CAUDIT Cloud Infrastructure Forward Commitment Program

Four Scenarios: How Credits Work in Practice

University A - "Hardware to Campus"

Profile: Large research-intensive university, Group of Eight

The situation:

University A operates a large-scale research computing platform that supports computational workloads across life sciences, physical sciences, engineering, and data-intensive social sciences. The platform was originally commissioned in 2016 and has been expanded through multiple investment phases, adding GPU-accelerated nodes, high-memory nodes for genomics and bioinformatics, and additional standard compute capacity. At its current scale, the platform comprises over 150 nodes, more than 5,000 cores, and multiple petabytes of high-performance parallel storage.

The problem is that the original Phase 1 and Phase 2 infrastructure, roughly 90 standard compute and high-memory nodes, is now approaching end of life. These nodes are running previous-generation Intel Xeon processors and DDR4 memory, and they're on extended Dell support that expires in early 2027. Performance per watt has degraded significantly compared to current-generation hardware, and the DDR4 dependency creates acute supply risk as manufacturers phase out production.

The university's research computing team has scoped a full replacement: next-generation Dell PowerEdge compute nodes with current-generation Intel Xeon processors and DDR5 memory, a GPU expansion with NVIDIA H100 accelerators to support the university's growing AI and machine learning research portfolio, and a high-performance storage refresh to replace ageing parallel storage capacity.

University A has a long-standing relationship with a trusted technology partner who provides complementary services around its research computing platform: deployment, integration, ongoing support, and specialist consulting. Historically, the university has procured infrastructure directly from Dell and engaged its partner for everything around it. That model works. They don't want to change it.

The bill of materials is fully scoped. The budget is approved across central IT and the Deputy Vice-Chancellor (Research) portfolio. The internal team and its trusted partner have the capability to deploy. What they don't have is confidence that the hardware will be available at the quoted price by the time procurement is executed, because in this market, a $10 million order placed in July could cost $11.5 to $13 million by the time it ships, and the GPU nodes alone have a 45+ week lead time through standard procurement channels.

What they need:

$10.8 million in Dell PowerEdge servers, GPU-accelerated nodes, high-performance storage, and high-speed networking, delivered to its on-campus data centre, deployed and commissioned by its own research computing team and its trusted partner.

How they use the program:

Item	Credit allocation
Dell PowerEdge R760 compute nodes (×60), replacing Phase 1 & 2 standard compute	$2,400,000
Dell PowerEdge R760 high-memory nodes (×18), genomics and bioinformatics	$1,260,000
Dell PowerEdge XE9680 GPU nodes (×10), NVIDIA H100, AI/ML research	$5,200,000
Dell PowerScale high-performance parallel storage	$1,140,000
Dell networking, high-speed InfiniBand fabric + Ethernet switching	$600,000
Remaining Dell extended support returned to university	($200,000 recovered)
Total credit purchase	**$10,800,000**

Credit split: 100% hardware

What happens:

- University A purchases $10.8M in credits prior to 22 April, scoped against its fully defined Dell BoM.
- Macquarie Cloud Services includes the BoM in late April bulk procurement with Dell. Macquarie Cloud Services works closely with Dell to identify high-risk items in the order, in this case the ten GPU nodes and the high-performance storage, and the consolidated order positions the university's allocation at the front of the queue. In a market where individual GPU orders face 45+ week lead times with no guaranteed allocation, that positioning matters.
- As hardware is manufactured and shipped to Australia, it is delivered directly to the university's on-campus data centre.
- The university's research computing team and its trusted partner rack, cable, configure, and commission the platform, exactly as they have for every previous phase. The existing partner relationship is unchanged. Macquarie Cloud Services is the procurement vehicle, not the delivery partner.
- Macquarie Cloud Services has no ongoing operational role. This is a hardware procurement, delivered through the program at locked pricing with priority allocation. The university continues to engage its trusted partner for all complementary services (deployment, integration, support, and consulting) as they always have.
- The remaining Dell extended support entitlement on the outgoing Phase 1 and Phase 2 nodes, approximately $200,000, is returned to the university, recovering value from what would otherwise be a sunk cost.

