

Tech Academy Stream & Schedule

The 2025/26 Tech Academy is structured as a single stream, designed to provide a balance of core technical and operational skills relevant to all school Tech Teams. The programme includes 5 core modules and 3 optional modules, giving you flexibility to focus on the areas most important to your school.

Consultancy Support

As part of the Tech Academy Experience, each participant school will be allocated a 9ine Technical Consultant for support. The Technical Consultant will ensure each school is onboarded, understands the schedule and will be on hand to answer any questions post each Tech Academy session. They will also organise up to three one hour 1:1 (per school) consultancy sessions (worth £480.00 / \$600.00) to support understanding and embedding of the topics.

**The times and dates in the table below are subject to change.*

Course Schedule - Core Modules		
*Date/Time	Academy Course Title	Description
14th January 2026 04:00pm UK	Cyber Awareness Audit & Best Practice	Human behaviour is one of the largest risk factors in cybersecurity. This module offers a practical framework for assessing and improving your school's cyber awareness programme. It covers training frequency, content selection, delivery methods, and the use of simulated phishing exercises. You'll learn how to measure awareness levels, close identified gaps, and align your programme with frameworks such as NCSC 10 Steps and ISO 27001.
18th February 2026 04:00pm UK	Vulnerability Management Implementation	Unaddressed vulnerabilities are one of the most common entry points for attackers. This module provides an in-depth guide to creating a structured vulnerability management process, from scanning and identification through to assessment, prioritisation, and remediation. It explains how to integrate vulnerability findings into patching workflows, use risk-based decision-making to focus resources where they matter most, and schedule regular assessments to track progress over time. The aim is to embed vulnerability management into daily IT operations to strengthen the school's security posture.

18th March 2026 03:00pm UK	Server Infrastructure Audit & Best Practice	Robust server infrastructure underpins every digital service in a school, from teaching tools to administrative systems. This module provides a comprehensive framework for auditing and optimising server environments, whether using VMware, Hyper-V, or other virtualisation platforms. It covers performance optimisation, security configuration, storage architecture, high availability, and redundancy planning. Ensuring servers are correctly configured, patched, and monitored reduces the risk of outages, data loss, and security breaches, while supporting scalability for future needs.
15th April 2026 04:00pm UK	Backups Systems Audit & Best Practice	Reliable backups are the safety net for recovering from cyber incidents, accidental deletions, or hardware failures. This module presents a framework for reviewing the scope, frequency, and storage of your backups. It includes guidance on implementing offline and immutable backups, testing restoration processes, and documenting backup configurations. Ensuring backups are secure, comprehensive, and regularly tested provides confidence that critical data can be restored when it matters most.
20th May 2026 04:00pm UK	Update and Patch Management Implementation	Applying updates and patches in a timely and controlled way is critical to closing known security vulnerabilities. This module guides you through building a robust update and patch management strategy for operating systems, applications, and firmware. It covers planning updates around academic calendars, testing patches before deployment, handling emergency updates, and maintaining detailed change records. The focus is on keeping systems secure without causing unnecessary disruption to school operations, while ensuring full visibility of patch status across the environment.

Optional Topics: Survey-Led Selection

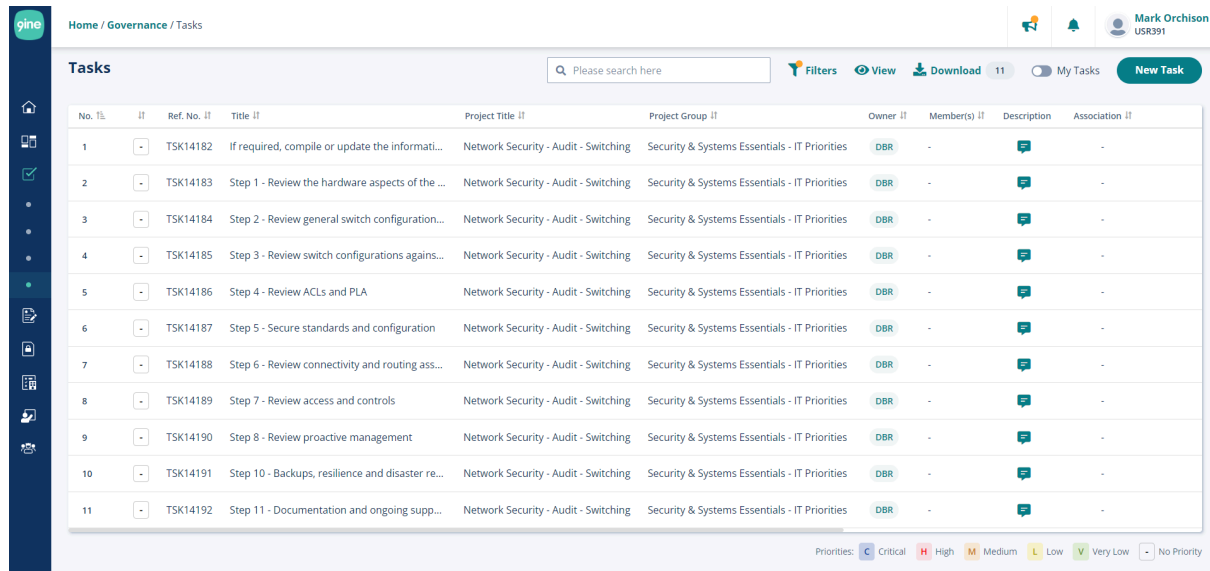
In addition to the 5 core modules, the Tech Academy offers 3 optional modules chosen by participants through a survey. These sessions allow schools to focus on areas of greatest interest and need, complementing the core programme. Provisional dates for the optional modules are:

Session	Date	Time (UK)
Optional 1	25th March 2026	3pm
Optional 2	22nd April 2026	4pm
Optional 3	27th May 2026	4pm

Proposed Topics (selection to be confirmed by survey)	
Academy Course Title	Description
Incident Management	Framework for responding to cyber attacks, data breaches, and major IT failures, with integrated privacy and regulatory considerations.
Network Switching Audit & Best Practice	Configuring and auditing networks for resilience, security, and operational efficiency.
Access Control List Implementation	Enforcing Zero Trust principles by restricting access and reducing the attack surface.
Wireless Audit & Best Practice	Optimising wireless performance and security through structured evaluation and configuration.
Firewall Audit & Best Practice	Auditing and configuring firewalls for maximum effectiveness and resilience.
Proactive Systems Management Implementation	Checklist-based daily, monthly, and annual system maintenance routines.
Systems Documentation Audit & Best Practice	Structured approach to documenting systems, processes, and configurations.
Disaster Recovery Implementation	Building a recovery plan to minimise downtime and disruption.
Active Directory Security Audit & Best Practice	Strengthening AD configurations against misconfiguration, misuse, and threats.
Email Protections Implementation	Technical measures (SPF, DKIM, DMARC, filtering) to defend against phishing and spoofing.
Anti-Virus Implementation	Selecting, deploying, and managing AV solutions across all school devices.

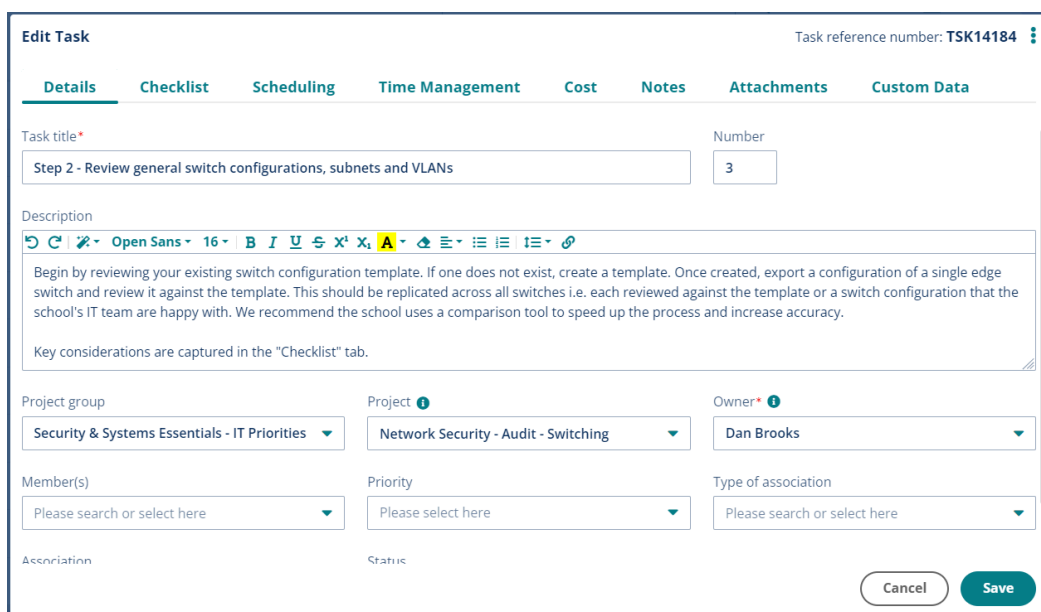
9ine Governance & 9ine Training Academy

The Governance Module and the Training Academy within the 9ine SaaS Platform are key components in the delivery of Tech Academy. The 9ine Governance Module is a powerful platform to operationalise each Tech Academy module, supporting tech teams to understand, plan, implement and report on progression.



