

NSW SMALL BUSINESS MONTH 2026

Is Your Website Quietly Becoming a Business Risk?

A practical website control check for growing small businesses

Wil Brown · Zero Point Development
Recorded 22 October 2026

EDITED TRANSCRIPT

Lightly edited for clarity and readability. Opening waiting-room chatter, an unrelated news aside, screen-control remarks and repeated audience thanks have been omitted. The discussion, examples and advice follow the session as delivered. This is a transcript, not a separate technical audit or fact-check.

Section timestamps refer to the supplied recording captions. Select a topic below to jump to that section in this PDF.

01:40 Welcome and acknowledgement

07:25 01 | Ownership and control

17:22 02 | Access and security

26:40 03 | Backups and recovery

36:19 04 | Enquiries, bookings and sales

43:12 05 | Documentation and continuity

50:00 Your checklist and next actions

54:37 Questions and closing remarks

Welcome and acknowledgement [01:40]

Today we're looking at: is your website quietly becoming a business risk? Websites run in the background. We all know we need them, but there are certain aspects that need to be looked after. There are responsibilities as well. You have to know things to be able to put things in place in case something goes wrong. That's what we're talking about today: practical control checks for small businesses to look after their website.

I would like to acknowledge the Traditional Custodians of the land on which we meet and pay my respects to their Elders past, present and future. I would like to extend that respect to the Aboriginal peoples present today. I'm proud to be hosting this event as part of the NSW Small Business Month programme in partnership with the NSW Government.

Opening poll: how much control do you have? [02:39]

Let's do a poll first. In the comments, type a number that matches your expectation. How confident are you that your business has full control of its website?

1. Very confident.
2. Fairly confident. You think someone should be looking after it, but you've not really checked whether that person is.
3. Not very confident. You know there are some gaps.
4. Honestly, you don't know where to start.

We've got some twos and threes. That's fairly average. I've given this webinar a few times now and usually get people in the middle. It's fine not to know where to start. If you don't want to broadcast that to everyone, that's okay.

Whatever answer you come up with, keep that in your mind. Today we're going to walk through five checks that will help you see what's covered, what needs checking and what needs some attention. You don't need to become a technical person. This is a non-technical talk. You just need to know what questions to ask and who is responsible. Thank you for adding those to the comments.

About Wil Brown [04:19]

A little bit about me. Hi, I'm Wil Brown. I'm a WordPress consultant and educator, and I run a business called Zero Point Development. I help businesses and organisations solve website problems, particularly when their website has grown into something they depend on for enquiries, bookings, payments, or delivery services. Often the challenge is understanding how everything fits together and who's responsible and what happens when something changes or stops working.

I also organise the WordPress Sydney and Elementor Australia meetups. So making technical topics practical and understandable is a big part of what I do. Today, I'm going to draw on some situations I've encountered with clients, including backups that couldn't be

used and important knowledge that left when someone retired. My aim is to help you ask better questions and leave with a clear idea of what to check next.

What would stop if your website stopped? [05:26]

If your website stopped working tomorrow, what would your business be unable to do? Do you actually know? You can add some stuff in the comments if you wish, but this is more kind of practical, just thinking in your head, jot it down on a bit of paper if you've got some there. But have a think, if your website stopped working, if you got up tomorrow, Friday morning, and your website was down, what would your business be unable to do?

So some examples are enquiries, so contact form, maybe bookings, payments, making sales for things, or you might have a customer portal or a membership site that they can't log into. So have a think about one or two key things that if your website stopped working that you'd be unable to do. Because we're going to work through what we need to do to bring those back up and running.

The five website control checks [06:20]

Here are the five checks we're going to explore today:

1. Ownership and control.
2. Access and security.
3. Backups and recovery.
4. Enquiries, bookings and sales.
5. Documentation and continuity.

An attendee mentioned sales. Of course, we're in business to make money, so sales is usually our number one.

For each of these checks, there are three responses to record:

Confirmed: you can verify it.

Need to check: you're relying on an assumption.

Needs action: you know there's a gap and something needs doing.

Not every item applies to every website in every instance. It's fine to leave today with questions to ask your team or IT provider. We'll finish by choosing three priorities to move forward with next.

01 | Ownership and control [07:25]

Let's start with ownership and control. Can your business actually take control of the things it depends on? Now, a website can be working perfectly while the business has very little visibility over the accounts behind it. So you can update a page, you can receive enquiries and you can pay your developer each month without knowing where the domain name is registered or how you'd recover access or how you get access to backups.