The outcome:

University A gets exactly what they would have received from a direct Dell procurement: the same hardware, delivered to the same data centre, deployed by the same team and the same partner. Nothing changes about its operating model or its partner relationships.

The difference is that they've locked pricing that would have been 15 to 20 percent higher by Q3 2026, they've moved to the front of the allocation queue for GPU nodes and other high-risk items that are otherwise subject to extended and unpredictable lead times, and they've recovered $200,000 from extended support they no longer need.

Total estimated cost avoidance: **$1.6M to $2.1M** compared to if they procured in Q3 2026 at prevailing market pricing.

In Customer A’s words:

> *Nothing changed about how we operate. Our partner still does the deployment. Our team still runs the platform. The only difference is we bought the hardware at a better price, with priority allocation on the items that matter most. The GPU positioning alone justified the decision.*

University B - "Hardware + Colocation"

Profile: Mid-size metropolitan university, strong engineering and health sciences faculties

The situation:

University B has a campus data centre that's approaching capacity. They've been planning a significant research compute expansion to support two concurrent initiatives: a new AI and machine learning capability for its engineering faculty, and a health data analytics platform for its medical school that requires sovereign hosting to meet HREC and ethics committee requirements for sensitive health data.

The campus facility can absorb some additional standard compute, but it cannot support the power density, cooling, or physical security requirements of GPU-accelerated nodes or a health data platform that needs to meet ISO 27001 and the Australian Government's Hosting Certification Framework. They've been evaluating colocation options for six months but haven't committed, partly because the pricing environment has been too volatile to lock in a multi-year agreement.

What they need:

$4.6 million across new Dell infrastructure and sovereign colocation, with the research compute and health data platform hosted off-campus in a certified sovereign facility, and the standard campus infrastructure refreshed on-site.

How they use the program:

Item	Credit allocation	Deployment
Dell PowerEdge R760 servers (×20), campus workloads, teaching labs, admin	$800,000	Delivered to campus
Dell PowerEdge XE9680 GPU servers (×4), AI/ML research compute	$2,080,000	Delivered to Macquarie Cloud Services colocation
Dell PowerEdge R760 high-memory nodes (×6), health data analytics	$360,000	Delivered to Macquarie Cloud Services colocation
Dell PowerStore 500T storage, research data	$320,000	Delivered to Macquarie Cloud Services colocation
Dell networking, campus refresh	$180,000	Delivered to campus
Macquarie Cloud Services colocation, 4 racks, power, cooling, connectivity (36 months)	$560,000	Macquarie Cloud Services sovereign data centre
Macquarie Cloud Services secure interconnect, campus to colocation facility	$120,000	Network service
Remaining Dell extended support returned to university	($80,000 recovered)	
Total credit purchase	**$4,600,000**	

Credit split: approximately 82% hardware ($3,740,000) / approximately 18% colocation and connectivity services ($680,000), with $80,000 recovered from extended support and $180,000 in campus networking.

What happens:

- University B purchases $4.6M in credits, scoped against a blended BoM of Dell hardware and Macquarie Cloud Services colocation services.
- Macquarie Cloud Services works closely with Dell to identify high-risk items in the order. The four GPU servers are the primary concern, and the consolidated order positions the university's allocation at the front of the queue.
- The 20 campus servers and networking equipment are delivered directly to the university as hardware becomes available.
- The GPU servers, health data nodes, and research storage are delivered to Macquarie Cloud Services' sovereign data centre, racked in dedicated colocation space that meets ISO 27001 and Hosting Certification Framework requirements.
- A secure, low-latency interconnect is provisioned between the campus network and the Macquarie Cloud Services facility.
- University B's research computing team and health data team access its respective platforms remotely. The university retains full administrative control of the hardware. Macquarie Cloud Services provides the facility (power, cooling, physical security, connectivity), not the management of the servers.
- The health data platform satisfies HREC and ethics committee requirements for sovereign hosting of sensitive research data, something the campus data centre could not certify.
- As the research programs mature, University B has the option to layer managed services on top, but that's a separate decision, made on its timeline.

