How do you know the ISMS is working?

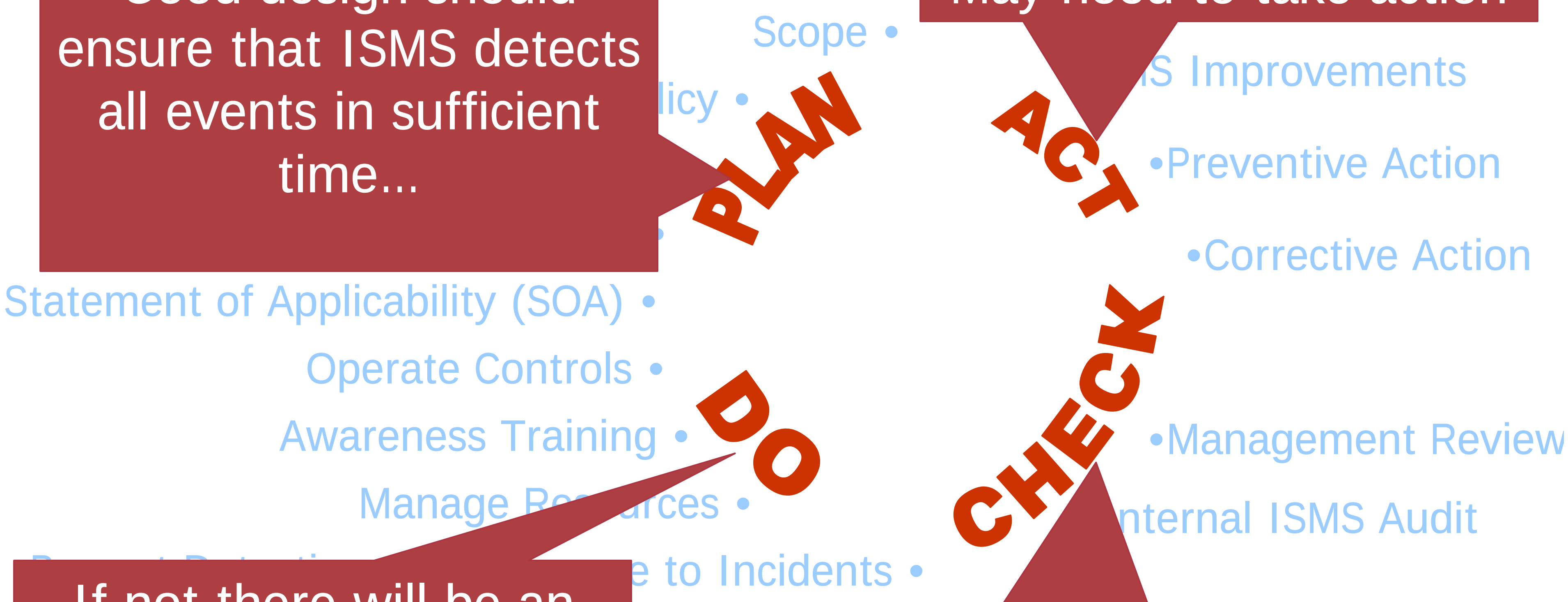
Dr. David Brewer,
www.gammassl.co.uk

7799 Goes Global

How do I know it is working?

Good design should ensure that ISMS detects all events in sufficient time...

May need to take action



Scope •

licy •

Statement of Applicability (SOA) •

Operate Controls •

Awareness Training •

Manage Re urces •

e to Incidents •

PLAN

DO

CHECK

ACT

S Improvements

•Preventive Action

•Corrective Action

•Management Review

nternal ISMS Audit

If not there will be an incident

Need other checks as well

The Plot

- Overture (time metrics, internal control and risk treatment plans)
- Incidents
- Check activities
- Is this all?
- Summary and conclusions

