Controls assurance and continuous assurance

MODULE 5 | 5.4.2 | STUDENT COMPANION

Assurance on controls asks whether controls are **suitably designed**, **in place** and **operating effectively** over a period. It can cover an entity's own controls or those of a **service organisation**. A **type 1** report covers design at a date; a **type 2** report adds operating effectiveness over a period, so only a type 2 report gives a user auditor evidence of operation. Even a clean report leaves the customer owning its **complementary user entity controls**. **Continuous assurance** moves testing closer to real time.

Assurance on an entity's own controls

The AUASB's standard on assurance engagements on controls (ASAE 3150) covers an entity's own controls, at reasonable or limited assurance, and can address their design, their implementation and their operating effectiveness throughout a period. In an **attestation** engagement, management describes and evaluates its controls and the practitioner reports on that evaluation; in a **direct** engagement, the practitioner does the evaluating. A regulator might require one, for example over the controls that protect client money, or a board might commission one over a new system.

Controls at service organisations

Many entities outsource processing such as payroll, cloud software, investment custody or payment handling. A **service auditor** can report on the service organisation's controls under ISAE 3402, or ASAE 3402 in Australia. The customer is the **user entity**, and its auditor (the **user auditor**) decides how far it can use the report when auditing the customer, under ASA 402.

Two types of service organisation report

	Type 1 report	Type 2 report
Covers	A description of the system, and whether the controls were suitably designed	The same, plus whether the controls operated effectively
Timing	At a specific date	Throughout a period, usually six or twelve months
Tests	No tests of whether the controls operated	Includes the tests performed and their results
For a user auditor	Design only: no evidence that the controls worked over time	The only one that gives evidence of operation over time

In the United States: SOC 1 reports cover controls relevant to customers' financial reporting; SOC 2 reports cover security, availability, processing integrity, confidentiality and privacy

Before a user auditor relies on the report

1. **Scope and period**
   The right services, systems and controls, for the right period
2. **Type**
   A type 2 report, if the auditor needs evidence the controls operated
3. **Exceptions**
   Did any tests find exceptions, and what do they mean for the user entity?
4. **Complementary controls**
   Controls the provider assumes customers have: check they're in place at the user entity, and test them if relying on a type 2 report
5. **Carved-out providers**
   Parts of the service handled by another provider and left out of the report
6. **Bridge letter**
   If the period stops short of the year end: ask about changes since, and consider other procedures

At Voltana

- The cloud provider of the new accounting system supplies a type 2 report for January to June 2026
- Controls effective, with one exception in the provider's change testing that didn't affect Voltana's modules
- Complementary control listed: each customer reviews its own users' access regularly
- Voltana's leftover project access rights show that control failed, so Linden Ridge must deal with it at Voltana

A clean report never covers the customer's own part of the controls

Complementary user entity controls are the customer's side of the bargain: the user auditor checks they are in place at the user entity, and tests them when relying on a type 2 report. **At Voltana**, the new system went live in February 2026 and the report runs to 30 June, Voltana's year end, so it covers the months that matter and no bridge letter is needed. The one exception didn't touch Voltana's modules. But the report assumes each customer reviews its own users' access, and the leftover project access rights in Voltana's management letter show that control failed. Linden Ridge must deal with that at Voltana, for example by testing who had access and what they did with it; the provider's clean report can't cover it.

Case note: Latitude Financial, 2023

In March 2023 the consumer lender Latitude Financial suffered a cyber attack that began at one of its major vendors, where the attacker obtained a Latitude employee's login credentials. The attacker used them to reach customer data held by Latitude and by two other service providers. About 14 million records were stolen: about 7.9 million driver licence numbers, about 53,000 passport numbers and about 6.1 million older customer records. Latitude refused to pay the ransom that was demanded, announcing its refusal on 11 April 2023.

