Human-E.S.C.A.P.E. Threat Model

A GRC Approach to Human-Centric Security Risk Management

> **Framework for identifying, assessing, and managing human-related cybersecurity risks through Governance, Risk, and Compliance principles**

Table of Contents

Overview

Human-E.S.C.A.P.E. is a governance, risk, and compliance (GRC) framework designed to help organizations identify and manage security risks related to human behavior. While companies spend millions on firewalls and antivirus software, **74% of data breaches involve the human element** (Verizon DBIR 2024).

This framework provides:

- ✅ Structured risk assessment for human vulnerabilities
- ✅ Policy and control recommendations
- ✅ Compliance mapping to ISO 27001, NIST CSF, SOC 2
- ✅ Practical implementation guidance for GRC professionals
- ✅ Business case and ROI analysis for stakeholders

Target Audience: GRC Analysts, Risk Managers, Compliance Officers, Security Awareness Professionals, and students pursuing cybersecurity/risk management careers

---

Why This Framework Matters

The Problem

Organizations invest heavily in technology but overlook the human attack surface:

Challenge	Impact
Phishing Success Rate	32% of employees click malicious links
Average Breach Cost	$4.88M per incident involving human error
Detection Time	287 days average to detect social engineering attacks
Organizations with Human Risk Programs	Only 23% have formal programs

Recent High-Profile Breaches

1. MGM Resorts (September 2023)

- **Method:** 10-minute phone call to help desk
- **Impact:** $110M loss, 9-day operational shutdown
- **Root Cause:** No identity verification protocol

2. Uber (September 2022)

- **Method:** MFA fatigue attack + fake IT impersonation
- **Impact:** $148M in fines, full network compromise
- **Root Cause:** Weak contractor security + no verification protocol

3. Twitter (July 2020)

- **Method:** Spear phishing targeting support staff
- **Impact:** 130 accounts compromised, $350M reputational damage
- **Root Cause:** No callback authentication for admin access

Common Thread: All attacks exploited human vulnerabilities, not technical weaknesses.

The E.S.C.A.P.E. Framework

Framework Components

ComponE.S.C.A.P.E. Framework — Understanding Social Engineering Manipulation

The E.S.C.A.P.E. Framework highlights six major factors attackers exploit in social engineering. It helps identify how emotions, context, and psychological biases are used to deceive individuals and organizations.

E - Emotional Manipulation

Definition: Exploiting emotions to bypass rational decision-making

Common Tactics:

- **Fear:** "Your account will be suspended immediately"
- **Urgency:** "Action required in 1 hour or lose access"
- **Greed:** "Claim your $500 bonus now"
- **Curiosity:** "See who viewed your profile"

Risk Assessment Criteria:

- Presence of emotional trigger words (Yes = +25 points)
- Urgent deadline specified (Yes = +30 points)
- Bypasses normal verification (Yes = +25 points)
- Authority figure invoked (Yes = +20 points)

Risk Score: 0-100 (100 = Critical)

S - Social Engineering Vectors

Definition: Methods used to manipulate humans into revealing information or taking actions

Attack Vector Statistics:

Vector	Prevalence	Success Rate	Avg Financial Impact

Phishing (email)	83%	32%	$1.8M
Vishing (voice call)	54%	28%	$2.1M
Smishing (SMS)	47%	21%	$890K
Pretexting (fake scenario)	38%	43%	$3.2M
Quid Pro Quo (favor exchange)	22%	19%	$1.1M

Control Requirements:

- Email authentication (SPF, DKIM, DMARC)
- Caller ID verification for sensitive requests
- SMS filtering and threat detection
- Employee training on pretext identification
- Out-of-band verification protocols

C - Cognitive Bias Exploitation

Definition: Leveraging mental shortcuts that lead to flawed decision-making

Top 5 Exploited Biases:

1. **Authority Bias** (68% success rate)
    - *Example:* "This is the CEO, I need this done now"
    - *Defense:* Challenge protocol for high-privilege requests
2. **Scarcity Bias** (3x effectiveness)
    - *Example:* "Limited time offer - only 5 spots left"
    - *Defense:* Verify urgency independently
3. **Social Proof** (54% effectiveness)
    - *Example:* "Your colleagues have already approved this"
    - *Defense:* Confirm with named colleagues directly
4. **Reciprocity** (71% compliance)
    - *Example:* Small favor → Major request acceptance
    - *Defense:* Separate personal relationships from security decisions
5. **Commitment & Consistency** (62% escalation)
    - *Example:* Small ask → Increasingly larger requests
    - *Defense:* Evaluate each request independently

A - Authority & Trust Abuse

Definition: Impersonating or leveraging trusted roles to gain compliance

CEO Fraud Attack Chain:

```
Step 1: Reconnaissance
  ↓ (LinkedIn, company website research)
Step 2: Email Spoofing
  ↓ (Create look-alike domain: ceo@company.com)
Step 3: Urgency Creation
  ↓ ("Wire transfer needed NOW")
Step 4: Authority Invocation
  ↓ ("I'm in a meeting, can't talk")
Step 5: Verification Bypass
  ↓ ("Don't call, just do it")
Step 6: Financial Loss
  ↓ (Average: $6.5M per incident)
```

Controls:

- Dual authorization for financial transactions >$10K
- Callback verification to known numbers
- Out-of-band confirmation (separate channel)
- Manager approval requirements
- Transaction velocity limits

P- Psychological Pressure Tactics

Definition: Time pressure and consequences to force quick decisions

Pressure Escalation Model:

Pressure Level	Language	Compliance Rate
Low	"When you have time..."	15%
Medium	"Please complete by end of day"	45%
High	"Required NOW or account locked"	78%

Red Flags:

- Artificial deadlines ("within 1 hour")

- Threat of negative consequences ("account suspension")
- Restricting consultation ("don't tell anyone")
- Bypassing normal channels ("off the record")

Defense Strategy:

- Establish "stop and verify" protocols
- No same-day execution for high-risk actions
- Required cooling-off periods
- Escalation paths for pressure situations

E - Environmental Context

Definition: Situational factors that increase vulnerability

Risk Multipliers:

Context	Risk Increase	Reason
Remote Work	+35%	Harder to verify physically
After-Hours Contact	+52%	Reduced vigilance, no colleagues nearby
New Employees (<90 days)	+127%	Unfamiliar with protocols
Quarter/Year-End	+43%	High stress, rushed decisions
During Layoffs/Crises	+67%	Emotional vulnerability, confusion

Controls:

- Heightened verification during high-risk periods
- Restrict sensitive operations to business hours
- Enhanced onboarding security training
- Buddy system for new employees
- Crisis communication protocols

Real-World Case Studies

Case Study 1: MGM Resorts Ransomware (September 2023)

Attack Overview:

- **Date:** September 10-14, 2023
- **Duration:** 10-minute phone call
- **Financial Impact:** $110M
- **Operational Impact:** 9-day shutdown, casino floors down

Attack Narrative:

Attacker: "Hi, this is John Smith from IT in Las Vegas. I'm locked out of my Okta account and have an urgent executive meeting. Can you reset my password?"

Help Desk: "Sure, let me verify... what's your employee ID?"

Attacker: "It's on my laptop which is locked. Can you look it up by my name? I'm really in a bind here."

Help Desk: "OK, I see you. I'll reset your password..."

[10 minutes later: Full domain admin access → Ransomware deployment]

E.S.C.A.P.E. Analysis:

Component	Score	Key Factor
E - Emotional	79/100	Empathy for "locked out" employee
S - Social Engineering	91/100	Professional impersonation
C - Cognitive Bias	76/100	Helpfulness bias overrode security
A - Authority	71/100	Claimed IT department affiliation
P - Pressure	84/100	"Urgent meeting" time constraint
E - Environmental	82/100	Help desk culture of quick resolution
OVERALL RISK	**80.5/100**	**HIGH-CRITICAL**

Human Control Failures:

1. ❌ No multi-factor identity verification
2. ❌ Password reset without manager approval
3. ❌ Admin privileges granted to compromised account
4. ❌ No anomaly detection for rapid privilege escalation

5. ❌ Weak help desk authentication protocols

Financial Breakdown:

- Operational loss: $50M (9 days downtime)
- Remediation: $35M (incident response, forensics)
- Ransom negotiation: $15M (not paid)
- Legal/Regulatory: $10M (investigations, fines)

Lessons Learned: ✅ Implement 3-factor identity verification for password resets ✅ Require manager approval for privileged account changes ✅ Callback verification to registered employee numbers ✅ Monitor for post-reset anomalous activity ✅ Help desk training on social engineering tactics

---

Case Study 2: Uber Data Breach (September 2022)

Attack Overview:

- **Date:** September 15, 2022
- **Method:** MFA fatigue + WhatsApp impersonation
- **Impact:** $148M in fines, full network compromise
- **Data Exposed:** Internal systems, source code, customer data

Attack Chain:

```
Stage 1: Initial Access
  └─ Purchased contractor credentials from dark web

Stage 2: MFA Fatigue Attack
  └─ Sent 50+ push notifications until contractor accepted

Stage 3: Fake IT Support
  └─ WhatsApp message: "Hi, this is Uber IT. We're getting
     alerts about your account. Please accept the MFA to help
     us investigate"

Stage 4: Network Access
  └─ Contractor clicked "Accept" → Full VPN access

Stage 5: Privilege Escalation
  └─ Found shared admin credentials in network shares

Stage 6: Full Compromise
```

└─ Access to AWS, internal tools, source code repositories

E.S.C.A.P.E. Scores:

- **E (Emotional):** 72/100 - Frustration from repeated notifications
- **S (Social Engineering):** 95/100 - Multi-channel impersonation
- **C (Cognitive):** 81/100 - Compliance to stop annoyance
- **A (Authority):** 89/100 - Convincing IT impersonation
- **P (Pressure):** 87/100 - Persistent notification fatigue
- **E (Environmental):** 68/100 - Contractor with less security culture

Overall Risk Score: 82/100 (CRITICAL)

Control Failures:

Stage	Human Failure	Prevention Control That Failed
Initial Access	Weak contractor password	Password policy enforcement
MFA Bypass	Accepted fatigue attack	MFA training & push limits
Trust Exploit	Believed fake IT via WhatsApp	Verification protocol
Escalation	Shared admin credentials found	Secret management

Mitigation Recommendations:

1. **MFA Controls:** Limit push notifications to 3 per hour
2. **Verification:** Out-of-band confirmation for IT requests
3. **Contractor Security:** Baseline security requirements in contracts
4. **Privileged Access:** PAM solution to eliminate shared credentials
5. **Monitoring:** Alert on repeated MFA denials

Case Study 3: Twitter Breach (July 2020)

Attack Overview:

- **Date:** July 15, 2020
- **Accounts Compromised:** 130 high-profile accounts (Obama, Biden, Musk, Gates)
- **Financial Loss:** $120K in Bitcoin scams
- **Reputational Damage:** $350M estimated

Attack Method:

- Spear phishing targeting Twitter support staff
- Vishing (phone-based social engineering)
- Credential harvesting via fake VPN portal

