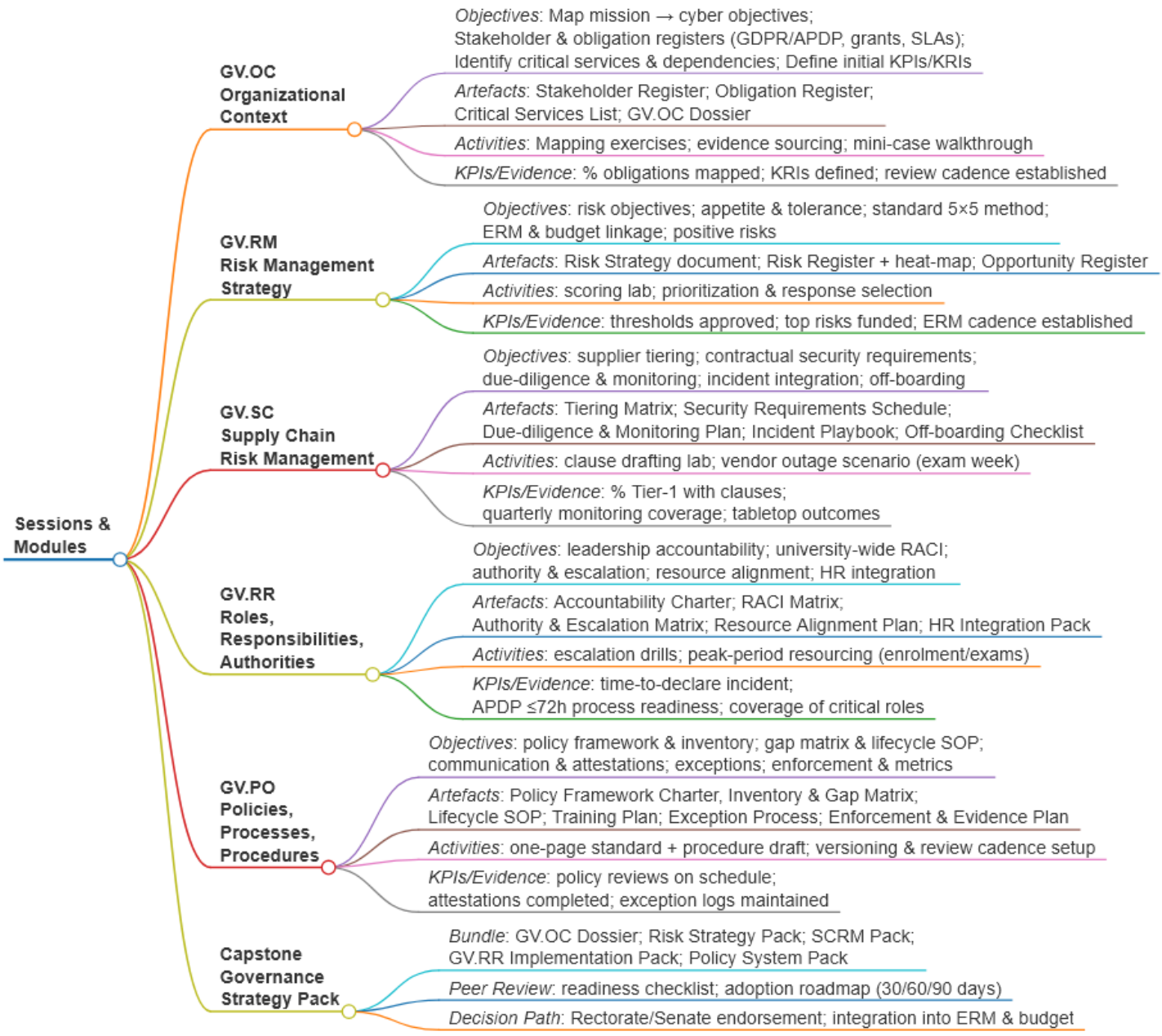
• **SCRM Pack (GV.SC).** Institutions produced a Supplier Tiering Matrix, a contract Security Requirements schedule (breach ≤72h, DPAs, DR/BCP, crypto, logging, SSO/MFA), a Due-Diligence & Monitoring plan, an SCRM Risk Register, an Incident Integration playbook, and an Off-boarding checklist. Together, these embed suppliers into incidents, audits, and lifecycle change where outages during exam windows matter most.

• **GV.RR Implementation Pack.** Participants finalized an Accountability Charter, a university-wide RACI, an Authority & Escalation Matrix (incident declaration, APDP notification, DR invocation), a Resource Alignment Plan (people/tools/budget by risk and peak periods), and an HR Integration pack (job-description clauses, onboarding, training, performance). This makes responsibility visible, auditable, and fundable.

