Reflective Synthesis — Security & Risk Management

Student: Ketan Dileep Mone

Programme: University of Essex Online – MSc Cyber Security

Module: Security & Risk Management

Module e-Portfolio URL:
https://ketanmone.github.io/srm/

Word Count: 1085 words

Introduction

This reflection follows **Rolfe et al. (2001)**'s *What / So What / Now What* model to evaluate my academic and professional development throughout the *Security and Risk Management* module.

Drawing from my artefacts—the **Team Cipher Risk Identification Report** (Unit 6) and **Individual Executive Summary** (Unit 11)—I critically analyse how my thinking evolved from theoretical understanding of risk frameworks to the practical application of quantitative modelling, governance, and ethical resilience.

What? — Summary of Experience

Early Foundations

Units 1 and 2 provided a conceptual base for the discipline.
Through readings on **ISO 31000** and **NIST SP 800-30**, I understood that risk is both contextual and continuous. Security management is a living system requiring monitoring and adaptation rather than static compliance.
Exploring **qualitative** and **quantitative** risk assessments revealed that subjectivity and statistical rigour must coexist.
The paper by **Spears and Barki (2010)** reinforced that user participation reduces the "compliance gap" by turning passive adherence into shared accountability.

Threat Modelling and Management

Units 3 and 4 translated risk concepts into operational analysis.
I practised **STRIDE**, **DREAD**, and **PASTA** frameworks, later using the **MITRE ATT&CK** matrix to link attacker tactics with control failures.
Creating attack-tree diagrams for my e-portfolio clarified how technical findings connect with business impact.

Standards and Governance

Units 5 and 6 bridged strategy and compliance.
The **GDPR case study** was my first encounter with legal interpretation of security.
Mapping Articles 32 and 33 to ISO 31000 controls illuminated how regulatory clauses translate into operational safeguards.
In the **Pampered Pets** group report, I aligned risks with mitigations following the ISO five-stage process.

Quantitative Risk Modelling

Units 7 and 8 advanced the technical dimension of my learning.
Through **Monte Carlo simulation** and **Bayesian inference**, I learned to represent uncertainty numerically—producing risk distributions rather than single-point estimates.
Integrating **AHP** and **TOPSIS** allowed structured comparison of competing priorities.
These units taught me that quantitative results gain legitimacy only when the underlying assumptions are transparent and validated through stakeholder review.

Business Continuity and Disaster Recovery

Units 9 and 10 positioned risk within organisational resilience.
Developing scenarios for **RTO** and **RPO** calculations clarified how technical specifications stem from business appetite, not engineering ambition.
I analysed **cold**, **warm**, and **hot** standby designs and explored **DRaaS** offerings to evaluate trade-offs between cost and dependency.

This shifted my perception of resilience from a defensive measure to a proactive design discipline.

Emerging Trends and Final Project

Units 11 and 12 addressed the future of **Security and Risk Management (SRM)**.
Exploring **AI-driven automation**, **Zero Trust Architecture**, and **quantum-resistant cryptography** contextualised my final assignment.
My **Executive Summary** combined Monte Carlo analysis and a multi-cloud **BC/DR** model, demonstrating measurable risk reduction from 21 % to below 10 %.
In the concluding debate, I defended the view that **AI-enabled, human-supervised automation** will dominate SRM evolution—a stance consistent with **Aven (2016)** and the **NIST AI RMF (2024)**.

So What? — Critical Reflection

Cognitive Transformation

Initially, I equated “security” with technical control. The iterative **Risk Management Process** taught me that sustainable security emerges from adaptive systems and informed decision-making.

The introduction of probability distributions revolutionised my mindset: uncertainty became quantifiable, and data became dialogue.

Presenting outcomes as ranges rather than absolutes encouraged strategic thinking in cost–risk trade-offs.

Collaboration and Leadership

Working in **Team Cipher** developed my collaborative literacy. The group spanned different time zones and professional backgrounds, requiring asynchronous coordination.

I began as an analyst but evolved into a facilitator—encouraging peers to justify assessments with evidence rather than intuition.

This improved our collective objectivity and mirrored **Fraser et al. (2021)**’s argument that mature risk cultures thrive on diversity of perspective.

