About RGP

• 4,000+ professionals
• Consultants with relevant experience of 8-15 years and above
• Worked with 86 of the Fortune 100
• Annually serve over 2,400 clients
• Helping locally and globally across more than 70 offices
• Delivered projects in over 48 countries
• 100% retention of top 50 clients
• Nasdaq: RECN
Ian Burnett
VP, Internal Audit and Compliance

Role and Experience
Ian is an experienced executive in the delivery of governance, risk and compliance services. Ian has more than 25 years of hands-on, practical experience - he is responsible for developing RGP’s capabilities to assist clients in properly identifying and managing their enterprise risks through delivery of robust internal audit capabilities for both regulatory compliance and operational efficiency and effectiveness. Ian has been involved with Sarbanes-Oxley Internal Control over Financial Reporting advisory services since inception of the Act in 2002.

Prior to RGP, Ian served as a director in RSM’s risk consulting practice. Ian also previously worked for Deloitte and KPMG’s risk advisory practice areas and has held leadership roles in corporate audit departments in industry. Ian has broad industry experience with primary focus on financial services and consumer and industrial products.

Ian serves on The Institute of Internal Auditors Atlanta chapter Board of Governors and serves as an ISACA Atlanta chapter Board member.

Education
• MBA, International Finance, Georgia State University
• BS, Mathematics, Vanderbilt University

Certifications
• CIA, CISA, CRMA, Cybersecurity Audit Certificate

Industry Experience
• Financial Services
• Consumer Products
• Industrial Products
• Broadcast Media
• Technology
• Pharmaceuticals
• Public Sector

Expertise
• Internal controls / SOX 404
• Business process and IT audit
• Risk assessment and ERM
• Quality Assessment Reviews

• Team leadership and project management
• Data mining and analytics
• Regulatory compliance, BSA/AML
• Third-party risk / contract compliance
Brian K. Gray
Sr. Cybersecurity Consultant

**Role and Experience**
Brian is an experienced consultant, leader, creator and collaborator with deep expertise within technology and all areas of information & cyber security. With a career spanning more than 25 years he brings a breadth and depth of schema and skillsets to a team. He loves helping teams solve challenging problems.

His experience ranges from roles at the 10-mile doer to 100,000 mile visionary levels. He has experience in education and companies within the financial, insurance, distribution, transportation, health and many within software development which includes a major Linux distribution. With his teaching and technology background he can help teams connect the dots between technologies, best practices and governing bodies to ensure projects are successful and RGP meets your expectations.

**Expertise**
- Consulting, Leadership and Collaboration
- Governance, Risk, Compliance, Fraud & Audit
- Data Privacy & Security: GDPR, CCPA, GLBA & HIPAA
- Security Technologies - IPS, IR, Firewall, DLP, Forensics, Vulnerabilities, PenTesting, Endpoint etc.
- Process, Workflow, Business Analytics & Automation
- Internal Controls, Assessment and mapping to standards and regulations.
- Training and Education

**Education**
- BS, Technology Education, North Carolina State University

**Certifications**
- Multiple industry certifications and training:
  - CSM, CISSP, CISA, CISM, CEH, CCSA, CCSE, CCNA, CCSP, RHCE, CNA, CNE, CNP, CLS, CLP & MCP

**Industry Experience**
- Financial & Insurance
- Information Technology
- Software Development
- Product Distribution
- Transportation
- Healthcare
**SWIFT Background**

1. **What does SWIFT stand for?**
   Society for Worldwide Interbank Financial Telecommunications

2. **When was it created?**
   SWIFT is a consortium that dates back to the 1970’s.

3. **Who are they?**
   Based in Belgium and overseen by the National Bank of Belgium and a committee composed of representatives from major banks throughout the world.

4. **What do they do?**
   SWIFT is a global member-owned cooperative and the world’s leading provider of secure financial messaging services.
Who uses Swift?

Traditionally

SCORE Membership
Standardized Corporate Environment

Corporations
- Access the SWIFT Network
- Access is to Financial organizations not corporation to corporation.