That doesn't mean that you need to take over all the technical work. Delegating that work is pretty sensible. What you need, though, is a clear understanding of the arrangements and a reliable way for authorised people to access the essential stuff. So when I say domain, I mean your web address, your .com, your .com.au, your .org.au, that sort of stuff. The hosting, that's where your website runs on.

And these can be the same provider or they can be separate providers. The platform or system you manage it, such as WordPress or Wix or Squarespace, that's a hosted website service. And as I say, it might be connected to your domain name or it might be separate. But it's worth looking at the accounts and worth identifying where those things are and who owns that stuff, because that's the big first step in looking after your website.

Identify the essential accounts [09:01]

So there are three groups here. First, your domain and DNS. So as I said, the domain is the address that people use to find you, the URL or your email as well. DNS is the set of directions. It's like a roadmap that sends visitors to the right place, the right web server. and it can also direct your email. So everyone at yourdomain.com.au, which is why changing any of these settings without understanding them can cause problems beyond just the website itself.

Now, good news is you don't need to learn how to configure DNS today. You just need to know who manages it and how to contact them. So if something goes wrong with your email, for example, you're not receiving emails, Who do you go to or which provider do you go to? Do you actually know that? Is that written down? Second is hosting or your website platform.

Some businesses pay for hosting separately. Others have subscription and bundles. The website builder, for example, hosting support altogether. Either way, we really need to record the provider and who manages that account so that if something goes wrong, then we know exactly where to go or who to go or who to contact. The third is software and connected services. Now, this is where the list can grow without anyone kind of really noticing.

Things like your booking system might be a separate service. Payments might go through another provider like Stripe or PayPal. Your forms on your website might send information to a CRM such as Salesforce or FluentCRM, or it might go to an email platform like Mailchimp or ActiveCampaign. So what you really need to do is think about the journey that your primary customers take through your websites.

Which service do they have to work with and interact with for that journey to go from start all the way to finish? Now, you don't need a perfect technical inventory to begin with. Just start with your web address, where the site runs, and the services that handle your most important business activities. Then you can ask your IT provider, if you have one, to fill in those gaps.

So, for example, a service provider might have just a single web page with a contact form that people will contact them or get in touch with their phone. So the customer journey would be they search for something, they click on the website, they send a form, the form then notifies the service, and then the service responds to the customer. And that would be the full thing.

If you're selling products, that's a little bit more complicated. People go on the website and look at your product list, then a single product. They might check reviews and videos, then purchase. There's a checkout, a payment, and then shipping or receiving a digital service. So depending on what your company does and what your website offers, people will be interacting with more different services.

So we need to understand where those services live, who owns them or who is the contact person for them.

Four questions for every account [12:24]

So for each of these accounts, there are four useful questions. One is who holds and manages it. And those can be different people. So your business might hold the account while your developer might manage it on your behalf. For your domain, ask who is listed as the registrant and whether those details reflect the business arrangement. What we mean by that is when you register a domain, somebody usually gives an email address, a phone number, and there'll be a business address as well.

And whoever's registered that domain, then if there's any changes to that domain, like renewals or expires, then that email address is then sent the notifications. The problems arise when a single person registers something, and then maybe a few years down the line, that person's gone away, has moved, and then email notifications say this domain's going to expire, keep going to this old email address.

And then the domain expires, email goes down, website goes down, things like that. So it's very important to know who manages that particular stuff. Number two is who pays and who receives all these renewal notices. So an automatic payment is useful, but credit cards can expire after a few years. So if the warning, say, goes to somebody who maybe left two years ago, then the business might never receive it.

And again, things start to expire without anyone knowing. Number three is can the business recover access? So check things like recovery email addresses for domain names or for website hosting packages and the phone number as well. Are they current? Can an authorised person use them? A login saved on one person's laptop isn't much of a recovery plan if it gets replaced or the person leaves that company.

And number four is what happens if you change suppliers. So for example, your developer might provide a paid software licence through their agency subscription for looking after your website. And that can be a perfectly reasonable arrangement. You just need to know whether it ends if you leave and go to another provider, whether you need your own subscription, and what it would affect if that subscription goes away or you can't pay for it.

The goal here isn't to implement anything or understand how the technology works. It's just for clarity. So don't start transferring accounts because this webinar has made you a bit nervous. Establish all the facts first. Who owns something? How do you know where to go? And all the renewal information. Then agree any changes with the people involved.

Audience question: Will we be able to get a copy of the slides?

Wil: Yes, I'll make the slides available afterwards. There's also a checklist I'll send out after the webinar.