The outcome:

University B solves three problems with one credit purchase: they refresh its campus infrastructure, they stand up a GPU-accelerated research capability in a facility that can support it, and they establish a sovereign health data platform that meets its compliance obligations. The colocation component gives them the power density, cooling, and certification they can't provide on campus, while the hardware remains theirs.

Total estimated cost avoidance on the hardware: $560,000 to $750,000 compared to Q3 2026 pricing. The colocation pricing is also locked for the credit term. And the $80,000 in recovered extended support offsets a portion of the colocation cost.

In Company B’s words:

> *We didn't have the space or the certification on campus for the GPU nodes or the health data platform. The program let us split the deployment: campus hardware where it made sense, sovereign colocation where it didn't, all from the same credit pool. And the ethics committee signed off on the health data hosting in two weeks because the Macquarie Cloud Services facility was already certified.*

University C - "Full Infrastructure Refresh: IaaS + On-Premises + Backup"

Profile: Regional university, lean IT team, strong nursing, education, and agricultural science programs

The situation:

University C has been running its core IT infrastructure out of a small on-campus server room for over a decade. The environment has grown organically: 28 servers across two generations of Dell PowerEdge hardware (R640s, R740s, and a handful of older R630s), supporting the student management system, learning management system, HR and finance platforms, research data storage, library systems, and internal business applications. The hardware is a mix of in-warranty and extended Dell support. The server room itself has limited cooling, aging UPS, no redundant power feeds, and a single point of failure on the network uplink.

The IT team of six manages everything: infrastructure, applications, helpdesk, security. They've known for two years that a full infrastructure refresh is overdue, but the scale of the project (scoping, procurement, deployment, migration, decommissioning) has been beyond what the team can absorb while keeping existing services running.

The new CIO, who joined 18 months ago, has a clear view: most workloads should move to sovereign IaaS, but a small number of latency-sensitive and locally-dependent systems (campus network management, local print services, building management system integration, and a legacy research instrument controller) need to stay on-premises. The strategy is a hybrid model: sovereign cloud for the bulk of the estate, lean on-premises for the handful of workloads that genuinely need to be local.

They also have no backup for its Microsoft 365 environment. Exchange Online, SharePoint, OneDrive, Teams: none of it is backed up beyond Microsoft's native retention. Their CISO has flagged this as a compliance gap for over a year, but it's been deprioritised against more urgent operational demands.

What they need:

A full infrastructure refresh: sovereign IaaS for the majority of workloads, a small on-premises hardware footprint for local services, migration support, and M365 backup to close the compliance gap.

How they use the program:

Item	Credit allocation
Macquarie Cloud Services Sovereign IaaS, compute, storage, networking for 22 migrated workloads (36 months)	$820,000
Migration services, workload assessment, migration planning, staged cutover for 22 workloads	$180,000
Dell PowerEdge R660 servers (×4), on-premises for campus network management, BMS integration, print services, research instrument controller	$160,000
Dell PowerStore 500T, local storage for on-premises workloads	$95,000

Dell networking, campus switch refresh	$120,000
Macquarie Cloud Services off-site backup replication, research data and critical on-premises systems replicated to Macquarie Cloud Services sovereign DC	$185,000
CAUDIT Cloud SaaS Backup (M365 + Entra ID), powered by HYCU R-Cloud, sovereign storage in Macquarie Data Centres, 4,200 staff users (36 months)	$226,800
Remaining Dell extended support returned to university	($85,000 recovered)
Total credit purchase	**$2,200,000**

Credit split: approximately 17% hardware ($375,000) / approximately 83% services (IaaS, migration, backup, M365 protection).