Governments
- Monitor activities for malicious intent.
SWIFT Technology Overview

**SWIFT – Network**
- Trusted and closed computer network providing global communication channels for customers to send inbound and outbound messages and files.

**SWIFT - Messaging**
- 25 + Million Messages a day
- 11,000 + users

**SWIFT - FIN**
- Application Used for inbound/outbound messaging

**Example Message Types**
- MT101 – Request for Transfer of Funds
- MT102 – multiple customer credit Transfer

**Example File Types**
- BAI2, EDI, ISO 20022, XML & NACHA

**SWIFT - FileACT**
- Application for file gets and pushes
SWIFT Message Types:
MT101 – Request for Transfer
MT102 – Multiple Customer Credit Transfer
MT202 – General Financial Institution Transfer
MT940 – Previous Day Statement Report
SWIFT - Back Office Integration

Business Integrations
SWIFT offers tools to help with back office integrations

SWIFT Integration Packages
- Suite of tools and adapters which allow for linking of back-office applications to SWIFT.
  - Alliance Access Integration Platform (IPLA)
  - SWIFT Integration Layer (SIL)

Examples of ERP Integrations
- SAP
- Oracle
- SAGE

Examples of HR Integrations
- PeopleSoft
- Workday

SWIFTNet Link
- Single-Window access to SWIFT
- Mandatory software for interoperability ensuring integrity, authentication and confidentiality.

SWIFT Alliance Gateway
- Application to Application Connectivity to the SWIFT IP Network.
- Consolidates data flows to/from SWIFT Network
Why did SWIFT create the Customer Security Program (CSP)?

Multiple Cyber Attacks in 2016

Most notable was the Bangladesh Bank
• Malware infection.
• Leads to $81 million dollars lost from accounts.

SWIFT Reaction
• Chairman Yawar Shah Stated:
  • “The growing cyber threat requires a concerted, community-wide response.”

SWIFT CSP is created
• The goal is to help members secure the systems they use to connect to the SWIFT network.

2017
Self-Attestation of your level of Compliance by December 31st

2018
Self-Attestation of Compliance by December 31st

2019
Self-Attestation of Compliance by December 31st (added controls)

2020
CSCF v2020
Mandatory compliance.

Requirements for Compliance
• Internal or External Assessment
• Must be performed by December 31st
• Attestation valid until the end of 2021

SWIFT Community Activities
• Reserves the right to mandate an independent external assessment
• Policy and CSCF updates follow an annual update cycle
• User Guide section transferred to KYC-SA documentation

Self-Attestation of Compliance by December 31st

SWIFT CSCF v2017 to v2021 Requirement Changes

2017
- 27 Controls
- 16 Mandatory
- 11 Advisory

2018
- 27 Controls
- 16 Mandatory
- 11 Advisory

2019
- 29 Controls
- 19 Mandatory
- 10 Advisory

Promoted
- 2.6 Operator Session Flows
- 2.7 Vulnerability Scanning
- 5.4 Password Storage

New Advisory
- 1.3A Virtualization Platform
- 2.10 Application Hardening

2020
- 31 Controls
- 21 Mandatory
- 10 Advisory

Promoted
- 1.3 Virtualization Platform
- 2.10 Application Hardening

New Advisory
- 1.4A Restrict Internet Access
- 2.11A RMA Controls

Scope Extension
- 2.4A Back-Office Data Flow – MQ/Middleware Servers

2021
- 33 Controls
- 23 Mandatory
- 10 Advisory

Promoted
- 1.4A Restrict Internet Access
- 2.11A RMA Controls
- 2.4A Back-Office Data Flow – MQ/Middleware Servers

New Advisory
- TBD

Scope Extension
- TBD
SWIFT CSCF v2020 Controls

1.1 SWIFT Environment Protection
1.2 Operating System Privileged Account Control
1.3A Virtualization Platform Protection
1.4A Restrict Internet Access

2.1 Internal Data Flow Security
2.2 Security Updates
2.3 System Hardening
2.4A Back Office Data Flow Security
2.5A External Transmission Data Protection
2.6 Operator Session Confidentiality and Integrity
2.7 Vulnerability Scanning
2.8A Critical Activity Outsourcing
2.9A Transaction Business Controls
2.10A Application Hardening
2.11A RMA Business Controls

3.1 Physical Security

Restrict internet access
Reduce attack surface and vulnerabilities
Physically secure the environment
### SWIFT CSCF v2020 Controls (Cont.)