“Our developer handles it” [15:22]

This is a favourite quote of mine. Our developer handles it, and it's an answer that I can understand. So you've hired someone because you don't want to spend your day managing website accounts. That's fair enough. The follow-up question is, can they show you the details and explain what happens if the arrangement changes? So it's all right to have somebody looking after stuff, but if they go away or disappear, then what happens?

So we need to know this. A good provider should be able to help you understand who the providers are, who holds each account, who receives renewal notices and how authorised access works, how you need to access to change something or modify something. And you can frame it quite simply. You can say: 'We're updating our business records. Can you help us document the accounts the website relies on and the handover arrangements?' It's as simple as that.

And so if you're not sure who hosts your website, get in contact with the IT provider and ask them these questions. Who do I contact? Who looks after it? Who's allowed to make changes? That sort of stuff. That's just ordinary housekeeping, business housekeeping. It's the same reason you keep records for your accountant, your insurer, other suppliers, things like that. Remember, a password on its own doesn't really tell you everything.

There may be a second authentication step, sometimes called MFA or 2FA, two-factor authentication. There might be a recovery email address or another account behind that service. We need clarity about what's happening, where those things are and who controls them. If you only follow up on one thing from this section, confirm the domain account and renewal contact. Make sure the answer is recorded somewhere the business can find it, rather than just one person.

02 | Access and security [17:22]

Check number two. This second check is about people. So do the right people have the right access? And these are all things that have come up in my twenty years of looking after clients and doing websites. It's amazing how when something goes wrong, a website goes down, for example, or a service isn't working, the business doesn't know where to go. So this is all about the clarity around that.

So we've just looked at the accounts the business depends on, domain name account, website account, hosting account, that sort of stuff. Now we're looking at the individuals who can use them. So for a website login, for example, administrator access, doesn't matter whether you're running Drupal or Joomla or WordPress or Wix or Squarespace, in general, an administrator access is the highest level. And that usually gives somebody the ability to change really important settings and manage other users.

Now that's a lot of control. Someone who maybe updates opening hours or some content on the pages, maybe publishes some blogs or updates an events calendar, probably shouldn't have access to everything. So the useful question here is, what does this person need to do their job today? So there might be many businesses here who are single person businesses, and that means you.

So you have an admin account, that makes sense because you're looking after everything. But then again, there might be organisations where we've got different layers. So we might have editors, we might have a website team, we might have a marketing team that go in and change different things. So the idea here is to really just understand who has control and do they have enough control just to do their job and not too much control.

Again, one of the things I see most often when I do website audits is when I log in, I see that everyone is admin. So there's now twenty, a hundred different admins because there might be a bit of the website that somebody needs access to. And it's just easier to give them just access to everything rather than kind of drill down to give them access to what they need.

But then there's a huge risk with that, because if you give everyone full control, then they can go in and change settings, for example. So this gives you a much better starting point than just giving everyone the same login and hoping that nothing goes wrong.

Review current and former users [19:49]

So a quick access review. Start with current staff and suppliers. Can they do the work they're responsible for? That is interacting with the website. And is their access to the website appropriate? Then look at people who have left. Think about former staff, freelancers, agencies, anyone who helped with a short project. An account may have been created for them, and that might be a perfectly good reason at that time.

But the question is, does that account still exist? Should it still exist? And please note, before you delete accounts, please check with your IT provider, your hosting provider or the business. Some accounts may own content or be connected to things like automated processes. So you just really want to remove unnecessary access without disrupting

something that the business still uses. But definitely look for former staff and contractors accounts that can be safely deleted.

They don't need access, should not have access anymore. Then you want to have a look at shared logins. If three people use the same account, it's harder to kind of know who changed something. And it's also harder when one of those people leaves. Because changing the access means kind of changing it for the other people. So where the service supports it, individual accounts make things much easier to manage.

I always advise my clients, don't share any logins. If you need, create a new user and give it to that person. I've come across lots of times where managers have PAs and the manager will just give them their login. And then if something goes wrong, who's to blame or should they have had that access anyway? No, they shouldn't. So don't stop at the website and the website dashboard.

Also include these things like your hosting account, your domain account, things like payment services, and any other important systems that are connected for your CRM, your email system. Who has access? Do they still need access? And revoke that access if needed. So a useful task today is to ask for a current user list. If you don't know how to get that, you can ask your IT provider, what are the current users on my system?