• **Policy System Pack (GV.PO).** Each HEI built a Policy Framework Charter, a Policy Inventory & Gap Matrix with owners and review dates, an approval workflow (Rectorate/Senate), a lifecycle SOP with change triggers, a Communication & Training plan with attestations, an Exception/Waiver process, and an Enforcement & Evidence plan tied to metrics. Policies move from static PDFs to a living system aligned to context and ERM.

Why this matters for Montenegrin HEIs

The GV.OC work anchors cyber decisions in local realities: exam integrity, GDPR/APDP reporting, research continuity, and constrained teams. With that anchor in place, the risk strategy clarifies thresholds the Rectorate can approve; SCRM brings cloud and eduroam partners into your incident and assurance loop; roles & authorities replace ad-hoc decision-making with a documented,



escalatable chain; and the policy system ensures updates, communications, exceptions, and enforcement have owners, cadence, and evidence. This end-to-end alignment is precisely what auditors, funders, and internal QA bodies look for when assessing readiness and maturity.

How we worked

The pedagogy emphasized production over presentation. Mini-lectures framed what "good" looks like; labs populated real templates with each institution's data; case studies simulated exam-week incidents and supplier failures; and the capstone pushed teams to compile packs ready for Rectorate/Senate review. Peer review surfaced cross-faculty nuances and aligned registers (risk, supplier, policy) with governance calendars before the next academic cycle.

What changes now

Institutions leave with governance-ready drafts rather than notes: a living GV.OC dossier, a ratification-ready Risk Strategy, an operational SCRM program, a codified authority model with resource alignment, and a policy system that is reviewable, communicable, and enforceable. The immediate next steps are to finalize owners, schedule Senate/Rectorate sign-offs, connect KPIs/KRIs to dashboards, and integrate supplier attestations and drills into the improvement loop. As these artefacts enter ERM and budget processes, risk decisions become explainable, repeatable, and evidence-backed.

Acknowledgements

Thank you to all European project partners and participants; your contributions, knowledge, and commitment shaped these results and the tools now ready for deployment across Montenegrin higher education.

Cybersecurity Awareness Month at UM FERI: Strengthening Digital Resilience Through Education

In October, the Faculty of Electrical Engineering and Computer Science at the University of Maribor (UM FERI) marked Cybersecurity Awareness Month with a series of educational activities dedicated to promoting digital safety and resilience.

One of the highlights was the Cybersecurity Academy 2025, a renewed cycle of specialized training sessions aimed at enhancing professional skills in the field of cybersecurity. The program, held between August 22 and October 1, 2025, included four focused modules:

- Web Security and Penetration Testing (in cooperation with *Viris d.o.o.*)
- Identification, Authentication, and Authorization (in cooperation with *Netis d.o.o.*)
- Digital Forensics
- Information Security Management

Each module combined theoretical knowledge with practical exercises, providing participants with hands-on experience in tackling real-world cybersecurity challenges. Upon completion, attendees received digital micro-credentials and certificates recognizing their newly acquired skills.

By combining academic expertise and industry collaboration, UM FERI continues to promote a culture of cybersecurity awareness, supporting a safer and more resilient digital future for all.

Top 10 obligations HEIs forget to map (and where to find evidence)

Many universities update policies without first mapping key obligations to verifiable evidence. The following checklist identifies ten frequently overlooked obligations and indicates where proof is typically found, who holds responsibility, and which metrics demonstrate performance.

Common pitfalls

- Policies exist without corresponding artefacts demonstrating execution
- Evidence stored in personal drives rather than a centralized register
- Vendors onboarded without RoPA/DPA/SCC updates
- Change activity during exam periods without escalation freezes
- KPIs/KRIs not reviewed at Rectorate/Senate cadence

The summary table provides an at-a-glance overview. Subsequent sections supply concise descriptions, typical failure modes, minimum evidence, accountable roles, and measurable indicators for each obligation.