<table>
<thead>
<tr>
<th>Prevent compromise of credentials</th>
<th>Manage identities and segregate privileges</th>
<th>Detect anomalous activity to systems or transaction records</th>
<th>Plan for incident response and information sharing</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1 Password Policy</td>
<td>5.1 Logical Access Control</td>
<td>6.1 Malware Protection</td>
<td>7.1 Cyber Incident Response Planning</td>
</tr>
<tr>
<td>4.2 Multi-factor Authentication</td>
<td>5.2 Token Management</td>
<td>6.2 Software Integrity</td>
<td>7.2 Security Training and Awareness</td>
</tr>
<tr>
<td></td>
<td>5.3A Personnel Vetting Process</td>
<td>6.3 Database Integrity</td>
<td>7.3A Penetration Testing</td>
</tr>
<tr>
<td></td>
<td>5.4 Physical and Logical Password Storage</td>
<td>6.4 Logging and Monitoring</td>
<td>7.4A Scenario Risk Assessment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6.5A Intrusion Detection</td>
<td></td>
</tr>
</tbody>
</table>

**V2020 Mandatory**

**V2019 Promoted**

**V2020 Advisory**
What happens if not compliant?

SWIFT enforces compliance through the community by peer awareness and data for companies to make decisions of potential risk of counterparts. Banking related penalties can be enforced but not controlled by SWIFT.

Self-Attestations
If members are not CSCF compliant or don’t submit self-attestations their status is visible to the SWIFT community and any member can determine their status.

Transactions
If parties that do transactions are not compliant SWIFT will inform counterparties and their ability to transact business and facilitate payments will be limited.

The Standards MT Release 2020
Financial Action Task Force (FATF-16) Can impose penalties for breaches of sanctions rules may include unlimited fines for companies and could mean prison for some individuals.

Bank Penalties
Reserve Bank of India slapped penalties on 36 banks for non-compliance.
Client needed a 2019 assessment performed for attestation of CSCF requirements compliance.

**Scope of Work**

- Analyzed the 3rd party assessment performed in 2018.
- Designed tooling to execute CSCF v2019 compliance assessment.
- Reviewed companies documented policies, processes and business practices.
- Conducted stakeholder meetings with security and technology run teams.
- Assessed 19 mandatory, 10 advisory and 2 new for v2020.
- Identified any gaps within the CSCF requirements.
- Proposed potential remediation steps.
- Worked with teams to remediate the gaps.
- Reviewed evidence of gaps being remediated.
- Helped teams close out Service Now GRC issue tickets.
- Provided final documentation.

**Result**

- Client was able to remediate any gaps in compliance with CSCF v2019.
- Client picked up cybersecurity expertise along the journey.
- Client identified process issues that needed improvement.
- Direction provided resulted in client being able to remediate the issues.
- All issues were remediated and company could show compliance.
- Company was able to show to SWIFT Self-Attestation for 2019 compliance achieved.
SWIFT CSCF v2019 Assessment – What’s Involved

Companies using SWIFT must comply with new security requirements. Compliance typically involves an assessment approach such as the following:

1. Assess against CSCF controls
2. Identify the disposition of controls
3. Validate – Evidence or stress-testing
4. Gap Analysis & Recommendations
5. Remediation & Reporting
# SWIFT CSCF v2019 Assessment – Mapping CSF Controls

