



What is the FSRA?

The Financial Services Reform Act (FSRA) was introduced to bring all financial services and products under one regulatory regime. It also aimed to increase the level of compliance and competency in the financial services industry. Two components of FSRA are licensing and training. Every person who gives advice about a financial product (e.g.) superannuation, insurance, derivatives or shares etc. must either hold an Australian Financial Services License (the licensee) or be authorized by a licensee to give advice on their behalf (referred to as an authorized representative).

Evaluate your situation

"But I only do our client's accounts?"

Are you sure that you only look after the accounts for your client? What would you say to Mr and Mrs Smith if in their accounts you saw that: their property was underinsured by 1/2 million? There was a potential year-end profit of \$300,000 and that the value of their share portfolio had doubled?

If you answered: "I'd tell them to increase their insurance by 1/2 million, think about putting \$100,000 into superannuation and the remaining \$200,000 into a negatively-geared investment property, or to sell some of their share portfolio" ... then you are giving financial product advice and fall under the FSRA rules!

What does the FSRA have to do with technology?

Policy statements and Guides are available from ASIC http://www.asic.gov.au/asic/asic_polprac.nsf/byheadline/Policy+fsr+?openDocument

These statements and guidelines cover a range of responsibilities including: Financial requirements, Advisers – conduct and disclosure, Training, Organisational capacities and other areas.

Organisational capacities includes "Technological resources" which encompasses IT systems and services.



FSRA technology requirements

ASIC have released a Small Business Guide to complying with PS 164 (Policy Statement 164)

[http://www.asic.gov.au/asic/pdflib.nsf/LookupByFileName/small_bus_compliance_guide.pdf/\\$file/small_bus_compliance_guide.pdf](http://www.asic.gov.au/asic/pdflib.nsf/LookupByFileName/small_bus_compliance_guide.pdf/$file/small_bus_compliance_guide.pdf)

Section 15 of this guide provides a useful checklist to evaluate whether your IT systems are adequate to meet the needs of your business on an on-going basis.

The checklist is relevant for **any business**, not just those that provide financial services.

Section 15 concentrates on data backup, data recovery and disaster recovery plans.

Off-site Backup Server

One of the solutions that ZEN provides is an Off-site Backup Server, this option addresses a key part of the 'Disaster Recovery' requirements of the ASIC checklist.

What would you do in the event of a 'disaster' at your office (say a fire) that resulted in the destruction of your server? How would you quickly get your business systems online with all your critical operational data intact? What would you do if all your staff were unable to work for days while your systems were restored? The cost in terms of lost productivity - or worse lost reputation - could be substantial.

The purpose of the Off-site Backup Server is to ensure that all critical office data (including e-mail) is synchronised to a dedicated server that is physically located at our premises (i.e. "off-site" away from your office).

For the technically minded

An encrypted link – a Virtual Private Network (or VPN) - is established between the office server ("primary") and the standby server ("off-site"). The purpose of VPN is to allow the Internet to be used as a medium for securely exchanging data between the two servers. The VPN is a cost-effective alternative to using a private, dedicated leased line for a private network.

Business critical data on the two servers is then synchronised at scheduled intervals through-out each day via scripts that are customised to meet the individual requirements of each client.

In the event of a 'disaster', the "standby server" is immediately available so that you can continue to work via remote access. Or the "standby server" can be delivered to your office (or some other location) to allow your business operations to continue normally.



Implementation

The following figures are provided as a guide, based on a recent implementation. Once your individual requirements and environment are understood, a final quotation can be provided prior to commencement.

		\$ Ex
Firewall		650
VPN setup	1/2 day	500
Setup synchronisation scripts & test	1/2 day	500
Dedicated Standby Server (Athlon 2200, 2 x 120GB disks "mirriored", 512MB memory)		1,250
Setup of backup server & initial data transfer	2 days	2,000
Implementation		\$4,900

On-going

Server hosting	\$20 per week
Data transfer - (2GB per month included)	\$20 per GB thereafter

Zero Effort Networking (ZEN) is experienced in accurately identifying computer network problems and acting swiftly to fix them. Since 1996 we have helped clients implement stable, reliable computer networks that take the worry out of network management. For further information you are welcome to contact us.

Zero Effort Networking Pty Ltd
ABN: 38 082 434 446
Telephone: 02 9676 3541
Facsimile: 02 8569 2012
E-mail: info@zeroeffortnetworking.com.au
Web: www.zeroeffortnetworking.com.au
Office: Suite 15, 18 Third Avenue, Blacktown NSW 2148

No part of this publication may be reproduced without written permission of the authors. Copying and distribution by any means is strictly forbidden. Additional copies may be obtained for free by contacting Zero Effort Networking.