And give me the level of access. And for each person, just go down that list and confirm who they are what access they have, and why they still need it. You can do that review with your provider or yourself. You don't have to work it all out yourself. You can go to your manager, for example. But it's a good thing to do, at least just now, and then build that into maybe something like a quarterly or six-monthly review process as well.

Passwords, authentication and recovery [22:29]

There are a few habits that make these access arrangements much more dependable. Things like using a different password for each important account and store those passwords in something called a password manager rather than just writing it down. That means that people don't have to remember every password or reuse the same password across several services. It also means that you can use complex passwords.

A lot of people avoid using complicated passwords because they can't remember it. But if you can't remember it, that means it's difficult for the hackers as well. So that's a good thing. Personally, I use something called Bitwarden for my personal stuff and my business password storage. The paid version, there is a free version, but there's a paid version that actually allows you to share passwords temporarily with other people via email.

And it doesn't actually reveal the password, just lets them use it. And then you can revoke that after, well, manually or after a certain time. So that's the one that I use, but there are many other software password managers out there. What I would also recommend is you turn on something called multi-factor authentication, MFA or 2FA, if that's available to you, especially for the admin accounts.

That's like an extra check beyond just the username and password. It will prompt for a code for your mobile phone. I use Google Authenticator on my phone. It comes up every thirty seconds, six digits change. So it gives you a thirty second window to enter your six digit code. And it's something you carry with you that even if someone can compromise your password, you shouldn't be able to get that one as well.

So that could be in the form of that authenticator code. It could be your phone. It might send a text message or it could be by email as well. So also include your email account in this. If someone gets access to your email, then they may be able to request things like password resets for other services. So for example, I use Google Workspace.

So I'm on Google, and whenever I access my Google account, it asks for my authentication into my email from my Google authenticator. I put in my six digits, and then I get access to my email. But if no one has those digits, then they can't get access to your email, and the same with admins on your website. But think about recovery as well as protection.

So what happens if the person with the authenticator app loses their phone or goes on leave or leaves the business? How can you get into that account? When you set up multi-factor authentication, you're usually given a set of codes, one-time codes, maybe six of them or ten of them. You need to be able to save those codes in a business, a shared business area that only authorised people can get access to.

Just in case, for example, the CEO's lost his phone and needs to get into his email, then that's the kind of the backup and the protection for those. So keep recovery details current, store them securely with access limited to authorised people. Your recovery arrangements need to work for the business without making sensitive information available to everyone. So a nice secure place to keep that stuff.

Finally, name the person responsible for updates and alerts. Things like we have a security plugin, doesn't really answer the question of who receives the alerts and what they do when one arrives. So the same applies to updates. If your provider is managing them, or are you managing them, or does someone check the important parts of the website afterwards is still working, things like that.

So these are ongoing responsibilities. They don't guarantee you'll never have a problem, but they make it much less likely that an avoidable gap sits unnoticed for months, like a contact form not submitting data or nobody receiving that notification because it's gone to an email address that nobody uses now or monitors. And that's of course lost business revenue. Now, let's look at what happens when something does go wrong.

03 | Backups and recovery [26:40]

So check number three is recovery. So the quote, we've got backups, sounds reassuring, but it leaves quite a few questions unanswered. Are the backups recent? Do they include everything you actually need to recover? Can someone restore them? And how long would that take? Now a backup is one part of getting the business back up and working again, but you also need a person who knows what to do, how to access the right accounts and a plan for customers while the website is unavailable.

This is an area where I've seen a lot of assumptions come unstuck. So let me give you an example.

The backup that crashed the website [27:23]

I had a client whose website crashed when the backup service ran. Now, you can understand the immediate concern. This person offered certification and membership. So they had thousands of people on the website, people going through courses and getting certificates, for example, and they had peak sessions. So a few months where they had lots and lots of people going through. And if the backup service ran, their website would go down and they need to contact the IT company to stop the server, restart the server, and everything would be okay again.

Now, of course, the website needs to stay available for the users to complete all their courses. And with the backup service bringing it down, what did the client do? They switched off the backup service. So that stopped the backup process from causing disruption, but it also meant that they now no longer had that backup protection in place. So the underlying problem hadn't been resolved.

Now, I'm not telling you that story to make fun of the decision or to bad-mouth the client. It was a reasonable decision to make because the immediate concern was the website, the revenue, the people using the website. So when something's interrupting your business, of course you want that interruption to stop. The problem is when a temporary workaround becomes the permanent arrangement and nobody comes back to fix it.