#	Obligation (what it means)	Where to find evidence	KPI/KRI
1	72h breach notification (GDPR 33/34)	ITSM incident tickets (with awareness timestamp + decision log), DPO breach log, notification emails/templates	% notifications ≤72h
2	RoPA (GDPR 30)	RoPA register, CMDB/system inventory, data-flow maps	% processes in RoPA
3	DPIA for high risk	DPIA reports, sign-offs, mitigations	% high-risk with DPIA
4	Data-subject rights ≤1 month	DSAR register, timestamps, responses	Median DSAR time
5	Cross-border transfers & SCCs	DPAs, SCC annexes, vendor list, TIAs	% vendors with valid SCC/DPA
6	Assessment data retention	Retention schedule, deletion logs, LMS/SIS config	% records purged on time
7	Supplier security obligations	Contract security schedule ID (e.g., SS-01 v2.3), ISO/SOC attestations, monitoring reports	% critical vendors monitored quarterly
8	Access recertification (IAM)	Quarterly attestations, JML logs, privileged list	% systems recertified on time
9	BC/DR meets RTO/RPO	DR plans, restore logs incl. alternate-site tests, test reports, sign-offs	% services meeting RTO/RPO
10	Security awareness coverage	LMS completion reports, quiz scores, training schedule	% trained per term; phish-test failure trend

Summary table

Timely **breach notification** requires demonstrable reporting to the national authority—and, where applicable, to affected individuals—within 72 hours of awareness. Failures commonly stem from missing awareness timestamps and absent templates. Minimum evidence consists of the incident ticket with awareness timestamp and decision log, a corresponding DPO breach-log entry, and the notification template with dispatch records. Accountability typically sits with the DPO and incident response; performance is indicated by the share of notifications issued within 72 hours.

Up-to-date **Records of Processing Activities (RoPA)** are often incomplete when new SaaS or research tools bypass registration. Evidence includes the RoPA itself, CMDB linkages, and data-flow diagrams. DPOs and process owners are accountable; coverage rate and time-to-register new systems are the principal indicators. Automated creation of RoPA entries via procurement intake reduces omissions.

For **Data Protection Impact Assessments (DPIAs)** on high-risk processing (e.g., proctoring, biometrics, special categories), informal assessments without documented approval are a typical gap. Required evidence includes the DPIA report, risk ratings, mitigations, and sign-offs. Accountability spans the DPO, Research Office, and IT; indicators include the percentage of high-risk systems with a DPIA and time from trigger to approval. Risk-gate questions in ethics and procurement forms ensure initiation.

Data-subject rights compliance is frequently undermined by untracked requests landing in generic inboxes. Evidence comprises a DSAR register with timestamps, response letters, and identity-verification records. Accountability typically involves the DPO, Student Services, and HR. Median and 95th-percentile completion times, plus the overdue rate, are standard indicators. Ticket-based routing with a 30-day SLA supports compliance.

For **cross-border transfers**, contracts may exist while SCC annexes and TIAs remain dispersed. Evidence should consolidate the vendor list with hosting/transfer countries, signed SCCs/DPAs, and TIAs. Legal/Procurement and the DPO hold accountability. Indicators include the proportion of vendors with valid SCCs/DPAs and completed TIAs; third-country vendors are flagged for follow-up.

Student assessment data retention frequently exists in policy but not in operational jobs. Evidence includes the retention schedule, deletion logs, and specific job configurations—e.g., LMS job GradePurge_Prod with cron 0 3 * * Sun. Responsibility is shared by the Registrar, IT, and QA. Indicators include the proportion of records purged on schedule; automated jobs with audit logs deliver proof.

In **supplier risk management (SCRM)**, security schedules are often omitted under purchasing pressure. Evidence consists of a contract-attached security schedule with a unique ID (e.g., SS-01 v2.3), vendor attestations (ISO/SOC), and monitoring outputs. Procurement, the CISO, and service owners share accountability. Indicators include the proportion of critical vendors monitored quarterly and with signed security schedules. Standard schedules with breach-notification ≤72h address baseline needs.

Access recertification (IAM) is commonly ad hoc and undocumented. Evidence includes signed recertifications, JML logs, and a privileged-user list. IT/IAM and HR hold accountability. Indicators include the percentage of systems recertified on time and counts of orphaned accounts. Exception lists for break-glass access with explicit expiry dates, together with calendarized quarterly reviews and exam-period change freezes, improve control.

For **business continuity and disaster recovery**, backups may exist without evidence of restores meeting RTO/RPO, particularly to an alternate site. Evidence includes DR plans, restore logs with timings, test reports,

and sign-offs. IT Ops and QA/Audit are accountable; indicators include the proportion of services meeting RTO/RPO and mean restore times. Scheduled semester-break tests and archived results provide assurance.

Finally, **security awareness** coverage can be inconsistent when HR and LMS data diverge. Evidence includes LMS completion reports, quiz scores, and the training calendar. HR/L&D and the CISO are accountable. Indicators pair completion rates with a phishing-test failure-rate trend. Auto-enrolment and periodic catch-up cycles improve adherence.