What happens:

- University C's original BoM was $2.2M in Dell server, storage, and networking hardware for a full like-for-like on-premises refresh.
- During scoping, the CIO presents the hybrid strategy: migrate the bulk of workloads to sovereign IaaS, retain a small on-premises footprint for the systems that genuinely need to be local, and use the remaining credits to close the M365 backup gap and establish off-site replication.
- The BoM is restructured. Credits are allocated across a mix of hardware, IaaS, migration services, and backup.
- Macquarie Cloud Services conducts a workload assessment across all 28 servers, identifies 22 workloads suitable for IaaS migration, and plans a staged cutover that minimises disruption to the six-person IT team.
- Four new Dell PowerEdge servers, a small storage array, and refreshed campus networking are delivered to the university for the on-premises workloads as hardware becomes available: campus network management, building management system integration, local print services, and the legacy research instrument controller.
- The 22 migrated workloads are hosted on Macquarie Cloud Services sovereign IaaS in Australian-owned and operated Macquarie Data Centres.
- CAUDIT Cloud SaaS Backup is deployed for M365 and Entra ID, with all backup data stored exclusively in Macquarie Data Centres, providing Australian control, governance, and operational independence from Microsoft's ecosystem.
- Off-site backup replication is established for the on-premises research data and critical systems, providing disaster recovery capability that the campus server room never had.
- The bulk of the old server room is decommissioned. The remaining Dell extended support across the outgoing fleet is returned, recovering approximately $85,000.
- University C's IT team is freed from managing 22 server workloads (patching, firmware updates, disk replacements, cooling failures) and can focus on service delivery, the small on-premises footprint, and user support.

The outcome:

University C has gone from a 28-server on-campus server room with no redundancy, no M365 backup, and no off-site replication to a hybrid infrastructure model: sovereign IaaS for the majority of workloads, a lean and modern on-premises footprint for the systems that need to be local, comprehensive M365 backup, and off-site disaster recovery. The IT team's operational burden has dropped dramatically. The M365 backup addresses a compliance gap that was previously unmitigated.

The $85,000 in recovered extended support partially offsets the on-premises hardware cost.

And the CIO has delivered the hybrid strategy they were hired to execute, funded through a single credit purchase.

In Customer C’s words:

> *We needed to modernise everything, but we couldn't do it all on-premises with a team of six. The program let us move 22 workloads to sovereign IaaS, keep the four that needed to stay local on new hardware, and finally close the M365 backup gap we'd been carrying for two years. One credit purchase, one program, the entire refresh.*

University D - "Managed SOC"

Profile: Small specialist university, arts and design focus, 4,500 students

The situation:

University D has a modest infrastructure footprint. Most of its compute is already in Azure, and its on-premises presence is limited to a few legacy systems and networking equipment. Their immediate infrastructure refresh need is small.

What keeps its CIO up at night is cybersecurity. They have no dedicated security operations capability. Their IT team of three handles everything from helpdesk to firewall management. They've had two near-miss phishing incidents in the last six months, and its most recent ISMS audit flagged the absence of 24/7 monitoring as a critical gap.

Until now, they've relied on AARNet's SOC service for basic security monitoring. But AARNet has announced that the SOC service is being turned off in October 2026. AARNet's replacement pathway is CrowdStrike Falcon Complete Next-Gen MDR, a capable platform, but one that introduces a new vendor, a new agent, and a new technology stack into an environment that's already stretched thin.

University D is an existing Microsoft 365 A5 licensee. Their A5 licensing already includes Microsoft Defender for Endpoint, Defender for Identity, and Defender for Cloud Apps. They've invested in the Microsoft security ecosystem. Their identity is in Entra ID. Their endpoint protection is Defender. Their cloud workloads are in Azure. They're already paying for these capabilities and they want to maximise that investment, not layer a competing stack on top of it.

Migrating to CrowdStrike would mean running a parallel security ecosystem alongside Microsoft: a new endpoint agent competing with Defender, a separate detection and response pipeline, a different management console, and a different vendor relationship, all managed by a three-person team that can barely keep up with what they have today. It doesn't align with its strategic direction, and it doesn't make financial sense when they're already paying for Defender through A5.

What they need:

A managed SOC service that maximises its existing Microsoft security investment, not one that replaces it with a competing stack. Operational before October 2026, delivered as a service, not a capital project.