So this had been going on for about eight months when I got brought on board. And I couldn't really do anything with the website because I had no access to backups. We were in a real rut at that point. So that can happen with all sorts of website processes, not just backups. Something causes trouble, someone switches it off, and six months later, everyone assumes that it's been kind of taken care of, but nobody has really looked into it.

So the question to ask isn't just, did we get backups when the site launched? It's what evidence do we have that they're running successfully right now? If a backup is causing problems, that needs investigation. Switching it off might remove the immediate problem, but you still need a working recovery arrangement that's ongoing to fit your business. And even when backups are running, there's other ways it can let you down.

Three ways a backup can fail [29:53]

These are three different problems I've encountered across many different types of websites and different types of industries and clients. Number one, or first is the backup is too old. So I've seen a monthly backup arrangement. So backups get done every month, but that leaves twenty days of sales data missing. For example, when the website needs to be recovered. The backup may have done exactly what it was configured to do, and it might run and it might work.

It just simply didn't match how that information in the business was working and how it was needed to be backed up. So there's too big a gap. Number two is the backup is incomplete. Now, I've seen backups only containing the database and others only containing the files. I've seen backups only backing up a particular directory, even though that's not the current one.

So for example, I work in WordPress, but the same can be for Wix and for Squarespace and for any other system, right? So on a typical WordPress website, files include things like images, documents, PDFs, website software itself. But the database stores much of the content, things like settings and records, people records, products, orders, things like that, bookings. So you generally need to have both parts together to recover the website properly.

And many backup software, many backup plugins, services come with a very light version and don't include everything. So that's definitely something to check to make sure that backup is complete. Otherwise, when you go to restore, you've not got everything there to bring your website back up and running. The third, and it does happen, is the backup is unusable. So I've encountered backups that look okay, it looks like a file, and it might be several gigabytes or megabytes in size, but when you go to unzip, unarchive, untar that particular archive, that compressed archive, then it comes up with an error. which is no use.

So files may be being created, but you can't assume that they're going to work unless you test them. So these are separate experiences, but they all kind of point to the same issue. Having something labelled as a backup doesn't establish you have a recovery process. Some information may still exist elsewhere, perhaps with a payment provider, but generally piecing those records together is going to take a lot of work.

You really need a complete backup system, a backup file, if you want to bring your website back up and running. Hosted platforms, they might have their own recovery and export options. So you really need to ask what yours really recovers, rather than assuming that every platform works the same way.

How much could the business lose? [32:47]

So before asking how often you need a backup, answer these two critical business questions. One is how long could you manage without the website? So how long can your website be down for without you start to lose critical audience, critical trust, authority, and sales? And number two is how much recent information can you afford to lose? And this is different for different websites.

So for example, take a website that mainly displays services and contact details. If the content rarely changes, its recovery may be quite different from a website that takes bookings through the day. For the bookings business, even a daily backup could leave a gap. You might need hourly or real-time backups. If it ran last night, what happens about today's bookings? So think about the work involved in reconstructing that information.

Could you identify the customers? Would you have to call them? Would the bookings be lost somewhere? Could there be uncertainty about availability or payments? That sort of stuff. Now, you don't need technical terminology for this conversation. If you use an IT provider, tell them what the business needs and work out a plan together. For example, you could say: 'We need to understand how we recover today's bookings and what we do while the booking system is unavailable.' So that might be, for example, putting up, changing the homepage, putting a notice on the homepage to say the booking system is down, please contact this email, this phone number or send to this email, things like that.

But having that in place so when something happens, you know what to do is what we're talking about today. So that will give your provider something useful and meaningful to plan around. You can work with them together. The right arrangement really just follows what your business needs and businesses, different businesses need different recovery options.

Evidence of a recovery plan [34:42]

So here's the evidence that I would ask for. If we're thinking about recovery plan, what is the date of the last successful backup and what does it include? Is there a copy available if the main hosting environment fails or becomes inaccessible? Who can restore it and how do we contact them? And when was a restoration last tested? A successful email is useful to say backup's been done, but a successful backup job and successful recovery aren't quite the same thing.

So a restoration test establishes whether the backup can actually do that job of bringing the whole website back up. Now that test should be carried out safely by somebody competent and knows what to do. And it's usually almost always done on a separate environment, something called a development server or staging server. Please don't practice by restoring an old backup over your live website.

That's going to be a disaster. So for a busy website, also ask what happens to information created during that recovery process. Now, you don't want new orders being taken in one place while an older version is being restored somewhere else. So we need to work out what happens with that. And finally, agree with what the customer should do while you're in that recovery process.