In practice, closing these ten gaps comes down to disciplined evidence, clear ownership, and one measurable KPI per obligation. Centralize proofs in your Obligation Register (breach tickets/DPO log, RoPA links, DPIAs, DSAR trail, SCCs/DPAs/TIAs, LMS purge logs, vendor security schedules/attestations, access-recert sign-offs/JML, DR restore reports, training completions) and name an accountable owner plus a backup for each row. Then set serviceable KPIs/KRIs (e.g., notifications ≤72h, % processes in RoPA, % high-risk with DPIA, median DSAR time, % vendors with SCCs, % purged on schedule, % recertified on time, % services meeting RTO/RPO, % trained per term) and review them at the Rectorate/Senate cadence. Finally, add triggers in Procurement, ITSM, HRIS, IAM, LMS, and SIEM so new systems, vendors, users, and incidents automatically generate register updates—turning policy promises into auditable, repeatable practice.

UPCOMING EVENTS

Two milestones are scheduled: a hands-on Onsite Govern Training designed to move governance artefacts from draft to adoption, and an All-Members Consortial Meeting in Podgorica focused on alignment of strategy, decisions, and next-quarter deliverables. Dates and venues appear below.

Event 1: Onsite Govern Training (Hands-On)

When & where

- Date: 25.–27.11.2025
- Venue: University of Donja Gorica, Oktoih 1, 81000 Podgorica

Learning goals & outcomes

- Finalize GV.OC Dossier and link KPIs/KRIs to governance calendars.
- Tighten Risk Strategy (appetite, 5×5 method) and budget linkage.
- Validate SCRM tiering and incident integration with live vendor examples.
- Agree roles & escalation for exam-period incidents.
- Prepare policy lifecycle updates and an exception workflow.

AGENDA (high level)

Day 1 Tue, 25 Nov

- 09:00–09:15: Registration.
- 09:15–09:20: Welcome by Prof.dr Milica Vukotić (Vice-Rector, UDG).
- 09:20–09:30: General introduction by Prof.dr Ramo Šendelj (Project Coordinator).
- 09:30–11:00: Training 1 – Cybersecurity Strategy (AGH University): Prof.dr Jerzy Duda (+ AGH colleague).
- 11:15–12:45: Training 2 – Information Security Risk Management (University Furtwangen): Prof.dr Christoph Reich, Prof.dr Daniel Schönle.
- 14:15–15:45: Training 3 – Acceptable Use of IT Resources Policy (University of Belgrade): Prof.dr Slavko Gajin, Prof.dr Branko Marović.
- 15:45–16:30: Discussion moderated by Prof.dr Ivana Ognjanović (UDG).

Day 2 Wed, 26 Nov

- 09:15–09:30: Registration.
- 09:30–11:00: Training 4 – Security Awareness & Training Policy (University of Maribor): Prof.dr Ines Kožuh, Prof.dr Irena Lovrenčič Držanič, Prof.dr Laura Horvat.
- 11:15–12:45: Training 5 – Risk Assessment Policy (University Furtwangen): Prof.dr Christoph Reich, Prof.dr Daniel Schönle.
- 14:15–15:45: Training 6 – Identification & Authentication Policy (University of Belgrade): Prof.dr Slavko Gajin, Prof.dr Branko Marović.
- 15:45–16:30: Discussion moderated by Prof.dr Luka Laković (UDG).

Day 3 Thu, 27 Nov

- 09:15–09:30: Registration.
- 09:30–11:00: Training 7 – Information Security Policy (AGH University): Prof.dr Jerzy Duda (+ AGH colleague).
- 11:15–12:45: Training 8 – Systems & Services Acquisition Policy (University of Maribor): Prof.dr Ines Kožuh, Prof.dr Irena Lovrenčič Držanič, Prof.dr Laura Horvat.
- 14:15–15:45: Training 9 – Mentoring Support for Creating Documents (All EU partners).
- 15:45–16:30: Closing discussion moderated by Prof.dr Ivana Ognjanović (UDG).

Artefacts produced

Peer-reviewed GV.OC, updated Risk Register, SCRM matrix & playbook, Authority & Escalation Matrix, and a Policy Lifecycle SOP (draft).

Event 2: All-Members Consortial Meeting (Podgorica)

When & where

- Date: 26.–27.11.2025
- Venue: University of Donja Gorica, Oktoih 1, 81000 Podgorica

Purpose

Consortium alignment on milestones, agreement on governance metrics and evidence cadence, approval of the next-quarter work plan, and exchange of field results.