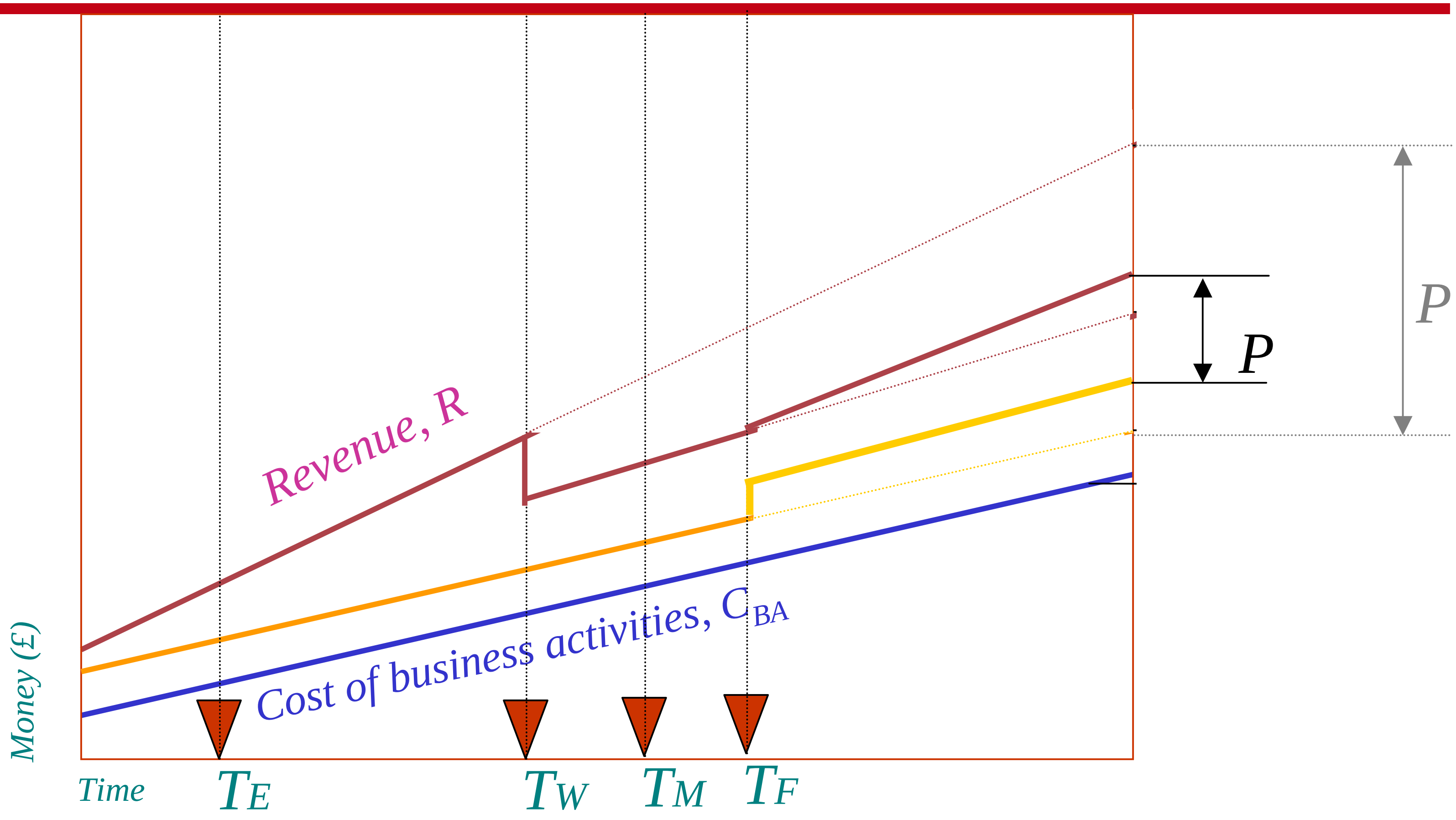
TIME METRICS

Time Metrics

"… detect the event in sufficient time to do something positive about it… "

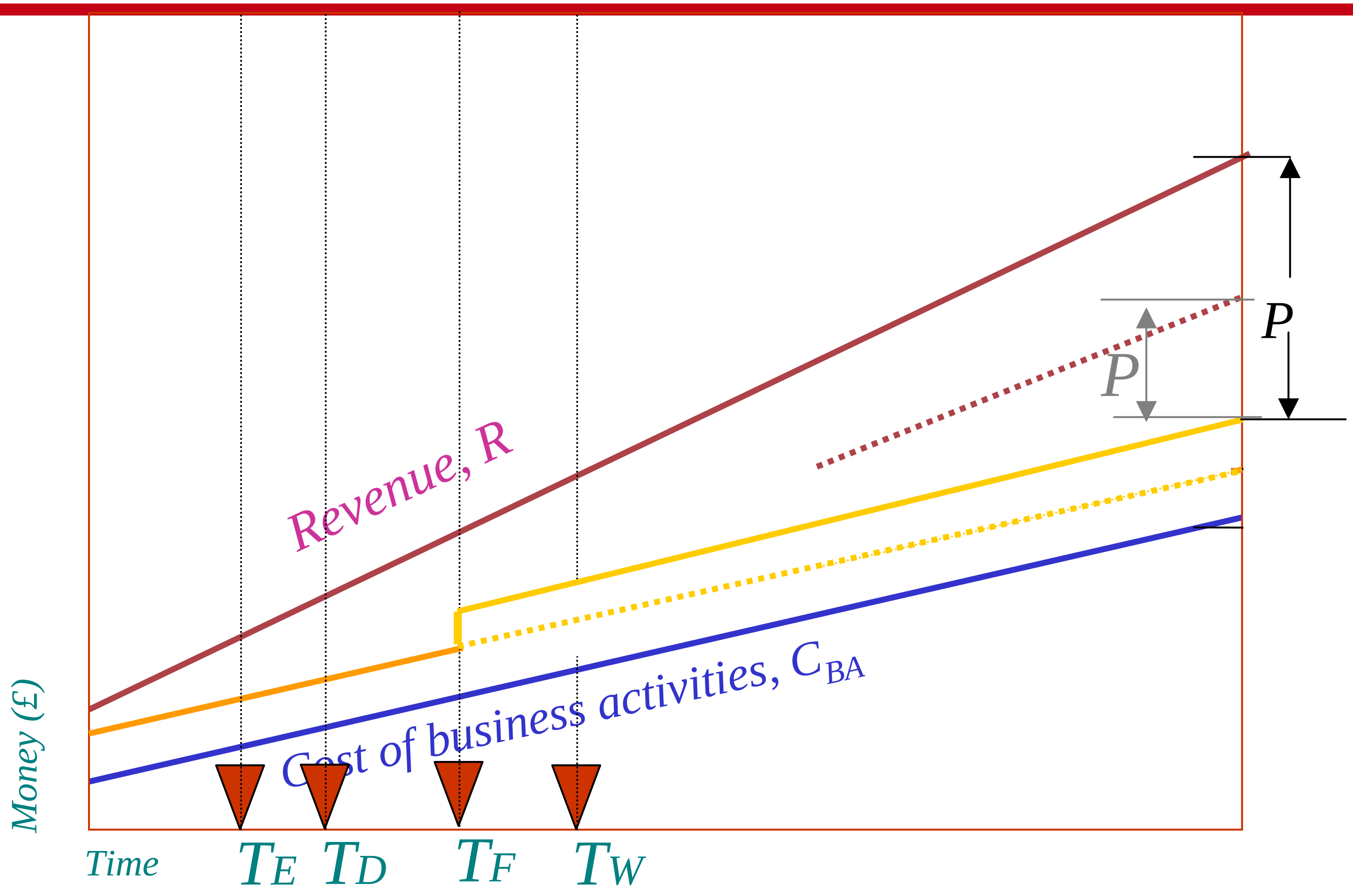
See http://www.gammassl.co.uk/topics/time/index.html