Is there a phone number? Is there an alternative booking system? Is there another way just to get in contact with a person so they can deal with the enquiry? A workable recovery plan joins all these pieces together. The backup, the person, the process, the temporary way of keeping the business moving, and the customer.

04 | Enquiries, bookings and sales [36:19]

The fourth check is whether the website is still doing its job. So far, we've talked about access problems, things going down, but some failures are much quieter. The homepage loads, the photos look good, nothing obvious seems broken, but meanwhile, an enquiry isn't reaching the business or a customer can't finish a booking. So this is a check that business owners and staff can help directly with.

You know what the customer is supposed to do. The task is to follow that journey all the way through rather than stopping just at the first page that looks okay. An example, a direct example from just a couple of months ago was that a client noticed that leads had dropped significantly and they tested the form on the website and submitted something and that worked.

It said it worked, but leads were still, nothing was coming through. And what we found out was that the bit of software that meant to send that lead up to Salesforce, that was broken. The form was working. Customers could type in their details and submit them, and the form said it had submitted successfully and someone would get in contact. But that information wasn't being passed to the business.

That pipeline was broken. The client said: 'We don't understand. The form works. Look, we've tested it.' But they hadn't gone through the whole journey. The customer fills in the contact form. The form submits and sends to Salesforce. Salesforce then sends a notification to the sales team. They hadn't followed that whole journey through.

Four checkpoints for an enquiry [38:01]

So let's take a look at that simple enquiry form. There are four checkpoints to look at for a very basic enquiry contact form. One is first, can the customer submit it? Now I know that a lot of businesses assume that the contact form is there and it works. And I know that a lot of clients, a lot of businesses don't test that regularly enough.

And you're really relying on a customer to call you or email you separately to say, we filled out some of your contact form and it didn't work. So we should be proactively testing that. So the first step is, can the form submit? Or is there something there that's stopping people completing it? Number two is what does the customer see afterwards? So the customer should get a useful confirmation that tells them what happened and then what the next step is.

I know a lot of, I work with WordPress, I know a lot of the contact forms, you press submit and a little graphic spins round, then stops. The contact form disappears and you might be left with a title saying 'Contact us' and nothing else. The customer is left asking: 'Did that work? Should I submit another one? What do I do now?' There should be a notification, a confirmation that tells them what happened: 'Your details have been sent.

Someone will respond to you within forty hours.' Number three is, does the business actually receive that enquiry? Now, this is the bit that sometimes assumes a thank you message on the website, and it doesn't really prove an email reached the right inbox. So

check that destination inbox, that destination place, whether it's a CRM, Salesforce, FluentCRM, ActiveCampaign, or whether it's just storing it within the website itself, sometimes called entries or form entries.

Check spam as well. If the form creates a record in your CRM or another system, go there and make sure it arrives. We're looking at the full journey. Number four is: who takes responsibility? A technically successful enquiry can still go nowhere if it lands in an inbox that nobody monitors. So what happens if the usual person is away on holiday? Maybe they're on long-term leave.

Does someone else know that they're meant to respond or look after that inbox? So when you test this, label the enquiry clearly as a test and let the relevant staff know, and then follow it through from submission to receipt and then to responsibility and follow up. That gives you a much better evidence than the form looks like it works. And it helps if you separate a website problem from an email delivery problem to an internal process gap.

So all three can have the same outcome from the customer's perspective.

Test the journeys that matter most [40:55]

So choose the journeys that matter most to your business, the critical ones first. For a service business, that could be a quote request. For another business, it might be to make a booking or completing a purchase. For a membership or training portal, that might be logging in and accessing something, a course that person has been paid for or registered for. So try those journeys from the customer side, including testing on a phone and a tablet, because the experience might be quite different from your main office computer.

With purchases or bookings, agree the safest method first. You don't want a test accidentally taking things like stock out of circulation or reserving real appointment bookings or triggering a fulfilment process. Now your provider can usually help plan for payments, notifications, and a cleanup afterwards. They might even give you something called a sandboxed staging server, which is lifting a copy of your live website, putting it into a safe environment where it captures emails and it captures payments, but in like a sandbox, a test environment.

So you can still test all the things like purchase and fulfilment, but it's in like a closed box. That's the best way to test that sort of stuff. Your IT provider can probably, or your hosting provider, can probably set that system up for you. If something fails, think about the connected services as well as the website. Has a subscription expired? Has an account connected stopped working?

Is a message going to maybe an old email address? Repeat important checks after significant website changes. So if you've done a big update to your website, you should probably go in and check that journey again. Then choose maybe a regular interval that reflects how much you depend on that journey. So maybe a quarterly review is useful for broader housekeeping. But a busy sales or booking process might need to be checked a bit more often than that.