How they use the program:

Item	Credit allocation
Macquarie Cloud Services Managed SOC, 24/7 monitoring, detection, and response, leveraging Microsoft Sentinel and the university's existing Defender suite (36 months)	$432,000
Security onboarding and integration: Sentinel workspace deployment, log source integration (Defender for Endpoint, Defender for Identity, Defender for Cloud Apps, Entra ID, Azure Activity), detection rule tuning, baseline establishment	$48,000
Incident response retainer	$20,000
Total credit purchase	**$500,000**

Credit split: 0% hardware / 100% managed security services

What happens:

- University D's original BoM was $500,000 in Dell networking and server hardware for a campus infrastructure refresh.
- During scoping, the CIO raises that its most urgent risk isn't infrastructure age. It's the loss of its AARNet SOC coverage in October and the absence of a replacement that maximises its existing Microsoft investment.
- The BoM is set aside entirely. Credits are redirected to Macquarie Cloud Services' Managed SOC service.
- Macquarie Cloud Services deploys a Microsoft Sentinel workspace and integrates the university's existing Microsoft security stack: Defender for Endpoint, Defender for Identity, Defender for Cloud Apps, Entra ID sign-in and audit logs, Azure Activity logs. The Defender telemetry the university is already generating through its A5 licensing becomes the foundation of the SOC.
- Macquarie Cloud Services provides the operational layer that the university can't build internally: detection engineering, alert triage, threat hunting, incident response, and 24/7 analyst coverage, all built on top of the Microsoft ecosystem the university has already paid for.
- No new endpoint agents are deployed. No competing security stack is introduced. Defender remains the endpoint protection platform. Sentinel becomes the SIEM. Macquarie Cloud Services operates the SOC.
- The service is operational before October 2026, providing continuity of security monitoring with no gap between the AARNet shutdown and the new capability.
- The three-person IT team is no longer responsible for security monitoring. They receive weekly threat briefings and escalation support from Macquarie Cloud Services analysts.

The outcome:

University D has gone from an expiring AARNet SOC service to 24/7 managed SOC coverage that maximises its existing Microsoft investment, without introducing a new vendor, deploying a new agent on every endpoint, paying for a competing detection and response pipeline, or without exceeding the $500,000 minimum commitment.

The Defender capabilities they were already paying for through M365 A5 are now feeding a properly operationalised SOC. The ISMS audit gap is closed. The AARNet transition is addressed with months to spare. And the CIO can demonstrate to its council that the university has 24/7 security monitoring in place, built on the technology they've already invested in, aligned with its strategic direction, and delivered without adding complexity to a three-person team.

The infrastructure refresh hasn't disappeared. It's been consciously deprioritised in favour of a more urgent risk, with the option to address it in a future program cycle or through a separate procurement.

In Customer D’s words:

> *AARNet's SOC is disappearing in October and the replacement doesn’t fit our stack. We're an M365 A5 shop. We're already paying for Defender across every endpoint. We didn't need another agent and another vendor. We needed someone to operationalise what we already have. The program let us redirect every dollar to a SOC that builds on our Microsoft investment, not one that competes with it.*

Summary: Four Universities, Four Outcomes, One Program

	University A	University B	University C	University D
Profile	Large Go8	Mid-size metro	Regional	Small specialist
Credit commitment	$10,800,000	$4,600,000	$2,200,000	$500,000
Hardware %	100%	~82%	~17%	0%
Services %	0%	~18% (colo + connectivity)	~83% (IaaS + migration + backup)	100% (SOC)
Dell BoM taken?	Yes, full	Yes, partial (campus + colo)	Yes, small on-prem footprint	No, redirected to SOC
Delivery model	Campus delivery, deployed by trusted partner	Campus + sovereign colocation	Hybrid: sovereign IaaS + lean on-prem	Managed service (Sentinel + Defender)
Extended support recovered	$200,000	$80,000	$85,000	n/a
Key outcome	$1.6M to $2.1M cost avoidance + priority GPU allocation, existing partner model preserved	GPU + health data platform + sovereign compliance	Full infrastructure modernisation + M365 backup	AARNet SOC replacement, Defender-native, no new stack

The point:

The program starts with a Dell bill of materials to ground the credit value. But where the credits end up depends entirely on what your institution actually needs. Hardware to campus, deployed by your existing partner. Hardware in colocation. A hybrid of IaaS and on-premises. No hardware at all. The program accommodates all four, because the credit mechanism is designed around institutional outcomes, not product categories.