Time Metrics



7799 Goes Global

Time Metrics

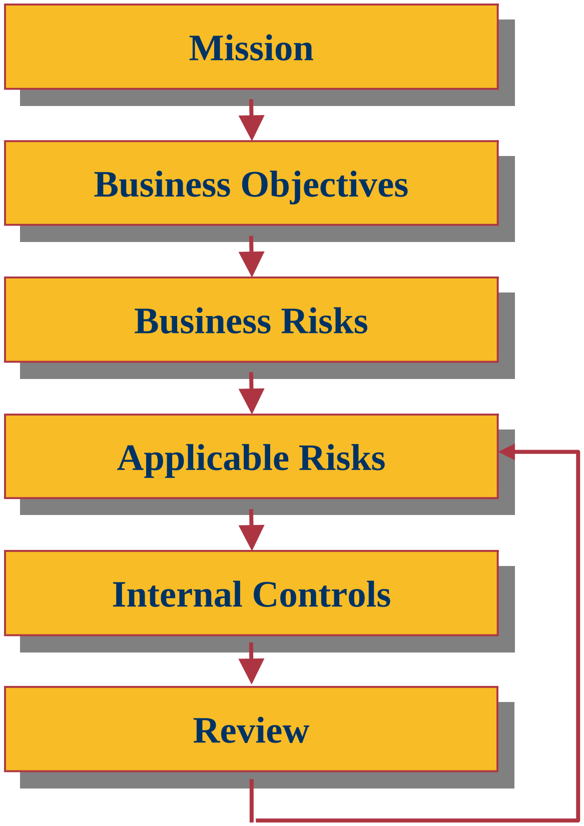


7799 Goes Global

INTERNAL CONTROL

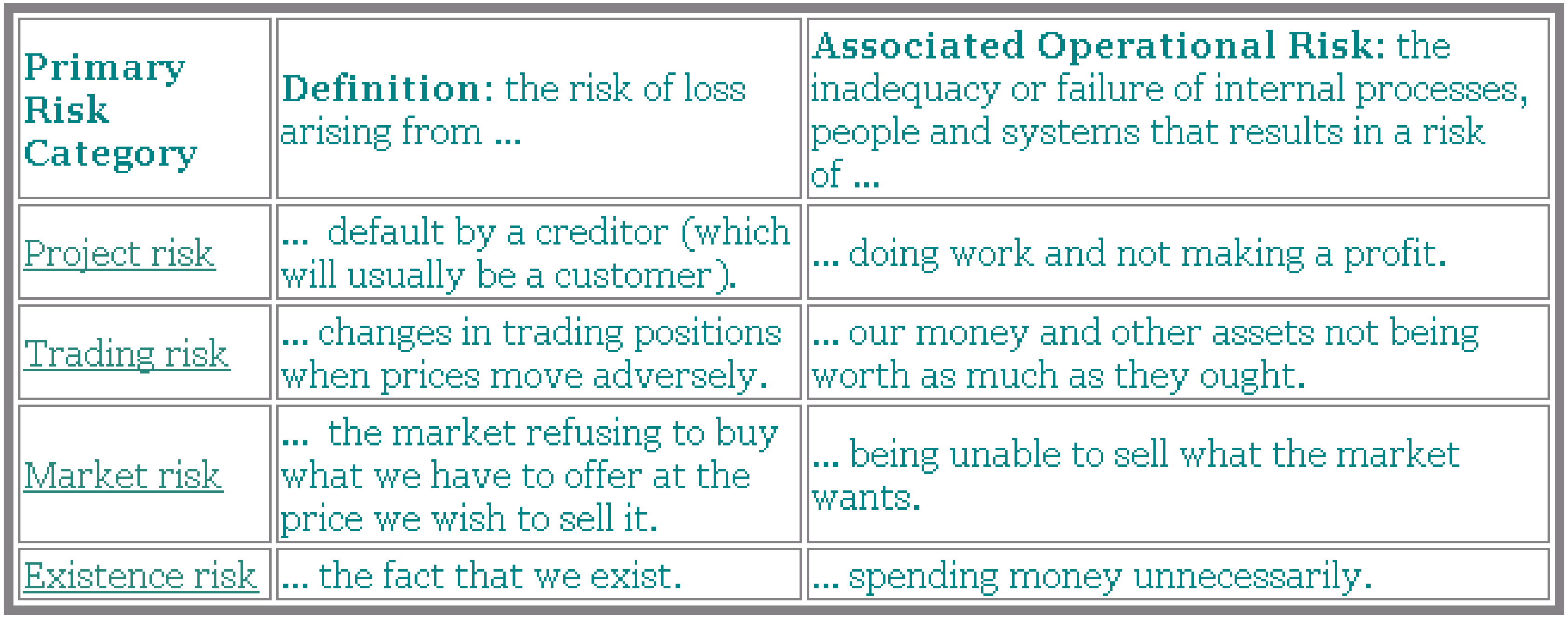
Internal Control

- Corporate Governance requirement
- Means to achieve objectives
  - *Operational procedures*
  - *Controls*
- Deming cycle (PDCA)
- Common to ISO 9001, BS7799-2 etc..