If you're doing like daily bookings, you might want to check at the end of the month that this system is still working properly. So start with one journey, the main journey that your business depends on. Confirm what success looks like, who checks it regularly, and what happens if it fails.

05 | Documentation and continuity [43:12]

Okay, fifth and last check. is whether someone else could pick this up. And what I mean by that is imagine the person who knows the website best is unavailable for a while. It could be leave, it could be illness, it could be retirement, or maybe there's a supplier changing direction on something. What would another competent person in your business struggle to find or explain If to say you're the person who knows everything and you go, could someone else pick that up and run with that?

So this isn't only about passwords and technical knowledge, knowing what plugins or pages or posts or CRMs you have. It might be knowing which report needs checking or why a particular approval step exists or which tasks still need to happen manually. So today we're looking for those dependencies. You don't have to document the entire business this afternoon, but you do want to notice where the important knowledge lives with just one person and maybe move that more into a broader business context.

When the knowledge retires with the person [44:24]

So one organisation I worked with fairly recently had a person who understood the entire setup and how it all fitted together. In fact, they developed it, they put it together, they ran with it for many, many years. They weren't a technical developer. They were the person who had worked out how the system should support the organisation, the business, and why things had been arranged in that particular way.

Then they retired, which happens. But most of that knowledge went with them because there wasn't any documentation to hand over. It was all in their head. So someone coming in afterwards could see the website. They could see all the different components. They could see the different systems. They knew what customers expected. What was harder to see was the reasoning behind them. So why does that information go there?

Who is supposed to check it? Is this step automatic or does someone need to do something manually for that to work? Why was this particular way chosen and why didn't it do this other way, which looks logically better than the way that it's been done? So those are business questions as much as technical ones. That's why just a list of software is not a complete handover.

It tells that next person what exists, but it may not explain to the organisation how it's actually used or why it's used or why it's implemented in such a way. The useful lesson to capture is the important decision and the recurring tasks while the person who understands them is still available before they leave. Even a short explanation of how does that work and why does it do it that way can give the next person a much better starting point.

What belongs in a handover record [46:15]

So a useful handover record can still be really small. It doesn't need to be pages and pages of documentation. Record the key accounts, renewal arrangements, how authorised access is obtained. Add your support contacts and the responsibilities. For example, who's looking after domains, who's looking after hosting, who handles website changes, who investigates payment or booking problems, things like that. Then record the connected services and the recurring manual tasks.

So the payment service, the CRM service, the Salesforce service, the person in marketing who runs a spreadsheet, the person in sales who exports the WooCommerce sales data for the month into the spreadsheet that then this other system needs, that sort of stuff. Document that sort of stuff. and include the recovery process and anything important like past decisions as to why something was implemented.

Now you don't need a history of every conversation, just focus on decisions that would be confusing and costly to rediscover if somebody leaves. Keep this record somewhere that the business controls and the authorised people can find. A document that only exists on one person's computer doesn't solve this problem. It's great for them, or if it's in their account, it's great for them.

But things like when people leave, particularly in larger organisations, accounts tend to get deleted. And if they've got the information there, that's no good. Update the documentation when something changes. If a new supplier comes along, if there's a new service, or if there's a change in responsibility, it's a good reason to review that relevant section in that documentation. Store passwords and recovery codes separately in maybe a password manager.

And the handover record can explain where the authorised access process is without becoming a document full of passwords and stuff. All we need to give is clear direction to where to go or who to go, what process to run. And give it a simple test. So give it to somebody else in their business and get them to say, look, you've come on, this person's left, this is now your decision.

Have a look at that documentation. Could you take that? Do you understand that process? If something goes wrong or if you need to update something, is there enough information there for you to run with it? If it only makes sense to the person who wrote it, then add enough context to make it useful for everyone else.

Give your records a home [48:47]

So where should you store all this information? Start with the business tools that your team already use. So things like a shared business folder in Google Workspace or Microsoft 365. You can hold your account register, your contacts and instructions. Make sure the business controls it and the right people can access it. Keep passwords and recovery codes in a business password manager like Bitwarden or 1Password.

Use your task tracker like Trello or Microsoft Planner, Asana, ClickUp, Notion, whatever you use in your business for things that need doing and then tasks that need doing and then link back to the relevant records that supports that process, that person to do that particular task. We're talking about SOPs here. Give someone responsibility for keeping that information current and make sure that other authorised person, people know where to find it.