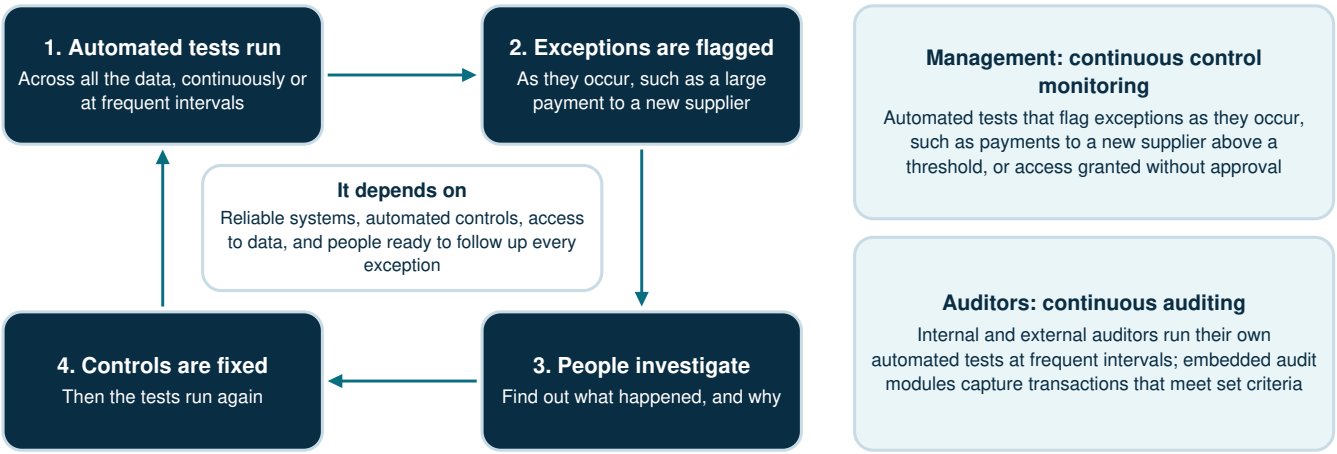
The lessons: an organisation's security is only as strong as the access it gives its suppliers, so boards need assurance over the providers they let inside, not only over their own controls. For auditors, access controls are both a service organisation issue and a user entity issue.

Source: Latitude Financial ASX announcement (16 March 2023) and cybercrime updates (27 March and 11 April 2023).

Continuous assurance

Continuous control monitoring is management's tool: automated tests that flag exceptions as they occur, such as payments to a new supplier above a threshold, or access granted without approval. **Continuous auditing** is the auditors' version: internal or external auditors run their own automated tests at frequent intervals, and some systems contain **embedded audit modules** that capture transactions meeting set criteria.

The continuous assurance cycle



Assurance moves closer to real time, but only real follow-up turns alerts into assurance

It works only with reliable systems, automated controls, access to the data and people ready to follow up every exception. Without the follow-up, it simply produces a growing list of unread alerts.

Does a clean service provider report end the customer's worries? No. The customer still owns its complementary controls, any services carved out of the report, and any months the report doesn't reach, as Voltana's leftover access rights showed.

Practice questions

MODULE 5 | 5.4.2 | TRY THESE BEFORE THE WORKED ANSWERS

Question 1 - Type 1 or type 2?

Situation	Type 1 or type 2? Why?
(a) Before signing with a new cloud payroll provider, a company's finance director wants to know whether the provider's controls are suitably designed. The service starts next month.	
(b) An investment fund's auditor plans to rely on the custodian's controls over recording trades for the whole financial year, to reduce substantive testing.	
(c) A retailer's auditor won't rely on its card payment processor's controls, but needs to understand them for its risk assessment.	
(d) After a near miss, an audit committee wants evidence that its outsourced IT provider's backup and recovery controls worked throughout the last six months.	

Question 2 - What does Brightstone's auditor still need to do?

Brightstone Cleaning Services Pty Ltd (imagined), a commercial cleaner with a 30 June 2026 year end, outsources its payroll to Paystead Payroll Services Pty Ltd (imagined), and its auditor plans to rely on Paystead's controls. From this extract of Paystead's controls report, identify what Brightstone's auditor still needs to do.