One Internal Control System

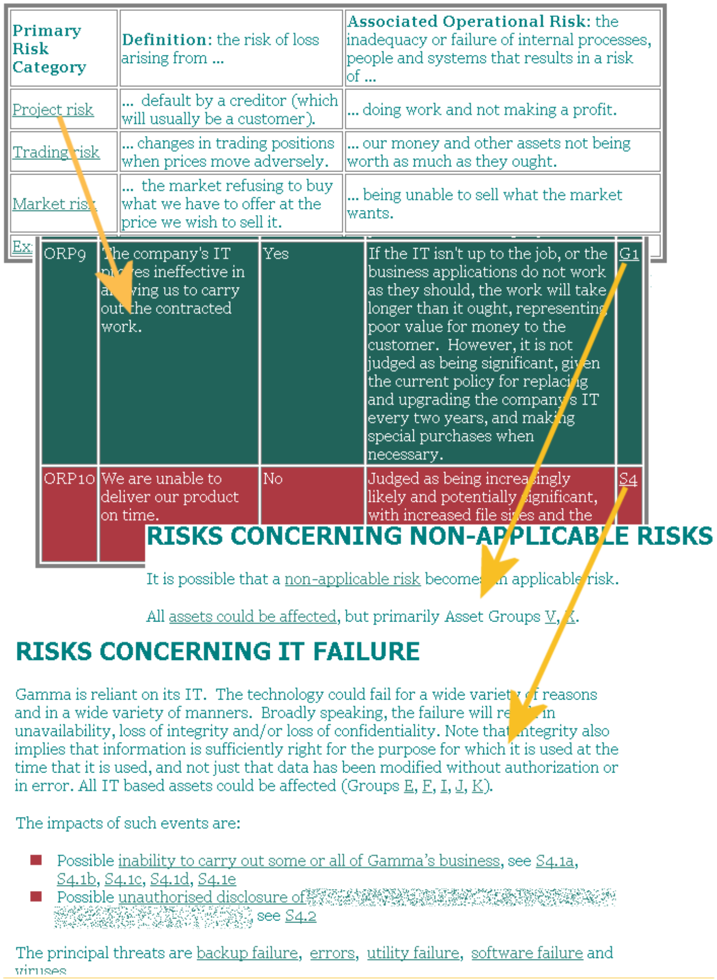
- All risks...



Primary Risk Category	**Definition:** the risk of loss arising from ...	**Associated Operational Risk:** the inadequacy or failure of internal processes, people and systems that results in a risk of ...
Project risk	... default by a creditor (which will usually be a customer).	... doing work and not making a profit.
Trading risk	... changes in trading positions when prices move adversely.	... our money and other assets not being worth as much as they ought.
Market risk	... the market refusing to buy what we have to offer at the price we wish to sell it.	... being unable to sell what the market wants.
Existence risk	... the fact that we exist.	... spending money unnecessarily.

An Example

- Gamma’s internal control system
- Finance, sales, marketing, R&D, projects, quality, information security



Primary Risk Category	**Definition:** the risk of loss arising from …	**Associated Operational Risk:** the inadequacy or failure of internal processes, people and systems that results in a risk of …
Project risk	… default by a creditor (which will usually be a customer).	… doing work and not making a profit.
Trading risk	… changes in trading positions when prices move adversely.	… our money and other assets not being worth as much as they ought.
Market risk	… the market refusing to buy what we have to offer at the price we wish to sell it.	… being unable to sell what the market wants.
Ex		

ORP9	The company's IT proves ineffective in allowing us to carry out the contracted work.	Yes	If the IT isn't up to the job, or the business applications do not work as they should, the work will take longer than it ought, representing poor value for money to the customer. However, it is not judged as being significant, given the current policy for replacing and upgrading the company's IT every two years, and making special purchases when necessary.	G1
ORP10	We are unable to deliver our product on time.	No	Judged as being increasingly likely and potentially significant, with increased file sizes and the	S4

RISKS CONCERNING NON-APPLICABLE RISKS

It is possible that a non-applicable risk becomes an applicable risk.

All assets could be affected, but primarily Asset Groups V, X.

RISKS CONCERNING IT FAILURE

Gamma is reliant on its IT. The technology could fail for a wide variety of reasons and in a wide variety of manners. Broadly speaking, the failure will result in unavailability, loss of integrity and/or loss of confidentiality. Note that integrity also implies that information is sufficiently right for the purpose for which it is used at the time that it is used, and not just that data has been modified without authorization or in error. All IT based assets could be affected (Groups E, F, I, J, K).

The impacts of such events are:

- Possible inability to carry out some or all of Gamma’s business, see S4.1a, S4.1b, S4.1c, S4.1d, S4.1e
- Possible unauthorised disclosure of [redacted], see S4.2