Now you can start off with one folder and one document. It doesn't need to be complicated. I've highlighted a lot of stuff today, but we don't need to do all that stuff today and not all at once. Just the important stuff and work through all that and just make sure it's up to date and relevant.

Your checklist and next actions [50:00]

Those are our five checks. Ownership, access, recovery, customer journeys, and continuity. The checklist helps you record where you stand with each one. And remember to give it a label. Confirmed means that you've checked the details and have something to support the answer. Need to check means that there's an assumption or an unanswered question. Needs action means you've found a gap that we need to do.

Now, you don't need to do all that stuff just now, but just highlighting the fact that that needs to be investigated or you need more evidence is a good step rather than unknown. So don't worry if you have quite a few entries in the middle category, need to check or need action. Turning an assumption into a specific question is a useful process.

This isn't a points-based test. Several tidy accounts don't cancel out one serious problem with recovery or access. But if something doesn't apply to your website, that's okay, but record it and see why it doesn't so the next person then doesn't have that issue. So as you look back over the five areas, pick the one that you most need to follow up and keep that in mind for your next step.

Choose three practical actions [51:12]

So choose three actions to take away from today. One is start with the gaps that could have the biggest consequence for your website. So that could be you don't know where the backups are and you're scared that your website goes down because it's critical. If you can't recover, for example, a key account, don't know whether your backups work or have a broken sales journey, those deserve your first attention.

Your actions might be confirm the domain name and account and renewal contact, ask a provider, your IT provider or your host for evidence of a restoration test and send a clearly labelled enquiry through the website to make sure your contact forms work. Number two might be to make each action specific or SMART, SMART, specific, measurable, achievable, relevant, and time bound. Give it an owner and a date.

So things like look at website security is kind of difficult to finish, but a task, maybe ask a provider to confirm who has administrator access by Friday is much, much clearer and

actionable. If you're attending this webinar as a member of staff, your action might just be to take these questions to the relevant person that's responsible, a manager or somebody else in another department.

You don't have to personally fix every issue that you identify, but identifying them is the key thing here. And then number three is review your progress. Then make the broader check a quarterly or a six-monthly or even a yearly habit. So revisit significant changes to staff, suppliers, the website. And if the answers conflict or work needs expertise that you don't have, that's a sensible point to bring in somebody else who knows this stuff.

So don't have to rely on just yourself. Go to the relevant department, relevant people, relevant providers. They're the experts. Ask them for that information, that help.

The downloadable checklist [53:10]

Okay, that's what we have today. I have a checklist for you. So I've got a little document, it's a few pages long and it covers different scenarios. It's an easy checklist and question a list or somewhere to store information. I will send this via email as well afterwards later on today. There's a QR code on screen and the URL is in the comments.

Use it with your team, your website provider to record details, identify what needs checking and agree the next actions. You don't have to complete it all in one sitting. Don't get scared if the big long document is quite a few pages, but don't get scared that just start at page one or start with the areas that matter most in your business and how it uses the website.

If you'd like help making sense of what you find, I do also offer a website audit and strategy sessions through my website Zero Point Development if you have got stuck somewhere. That gives us a way to look more closely at your setup, understand the business priorities, work out what needs attention next. The checklist, though, is a useful place to start either way.

You can take these questions straight to the people who already support your website. As I say, you can download that resource at the moment, and I'll send that via email afterwards.

Questions and closing remarks [54:37]

If you've got any questions, please drop them in the comments. If you've got follow-up questions, or don't want to put sensitive information in the comments, feel free to contact me.

If anything from this webinar has worried or stressed you, if there's something you don't understand or you've got a big problem, please reach out. I'm happy to point you in the right direction and get you up and running on this topic.

We covered a lot today. We ran through those five checks. Hopefully it's given you some ideas. Maybe you've thought about gaps in what you understand about your website or how it works. Maybe you're now wondering whether your contact form is sending information. Perhaps it's time to schedule a test and make sure it submits, sends information, and somebody in the business receives it and can act on it.

If you've got any WordPress questions as well, I'm a WordPress expert, so you're welcome to jot them down.

Thank you to everyone for attending. I'll put the recording on YouTube and send you a link. The slides will also be available, and I'll send a link to everyone on the webinar. I'm glad you've got a couple of things to take away and check on. That was the main point of today.

There are no more questions, so thank you for your time this morning and for being part of NSW Small Business Month. I hope to see you at the next webinar: 'What Happens If Your Website Person Disappears?' Thank you, everyone. See you again.