No.	Ref. No.	Title	Project Title	Project Group	Owner	Members	Description	Association
1	TSK14182	If required, compile or update the informati...	Network Security - Audit - Switching	Security & Systems Essentials - IT Priorities	DBR	-		-
2	TSK14183	Step 1 - Review the hardware aspects of the ...	Network Security - Audit - Switching	Security & Systems Essentials - IT Priorities	DBR	-		-
3	TSK14184	Step 2 - Review general switch configuration...	Network Security - Audit - Switching	Security & Systems Essentials - IT Priorities	DBR	-		-
4	TSK14185	Step 3 - Review switch configurations agains...	Network Security - Audit - Switching	Security & Systems Essentials - IT Priorities	DBR	-		-
5	TSK14186	Step 4 - Review ACLs and PLA	Network Security - Audit - Switching	Security & Systems Essentials - IT Priorities	DBR	-		-
6	TSK14187	Step 5 - Secure standards and configuration	Network Security - Audit - Switching	Security & Systems Essentials - IT Priorities	DBR	-		-
7	TSK14188	Step 6 - Review connectivity and routing ass...	Network Security - Audit - Switching	Security & Systems Essentials - IT Priorities	DBR	-		-
8	TSK14189	Step 7 - Review access and controls	Network Security - Audit - Switching	Security & Systems Essentials - IT Priorities	DBR	-		-
9	TSK14190	Step 8 - Review proactive management	Network Security - Audit - Switching	Security & Systems Essentials - IT Priorities	DBR	-		-
10	TSK14191	Step 10 - Backups, resilience and disaster re...	Network Security - Audit - Switching	Security & Systems Essentials - IT Priorities	DBR	-		-
11	TSK14192	Step 11 - Documentation and ongoing supp...	Network Security - Audit - Switching	Security & Systems Essentials - IT Priorities	DBR	-		-

Within each task checklists provide further clarity on the steps that need to be taken and addressed. Additional powerful features enable your school to manage operationalisation of your cyber hardening programme through scheduling and allocating colleagues to complete tasks, capture time spent, allocate task costs, collaborate on task completion with notes and add attachments.



Edit Task Task reference number: TSK14184

Details Checklist Scheduling Time Management Cost Notes Attachments Custom Data

Task title* Step 2 - Review general switch configurations, subnets and VLANs Number 3

Description

Begin by reviewing your existing switch configuration template. If one does not exist, create a template. Once created, export a configuration of a single edge switch and review it against the template. This should be replicated across all switches i.e. each reviewed against the template or a switch configuration that the school's IT team are happy with. We recommend the school uses a comparison tool to speed up the process and increase accuracy.

Key considerations are captured in the "Checklist" tab.

Project group Security & Systems Essentials - IT Priorities Project Network Security - Audit - Switching Owner Dan Brooks

Member(s) Please search or select here Priority Please select here Type of association Please search or select here

Association Static

Cancel Save

The granularity of Checklists within each task supports Tech Academy participants to understand the technical planning, engineering and testing required to successfully complete each component of this cyber & systems hardening programme.

Edit Task Task reference number: **TSK14184**

Details Checklist Scheduling Time Management Cost Notes Attachments Custom Data

Please type here to add checklist item + Add

- ☐ Ensure that all switches are managed and have static IP addresses defined for management.
- ☐ Review the VLAN configuration looking at the settings, IP addressing and features which have been configured. Generally this is reviewed from the core switch configuration; as part of this task you should be looking at the VLAN IP configuration; is this consistently using the first or last usable address of each subnet. Are all DHCP helper addresses correctly defined.
- ☐ Review the subnet configuration ensuring that the network addresses do not overlap with one another and subnet mask are correctly defined. This would generally be defined within the VLAN structure.
- ☐ Check the capacity of each VLAN to see if any scopes need to be enlarged/extended.

Cancel Save

Supporting the scope of each task is a calculation for the amount of time it will take to complete the task and associated checklist. This supports the tech team in planning, resourcing and communicating the scope and timescales for implementation.

Edit Task Task reference number: **TSK14184**

Details Checklist Scheduling Time Management Cost Notes Attachments Custom Data

Estimated time
2d

Total logged time i
No time logged 2d remaining

Log Time
Time spent
Please type here (1w 2d 6h 2m) ☐ Reference only i

Further information
Please type here

Time Log Delete All
SK 16/Jan/2023, 14:36
Estimated time of 2d added

Cancel Save