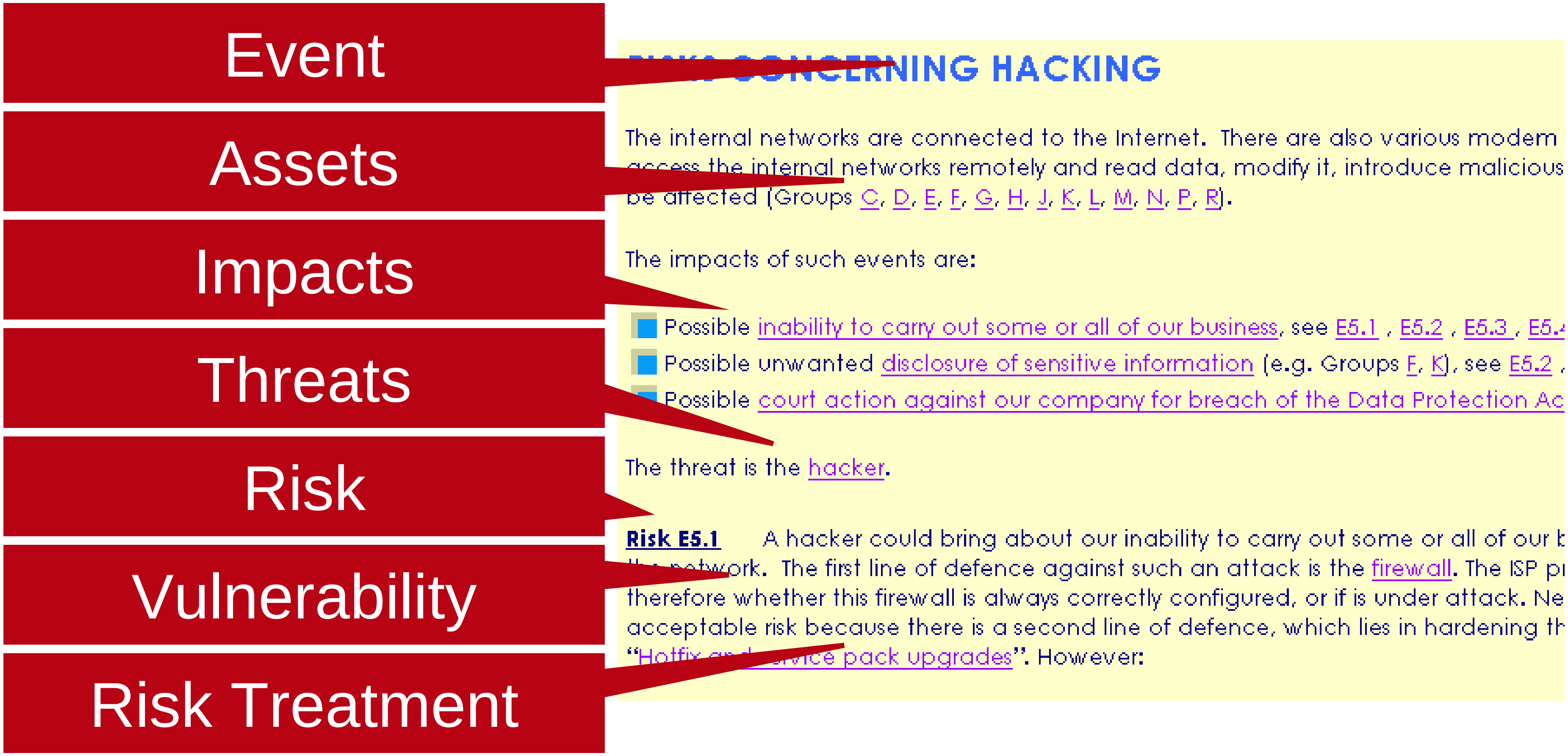
The principal threats are backup failure, errors, utility failure, software failure and viruses

7799 Goes Global

RISK TREATMENT PLANS

GAMMA

Risk Treatment Plans



Event

Assets

Impacts

Threats

Risk

Vulnerability

Risk Treatment

RISKS CONCERNING HACKING

The internal networks are connected to the Internet. There are also various modem
access the internal networks remotely and read data, modify it, introduce malicious
be affected (Groups C, D, E, F, G, H, J, K, L, M, N, P, R).

The impacts of such events are:

- Possible inability to carry out some or all of our business, see E5.1 , E5.2 , E5.3 , E5.
- Possible unwanted disclosure of sensitive information (e.g. Groups F, K), see E5.2 ,
- Possible court action against our company for breach of the Data Protection Ac

The threat is the hacker.

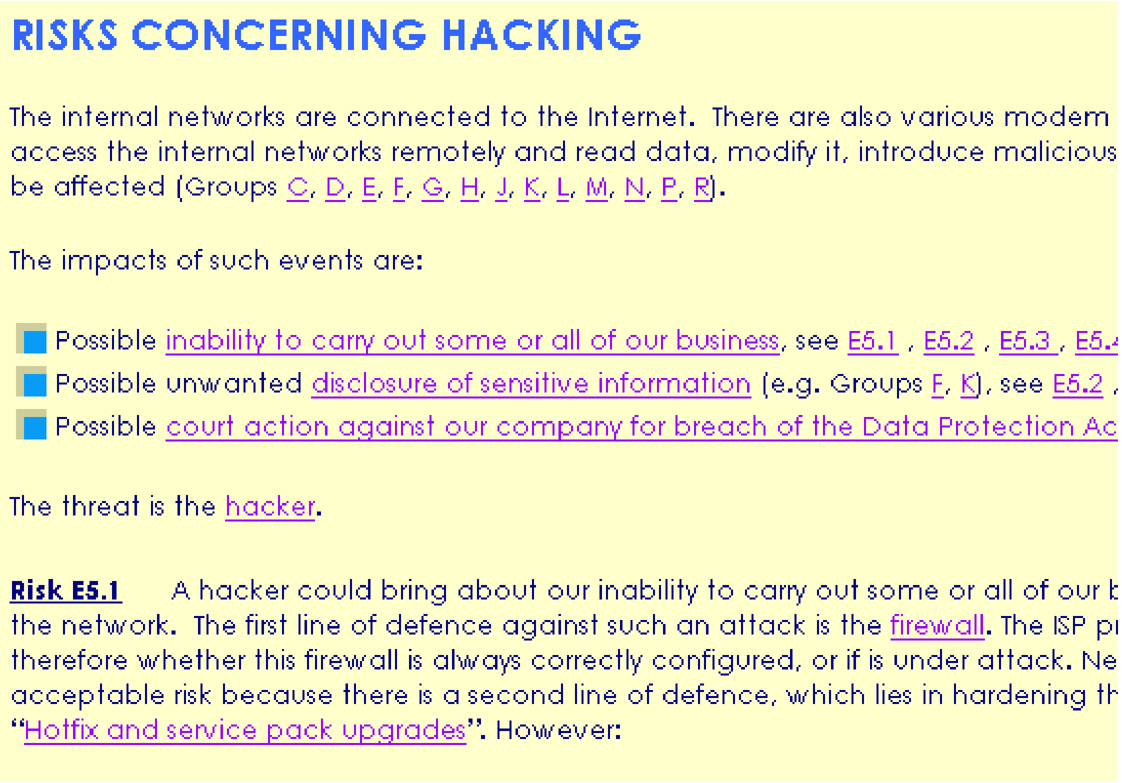
Risk E5.1 A hacker could bring about our inability to carry out some or all of our b
the network. The first line of defence against such an attack is the firewall. The ISP pr
therefore whether this firewall is always correctly configured, or if is under attack. Ne
acceptable risk because there is a second line of defence, which lies in hardening th
"Hotfix and service pack upgrades". However:

7799 Goes Global

GAMMA

Risk Treatment Plans

- Tell it like a story
- Methodology
  - *Good plot*
  - *Happy ending*
- Uses time metrics
- Ask “what if it doesn’t work?”



RISKS CONCERNING HACKING

The internal networks are connected to the Internet. There are also various modem access the internal networks remotely and read data, modify it, introduce malicious be affected (Groups C, D, E, F, G, H, J, K, L, M, N, P, R).

The impacts of such events are:

- Possible inability to carry out some or all of our business, see E5.1 , E5.2 , E5.3 , E5.
- Possible unwanted disclosure of sensitive information (e.g. Groups F, K), see E5.2 ,
- Possible court action against our company for breach of the Data Protection Ac

The threat is the hacker.

Risk E5.1 A hacker could bring about our inability to carry out some or all of our b the network. The first line of defence against such an attack is the firewall. The ISP p therefore whether this firewall is always correctly configured, or if is under attack. Ne acceptable risk because there is a second line of defence, which lies in hardening th “Hotfix and service pack upgrades”. However:

- Encourages well formed controls (i.e., self-policing)

7799 Goes Global

INCIDENTS

Incidents?

■ Safe found unlocked	✓ *possible unauthorised disclosure*
■ Blue death	✗ *usually no impact*
■ Hard disc crash	✗ *ditto*
■ Adware virus	✓ *possible unauthorised disclosure*
■ Fox hunting protestors	✓ *adverse press coverage*

Definition of an Incident

“… an occurrence of an impact… “

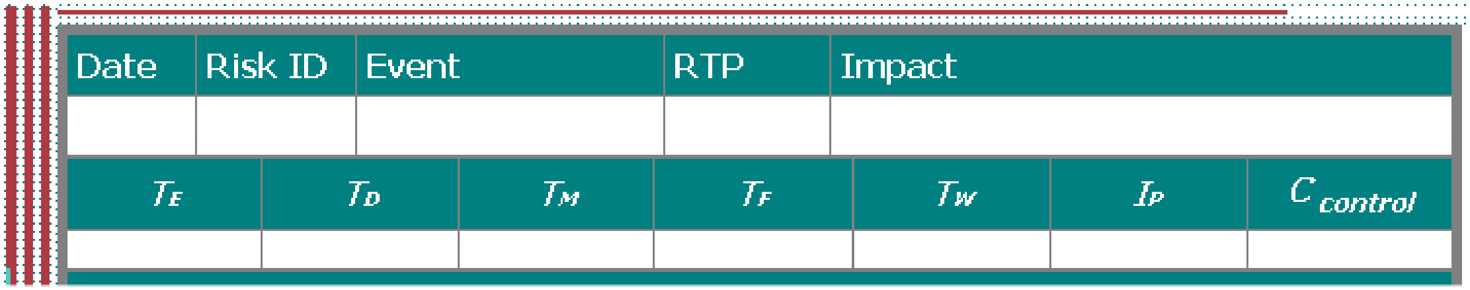
Impacts

- Adverse press coverage
- Court action against company
- Court action against director
- Inability to carry out some or all of company's business
- Loss of key staff
- Loss of customer confidence
- Loss of revenue
- Loss of the monetary value of property and contents
- The company goes to the wall
- Unanticipated costs
- Unauthorised disclosure

YOU CHOOSE

Incident Analysis

- Was it an applicable or non-applicable risk?
- Discover whether controls operated within their design parameters
- Corrective, preventive action or improvements?



Date	Risk ID	Event	RTP	Impact

T_E	T_D	T_M	T_F	T_W	I_P	$C_{control}$

Extract from Gamma incident analysis proforma

7799 Goes Global

Is this good enough?

- No
  - *There could be no incidents because there are no events*
- Two strategies
  - ~~*Monitor events*~~
  - *Monitor controls* ✓
- But if there are no events, monitoring won't tell if controls are working
- Might not know what the event is
- Could be billions of them – duplication of control?