<table>
<thead>
<tr>
<th>Mandatory Security Controls</th>
<th>Control Objective</th>
<th>Relevant Industry Guidance &amp; Frameworks</th>
<th>Cybersecurity or Information Security Controls-Mappings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1. Restrict Internet Access and Segregate Critical Systems from General IT Environment</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1 SWIFT Environment Protection</td>
<td>Ensure the protection of the user’s local SWIFT infrastructure from potentially compromised elements of the general IT environment and external environment.</td>
<td>NIST CSF - Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.</td>
<td>PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.</td>
</tr>
<tr>
<td>1.2 Operating System Privileged Account Control</td>
<td>Restrict and control the allocation and usage of administrator-level operating system accounts.</td>
<td></td>
<td>NIST SP 800-53 Rev. 4 AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24</td>
</tr>
<tr>
<td><strong>2. Reduce Attack Surface and Vulnerabilities</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.1 Internal Data Flow Security</td>
<td>Ensure the confidentiality, integrity, and authenticity of data flows between local SWIFT-related applications and their link to the operator PC.</td>
<td>Data Security (PR.DS): Information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information.</td>
<td>PR.DS-2: Data-in-transit is protected</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NIST SP 800-53 Rev. 4 SC-8, SC-11, SC-12</td>
</tr>
</tbody>
</table>
SWIFT CSCF v2019 Assessment

Assess against CSCF Controls
Companies compliance posture against the 19 mandatory and 10 advisory controls.

Identify the Disposition of controls
- Satisfied
- Partially Satisfied
- Not Satisfied

Validate – Evidence or stress-testing
Compare information gathered to support the disposition of the design, implementation and effectiveness of the controls.

Assessment
- Stakeholder Meetings
- Documentation Review
- Site visits
- Operational review

Gap Analysis and Recommendations
Highlight disposition of controls and prioritized recommendations for bringing controls into compliance.

Remediation & Reporting
Provide assistance during remediation and determine if disposition of the controls change. Provide reports to show disposition status and final report for executive and SWIFT review.
### SWIFT CSCF v2019 Assessment – Controls Discussion

<table>
<thead>
<tr>
<th>Mandatory Security Controls</th>
<th>Control Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Restrict Internet Access and Segregate Critical Systems from General IT Environment</td>
<td></td>
</tr>
<tr>
<td>1.3A Virtualization Platform Protection*</td>
<td>Secure virtualization platform and virtual machines (VM’s) hosting SWIFT related components to the same level as physical systems.</td>
</tr>
<tr>
<td>2. Reduce Attack Surface and Vulnerabilities</td>
<td></td>
</tr>
<tr>
<td>2.2 Security Updates</td>
<td>Minimize the occurrence of known technical vulnerabilities within the local SWIFT infrastructure by ensuring vendor support, applying mandatory software updates, and applying timely security updates aligned to the assessed risk.</td>
</tr>
<tr>
<td>2.3 System Hardening</td>
<td>Reduce the cyber attack surface of SWIFT-related components by performing system hardening.</td>
</tr>
<tr>
<td>2.7 Vulnerability Scanning</td>
<td>Identify known vulnerabilities within the local SWIFT environment by implementing a regular vulnerability scanning process and act upon results.</td>
</tr>
<tr>
<td>2.10A Application Hardening*</td>
<td>Reduce the attack surface of SWIFT-related components by performing application hardening on the SWIFT-certified messaging and communication interfaces and related applications.</td>
</tr>
<tr>
<td>4. Prevent Compromise of Credentials</td>
<td></td>
</tr>
<tr>
<td>4.2 Multi-factor Authentication</td>
<td>Prevent that a compromise of a single authentication factor allows access into SWIFT systems, by implementing multi-factor authentication.</td>
</tr>
</tbody>
</table>
Thank You, Questions?
Useless Trivia – Name this planet and its average surface temperature (within 100 degrees F)

source: www.jpl.nasa.gov
Useless Trivia – Name this planet and its average surface temperature (within 100 degrees F)

Venus

864 F

source: www.jpl.nasa.gov

source: www.space.com
Useless Trivia – When was the first Valentine’s Day and who invented it?

Hope you have a
Happy Valentine’s Day!
Useless Trivia – When was the first Valentine’s Day and who invented it?

486 AD

The Romans