Section	Extract
Type and period	Type 2, on Paystead's payroll processing system, for 1 July 2025 to 31 March 2026
Scope	Payroll calculation and payment of net pay. Paystead's superannuation clearing service, which Brightstone also uses, is not covered
Subservice organisation	Paystead's servers are hosted by an outside data centre company, whose controls are carved out of this report
Exceptions	Control 4.2: for 3 of 25 new employees added to customers' payrolls, Paystead couldn't produce the customer's signed authorisation
Complementary user entity controls	Customers should (1) authorise every new employee and pay-rate change before sending it to Paystead; (2) review Paystead's exception report before each pay run is released; (3) limit who can approve pay runs on Paystead's portal

Question 3 - Continuous monitoring for Bandstand Tickets

Bandstand Tickets Pty Ltd (imagined) sells concert tickets online, paid by card. It keeps a booking fee and pays each promoter the ticket money after the concert, less refunds. Staff issue refunds and complimentary tickets, and set prices from promoters' instructions. Design three continuous monitoring tests.

Test: what it checks	What a flag could mean	Who follows up, and how
1.		
2.		
3.		

Worked answers

MODULE 5 | 5.4.2 | WORKED ANSWERS - ATTEMPT THE QUESTIONS FIRST

Question 1 - Type 1 or type 2?

	Report	Why
(a)	Type 1	The question is whether the controls are suitably designed, before the service even starts. A report on design at a date is what's needed; there is no history of operation to test yet
(b)	Type 2	Relying on controls needs evidence that they operated throughout the period. The report should cover as much of the year as possible, with a bridge letter and other procedures for any gap
(c)	Type 1 is enough	Without reliance, the auditor only needs to understand the service and the design of the relevant controls to assess risks; a type 2 report would also do
(d)	Type 2	The committee wants evidence that the controls worked over six months; a type 1 report shows only their design at a date

Question 2 - Brightstone's auditor (suggested)

- **Bridge the gap, 1 April to 30 June 2026.** Obtain a bridge letter from Paystead about any changes to its controls since 31 March, and perform other procedures for those three months, such as testing some April to June pay runs. The report says nothing about them.
- **The exception.** Find out its cause and whether any Brightstone employees were affected; test Brightstone's own authorisations for new starters; decide whether reliance on that control is still justified, or extend substantive testing of new starters.
- **Complementary user entity controls.** Check that Brightstone's side is in place and, because the auditor is relying on the type 2 report, test it: authorisation of new employees and pay-rate changes before they go to Paystead, review of the exception report before each pay run, and limited, reviewed access to approve pay runs on the portal. If these fail, Paystead's good controls don't help.
- **The carved-out data centre.** Decide whether the hosting company's controls (security, availability, data integrity) matter to the audit. If they do, obtain its own controls report or other evidence, or check how Paystead monitors it.
- **Superannuation.** The clearing service is outside the report, so test superannuation directly: recalculate contributions for a sample of employees and agree the payments to the funds, including their timing.
- **The report itself.** Check that it covers the services and system Brightstone uses, that the service auditor is competent and independent, and read the tests and results, not just the opinion.

Question 3 - Bandstand Tickets (any three; suggested)

Test: what it checks	What a flag could mean	Who follows up, and how
Refunds: each refund compared with the original sale; flag refunds to a different card, above the price paid, for a concert that wasn't cancelled, or many by one staff member	Staff or customer fraud, or refund errors	The finance manager reviews flags daily, checks the authority and the customer record; repeat flags for one person go to senior management
Complimentary tickets: count per concert and per staff member; flag any above the promoter's approved number, or issued without an approval reference	Free tickets resold by staff, or lost ticket revenue	The operations manager checks the promoter's written approval and cancels unapproved tickets before the concert
Prices: each sale compared with the price set from the promoter's instructions; flag any sale below it, or any price change after sales open without the promoter's approval	Unauthorised discounts, or errors when prices were set up	The event coordinator confirms with the promoter, corrects the price and reports any shortfall to the promoter
Also possible: promoter payouts made soon after a change of bank details; user access granted without approval; refunds processed by the person who made the sale	Payment fraud, or weak access controls	Finance or IT security, with any confirmed problem escalated and the control fixed