CHECK ACTIVITIES

Check Activities

- See Appendix B to BS 7799-2:2002
  - *Internal MS audits*
  - *Management system reviews*
  - *Routine checks*
  - *Self policing procedures*
  - *Lessons learnt from others*
  - *Trend analysis*
  - *Intrusion detection*
  - *External audits (financial, quality, security…)*

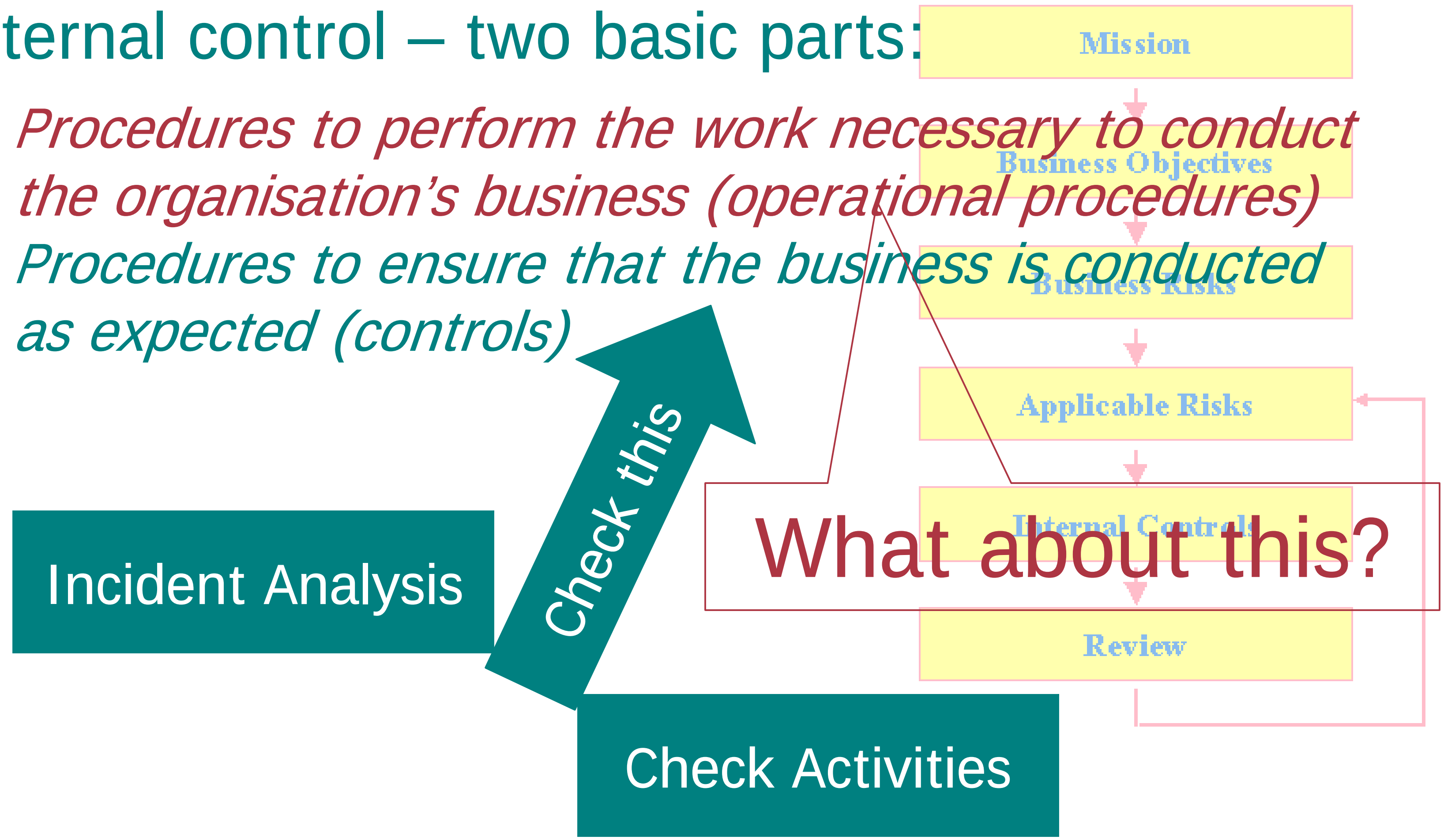
Routine Checks

- Daily
  - *Office still locked …*
  - *AV controls running …*
- Month end
  - *Billing information, reconciliations …*
  - *Status of projects …*
- Periodic
  - *Technical compliance with policy …*
  - *AV, IDS log inspections …*
  - *Back-ups taken and recovery is possible*
- Ask: are they working within their design parameters

IS THERE ANYTHING ELSE?

Possibly

- Internal control – two basic parts:
  - *Procedures to perform the work necessary to conduct the organisation's business (operational procedures)*
  - *Procedures to ensure that the business is conducted as expected (controls)*



Incident Analysis

Check this

Check Activities

What about this?