E.S.C.A.P.E. Breakdown:

```
┌──────────────────────────────────────────────────────────────┐
│ Component: Emotional Manipulation                            │
│ • Urgency: "Security incident needs immediate fix"           │
│ • Fear: "Account lockout imminent"                           │
│ RISK SCORE: 85/100                                           │
├──────────────────────────────────────────────────────────────┤
│ Component: Social Engineering                                │
│ • Vishing (phone) targeting support staff                    │
│ • Fake VPN portal for credential harvesting                  │
│ RISK SCORE: 92/100                                           │
├──────────────────────────────────────────────────────────────┤
│ Component: Cognitive Bias                                    │
│ • Authority bias (impersonated IT department)                │
│ • Time pressure (urgent security response)                   │
│ RISK SCORE: 78/100                                           │
├──────────────────────────────────────────────────────────────┤
│ Component: Authority Abuse                                   │
│ • Impersonated internal IT security team                     │
│ • Leveraged internal admin tools                             │
│ RISK SCORE: 88/100                                           │
├──────────────────────────────────────────────────────────────┤
│ Component: Psychological Pressure                            │
│ • "Fix this now or accounts will be locked"                  │
│ • Multiple employees targeted simultaneously                 │
│ RISK SCORE: 81/100                                           │
├──────────────────────────────────────────────────────────────┤
│ Component: Environmental Context                             │
│ • Remote work environment (COVID-19 pandemic)                │
│ • Distributed workforce = weak verification                  │
│ RISK SCORE: 75/100                                           │
└──────────────────────────────────────────────────────────────┘

OVERALL HUMAN RISK SCORE: 83/100 (CRITICAL)
```

Root Causes:

- Employees granted admin access without callback verification
- No secondary authentication for high-privilege requests

- Insufficient social engineering awareness training
- Over-reliance on IT department authority

Recommended Controls:

1. Mandatory verbal verification for admin access requests
2. Challenge protocol for unusual IT requests
3. Segregation of duties (no single person has full admin)
4. Regular social engineering simulation testing

GRC Integration

Governance Structure

Roles & Responsibilities:

Role	E.S.C.A.P.E. Responsibilities
Board	Approve human risk budget, review annual risk posture
CISO	Own E.S.C.A.P.E. framework implementation, report to board
GRC Manager	Conduct risk assessments, maintain risk register, audit controls
Compliance Officer	Map to regulations, manage policy updates, coordinate audits
HR	Partner on training, background checks, offboarding
Department Managers	Enforce policies, report incidents, support culture
Employees	Follow policies, report suspicious activity, complete training

---

Risk Management Integration

Risk Register Template

How to document E.S.C.A.P.E. risks in your existing risk register:

Field	Example Entry
Risk ID	HR-SE-001

Risk Category	Human Risk - Social Engineering
Description	Employees may be manipulated through phishing emails to reveal credentials or approve fraudulent transactions
E.S.C.A.P.E. Score	76/100 (High)
Likelihood	High (32% phishing success rate)
Impact	High ($1.8M average loss per incident)
Inherent Risk	Critical
Current Controls	• Email filtering • Annual security training • Incident reporting process
Control Effectiveness	Partially Effective (60%)
Residual Risk	High
Treatment Plan	• Implement quarterly phishing simulations • Add verification protocol for financial transactions • Deploy user behavior analytics
Risk Owner	Director of Information Security
Target Date	Q2 2025
Residual Risk (Post-Treatment)	Medium

Risk Assessment Process

Quarterly E.S.C.A.P.E. Risk Assessment:

```
Step 1: Data Collection (Week 1)
  └─ Gather metrics:
    • Phishing simulation results
    • Incident reports (last quarter)
    • Training completion rates
    • Control effectiveness testing

Step 2: Risk Scoring (Week 2)
  └─ Calculate E.S.C.A.P.E. scores for:
    • Each department
    • Each employee role
```

```
    • Each attack vector

Step 3: Control Evaluation (Week 2-3)
  └─ Test control effectiveness:
    • Policy compliance audits
    • Verification protocol testing
    • Security awareness interviews

Step 4: Risk Register Update (Week 3)
  └─ Update documented risks with:
    • Current E.S.C.A.P.E. scores
    • Control effectiveness ratings
    • Residual risk levels

Step 5: Executive Reporting (Week 4)
  └─ Present to leadership:
    • Risk trend analysis
    • Top 5 human risks
    • Control gaps and recommendations
    • Budget requests for mitigation
```

Policy Framework

Required Policies for E.S.C.A.P.E. Implementation:

1. Authentication & Verification Policy

Purpose: Establish identity verification requirements to prevent social engineering

Key Requirements:

- **Password Resets:**
  - Multi-factor identity verification (3 of 5 questions)
  - Callback to registered employee phone number
  - Manager approval for accounts with admin privileges
  - Temporary password with forced change on first login
- **Financial Transactions >$10,000:**
  - Dual authorization required
  - Out-of-band confirmation (separate communication channel)
  - 24-hour delay for new payee additions
  - Transaction review by manager
- **Admin Access Requests:**
  - Written business justification

    - Manager and CISO approval
    - Time-limited access (max 90 days)
    - Access review and recertification

Compliance Mapping:

- ISO 27001: A.9.2.1, A.9.2.4
- NIST CSF: PR.AC-1, PR.AC-7
- SOC 2: CC6.1, CC6.2

---

2. Security Awareness & Training Policy

Purpose: Ensure all personnel can recognize and respond to social engineering attempts

Requirements:

Role	Annual Training Hours	Simulation Frequency	Topics
All Employees	8 hours	Quarterly phishing	• Phishing identification • Password security • Incident reporting
Finance/Accounting	16 hours	Monthly	• Wire fraud • Invoice scams • CEO fraud
IT/Help Desk	24 hours	Bi-weekly	• Social engineering tactics • Verification protocols • Vishing attacks
HR	12 hours	Monthly	• Pretexting • PII protection • Background verification
Executives	8 hours	Quarterly	• Targeted attacks • Board security • Spear phishing
Contractors	4 hours	Upon onboarding	• Basic security • Reporting procedures

Training Delivery:

- Micro-learning modules (10-15 minutes)
- Interactive scenarios
- Gamified challenges with leaderboards

- Real-world case studies

Compliance Mapping:

- ISO 27001: A.7.2.2
- NIST CSF: PR.AT-1, PR.AT-2
- PCI-DSS: Requirement 12.6

---

3. Incident Response Policy (Human Element)

Purpose: Define response procedures for social engineering incidents

Incident Categories:

Category	Examples	Severity	Response Time
P1 - Critical	Successful CEO fraud, credentials compromised	Critical	15 minutes
P2 - High	Phishing click with malware download	High	1 hour
P3 - Medium	Phishing click (no credential entry)	Medium	4 hours
P4 - Low	Reported suspicious email (no interaction)	Low	24 hours

Response Steps:

1. **Report** - Employee reports via security hotline/email
2. **Contain** - Disable affected accounts, block malicious domains
3. **Investigate** - Analyze attack method using E.S.C.A.P.E. framework
4. **Remediate** - Reset credentials, remove malware, patch control gaps
5. **Learn** - Conduct post-incident review, update training
6. **Communicate** - Alert other employees to threat

No-Blame Culture:

- Employees who report incidents receive recognition, not punishment
- Focus on system/process improvement, not individual fault
- Incident debriefs emphasize learning

Risk Assessment Methodology

Human Risk Scoring Model

Formula:

Human Risk Score = Weighted Average of E.S.C.A.P.E. Components

Risk Score = (E × 0.20) + (S × 0.25) + (C × 0.15) +
(A × 0.20) + (P × 0.10) + (E × 0.10)

Where each component is scored 0-100

Weights Explanation:

- **E - Emotional (20%):** High weight because emotions override logic
- **S - Social Engineering (25%):** Highest weight - direct attack method
- **C - Cognitive (15%):** Moderate - not everyone falls for same biases
- **A - Authority (20%):** High weight - very effective tactic
- **P - Pressure (10%):** Lower weight - varies by individual resilience
- **E - Environmental (10%):** Contextual modifier

Risk Level Classification:

Score Range	Risk Level	Action Required
0-29	**LOW**	Monitor, maintain current controls
30-49	**MODERATE**	Enhance training, test controls quarterly
50-69	**HIGH**	Implement additional controls, monthly testing
70-100	**CRITICAL**	Immediate action, dedicated resources

Assessment Tool: Risk Calculator

Step-by-Step Process:

Step 1: Score Each Component (0-100)

E - Emotional Manipulation

- Contains fear trigger (+25 points)
- Creates artificial urgency (+30 points)

- Invokes authority figure (+20 points)
- Bypasses normal verification (+25 points)