Emotional and Ethical Insights

Quantitative modelling initially provoked anxiety; numbers seemed intimidating until I contextualised them using **Olsen and Desheng (2020)**.

Ethically, the GDPR case study and **BCS Code of Conduct (2021)** reminded me that compliance frameworks safeguard people, not paperwork.

Unit 11’s focus on AI governance challenged me to consider bias, accountability, and transparency. I now advocate for **human-in-the-loop** oversight—machines provide scale, but humans retain moral agency.

Skill and Knowledge Development

Across twelve units I developed:

- Proficiency in **ISO / NIST** standards mapping.
- Capability to design **Monte Carlo** and **Bayesian** simulations.
- Experience in **BC/DR** planning using measurable RTO/RPO targets.
- Communication competence in translating analytics into executive narratives.

  Together, these built an integrated skill set—technical, analytical, and ethical—that enhances both academic and professional performance.

Now What? — Future Application

Continuous Risk Culture

I will initiate each project with a **Risk Charter** capturing scope, assets, tolerance, and response strategy.
Following **NIST SP 800-34 Rev. 2**, quarterly **table-top exercises** and **post-incident reviews** will institutionalise learning loops.
Documenting lessons openly should embed resilience as a shared organisational behaviour rather than a compliance requirement.

Advancing Quantitative Practice

To extend the foundation laid by this module, I plan to model interdependent systems through **Bayesian Networks** and **Attack–Defence Trees** (Zografopoulos et al., 2021).
Introducing **chaos engineering** in controlled environments will stress-test continuity assumptions and validate probabilistic predictions.

Ethical AI and Governance

My forthcoming research will align with the **EU AI Act (2025)** and **NIST AI RMF**, focusing on transparent, bias-aware algorithms for cyber-risk scoring.
The objective is to operationalise fairness and explainability in automated decision-making—ensuring that efficiency never overrides accountability.

Leadership and Communication

Future collaborations will apply **servant-leadership** principles: active listening, empathy, and inclusion.
I will continue converting complex analysis into **visual narratives**—probability bands, decision trees, and scenario dashboards—so that both executives and engineers can act confidently.
The feedback from my Unit 6 report reinforced the value of brevity and clarity; hence, every deliverable will balance precision with accessibility.

Professional Trajectory

The module has re-oriented my career ambitions toward **governance-driven cybersecurity consulting**, integrating quantitative analytics with ethical oversight.
By uniting **risk science**, **design thinking**, and **data ethics**, I aim to contribute to organisations that view resilience not merely as recovery but as competitive advantage.

Conclusion

My learning journey in this module can be summarised through three enduring transformations:

1. **From Compliance to Resilience** — I learned that security frameworks succeed only when embedded in culture and verified through data.

2. **From Individual to Collaborative Mindset** — Team Cipher taught me to balance expertise with humility, valuing discussion as a form of validation.

3. **From Static Control to Adaptive Governance** — Integrating AI, automation, and quantitative reasoning revealed that modern SRM is a continuous feedback ecosystem.

Although I attended only two live seminars, systematic engagement with recordings, extended readings, and self-imposed reflection ensured that learning remained active rather than passive.

Going forward, I intend to apply this mindset—balancing numerical evidence with human judgement—to build enterprises that are **not only secure but genuinely resilient and accountable**.

References

Aven, T. (2016) ‘Risk assessment and risk management: Review of recent advances’, *European Journal of Operational Research*, 253(1), pp. 1–13.

BCS (2021) *Code of Conduct*. The Chartered Institute for IT.

Fraser, J.R.S., Quail, R. and Simkins, B. (2021) *Enterprise Risk Management*. Springer.

Olsen, T.L. and Desheng, D.W. (2020) *Research Methods and Applications in Quantitative Risk Management*. Springer.

Rolfe, G., Freshwater, D. and Jasper, M. (2001) *Critical Reflection for Nursing and the Helping Professions: A User’s Guide*. Palgrave Macmillan.

Spears, J.L. and Barki, H. (2010) ‘User participation in information systems security risk management’, *MIS Quarterly*, 34(3), pp. 503–522.

Zografopoulos, I. et al. (2021) ‘Cyber-physical energy systems security: Threat modelling and metrics’, *IEEE Access*, 9, pp. 29775–29818.