Dealing with Business Objectives

- Could use performance metrics
- But if we have an objective there will always be a risk of not meeting it:
  - *May be applicable or non-applicable*
  - *Ought to feature in an RTP*
    - *E.g. Are sales on target?*
    - *Has customer paid*
- Routine checks (our month end checks) are an example
- Use as a cross-check
  - *Might show omissions in RTP*

SUMMARY & CONCLUSIONS

Summary

- Detect the event in sufficient time to do something positive about it

- Tell it like a story RTP approach encourages well formed controls
  - *And everyone understands*
  - *Focus is on business issues as well as technology*

- Incident = occurrence of impact

- Incident analysis + check activities + time metrics = sound internal control

- Monitor performance against objectives as a cross check

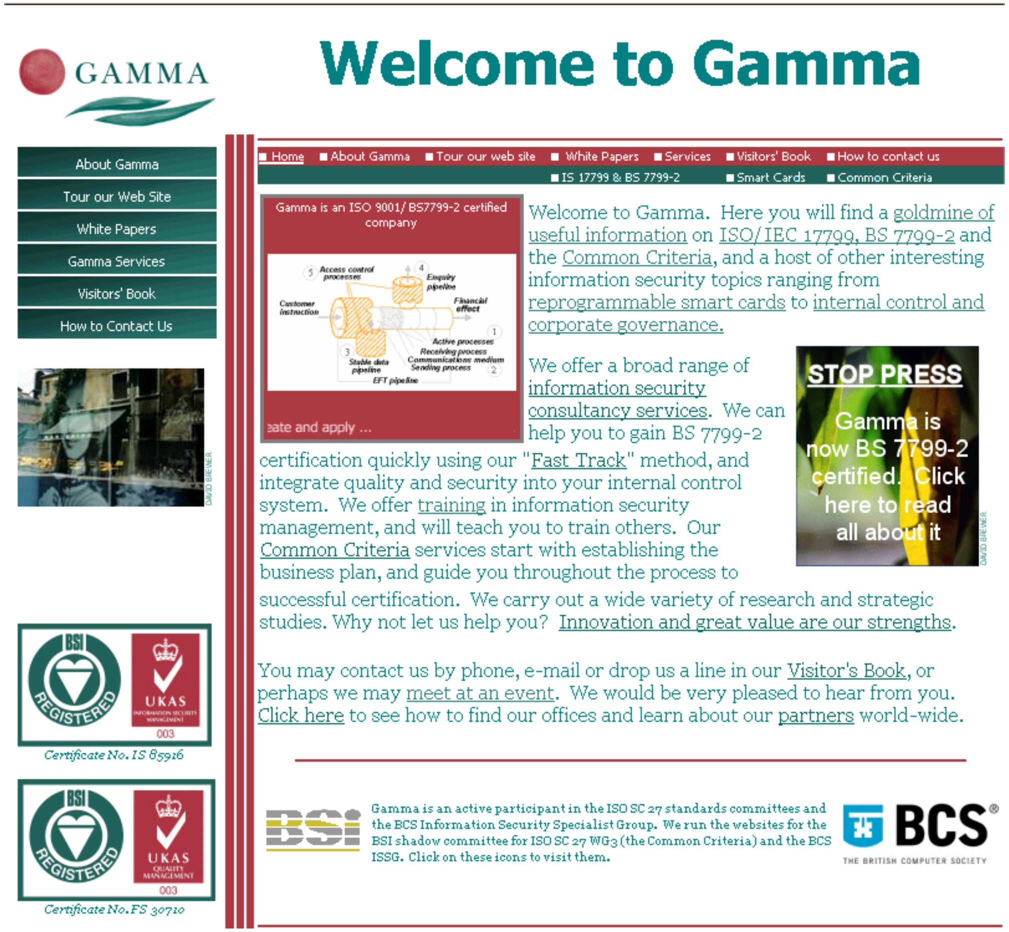
Conclusions

- This works
- Addresses the whole ICS, not just information security
- Meets all requirements of BS 7799-2:2002
- But principles also apply to the whole ICS
- Information assurance is not just security as traditionally understood

GAMMA

For Further Information

- www.gammassl.co.uk
- Time paper
- Fast track ISMS certification paper
- Certification experiences
- BS 7799-2, Common Criteria
- Conference papers
- This one “How do you know the ISMS is working?”



GAMMA

Welcome to Gamma

About Gamma
Tour our Web Site
White Papers
Gamma Services
Visitors' Book
How to Contact Us

■ Home ■ About Gamma ■ Tour our web site ■ White Papers ■ Services ■ Visitors' Book ■ How to contact us
■ IS 17799 & BS 7799-2 ■ Smart Cards ■ Common Criteria

Gamma is an ISO 9001/ BS7799-2 certified company

eate and apply ...

Welcome to Gamma. Here you will find a goldmine of useful information on ISO/IEC 17799, BS 7799-2 and the Common Criteria, and a host of other interesting information security topics ranging from reprogrammable smart cards to internal control and corporate governance.

We offer a broad range of information security consultancy services. We can help you to gain BS 7799-2 certification quickly using our "Fast Track" method, and integrate quality and security into your internal control system. We offer training in information security management, and will teach you to train others. Our Common Criteria services start with establishing the business plan, and guide you throughout the process to successful certification. We carry out a wide variety of research and strategic studies. Why not let us help you? Innovation and great value are our strengths.

STOP PRESS

Gamma is now BS 7799-2 certified. Click here to read all about it

You may contact us by phone, e-mail or drop us a line in our Visitor's Book, or perhaps we may meet at an event. We would be very pleased to hear from you. Click here to see how to find our offices and learn about our partners world-wide.

REGISTERED BSI UKAS INFORMATION SECURITY MANAGEMENT 003
Certificate No. IS 85916

REGISTERED BSI UKAS QUALITY MANAGEMENT 003
Certificate No. FS 30710

BSI

Gamma is an active participant in the ISO SC 27 standards committees and the BCS Information Security Specialist Group. We run the websites for the BSI shadow committee for ISO SC 27 WG3 (the Common Criteria) and the BCS ISSG. Click on these icons to visit them.

BCS® THE BRITISH COMPUTER SOCIETY

GAMMA

How do you know the ISMS is working?

Dr. David Brewer, www.gammassl.co.uk

7799 Goes Global