S - Social Engineering Vector

- Phishing email detected (+20 points)
- Vishing (phone call) attempt (+25 points)
- Smishing (SMS) attempt (+20 points)
- Pretexting with fake scenario (+30 points)
- Multiple channels used (+5 points)

C - Cognitive Bias

- Authority bias exploited (+20 points)
- Scarcity/urgency bias (+20 points)
- Social proof referenced (+15 points)
- Reciprocity leveraged (+15 points)
- Commitment escalation (+15 points)

A - Authority Abuse

- Impersonates executive (+30 points)
- Claims IT/security role (+25 points)
- References internal systems (+20 points)
- Uses company terminology (+15 points)

P - Psychological Pressure

- Immediate action demanded (+30 points)
- Threatens negative consequences (+25 points)
- Restricts verification (+20 points)
- Creates time scarcity (+15 points)

E - Environmental Context

- After business hours (+20 points)
- Targets new employees (+30 points)
- During high-stress period (+20 points)
- Remote work scenario (+15 points)

Step 2: Calculate Weighted Score

Example Calculation:

Scenario: CEO fraud email requesting urgent wire transfer

Component Scores:
- E (Emotional): 75 (fear of CEO anger, urgency)
- S (Social Eng): 70 (email phishing with spoofed domain)
- C (Cognitive): 60 (authority bias, time pressure)
- A (Authority): 85 (CEO impersonation, legitimate-looking)
- P (Pressure): 80 (1-hour deadline, threats)
- E (Environmental): 50 (during business hours, to experienced employee)

Risk Calculation:
= (75 × 0.20) + (70 × 0.25) + (60 × 0.15) +
  (85 × 0.20) + (80 × 0.10) + (50 × 0.10)
= 15 + 17.5 + 9 + 17 + 8 + 5
= 71.5/100

Risk Level: CRITICAL

Step 3: Interpret Results

For Risk Score of 71.5 (Critical):

Immediate Actions:

1. Alert finance team to threat
2. Verify all pending wire transfers
3. Implement dual authorization temporarily
4. Conduct emergency awareness briefing

Short-Term Controls:

1. Email banner for external emails
2. Out-of-band verification for CEO requests
3. Phishing simulation with similar scenario
4. Update incident response playbook

Long-Term Strategy:

1. Deploy email authentication (DMARC)
2. Implement transaction velocity limits
3. Establish executive communication protocols
4. Quarterly CEO fraud simulations

Implementation Roadmap

Phase 1: Foundation (Months 1-2)

Objectives:

- Establish baseline human risk posture
- Gain executive buy-in
- Form governance structure

Activities:

Week	Activity	Owner	Deliverable
1-2	Baseline risk assessment	GRC Manager	Initial E.S.C.A.P.E. scores by department
2-3	Executive presentation	CISO	Approved budget and roadmap
3-4	Policy gap analysis	Compliance Officer	Policy update requirements
4-6	Governance structure	GRC Manager	Roles, responsibilities, reporting
6-8	Pilot phishing simulation	Security Team	Baseline click rate and reporting rate

Success Metrics:

- Baseline risk score documented
- Executive sponsor identified
- Budget approved
- Governance structure established
- Current-state phishing rate measured

Budget Estimate (Small-Medium Org):

- Risk assessment tools: $5,000
- Consulting (if needed): $20,000
- Internal labor: 40 hours × $75/hr = $3,000
- **Total Phase 1:** ~$28,000

Phase 2: Control Implementation (Months 3-6)

Objectives:

- Deploy technical and administrative controls
- Update policies and procedures
- Begin training program

Technical Controls:

Control	Purpose	Tool/Solution	Cost Estimate
Email Security	Block phishing, add warning banners	Proofpoint, Mimecast, MS Defender	$10-30K/year
Awareness Platform	Deliver training and simulations	KnowBe4, Cofense, Infosec IQ	$15-40K/year
MFA Enhancement	Prevent credential theft	Duo, Okta, MS Authenticator	$5-15K/year
User Behavior Analytics	Detect anomalies	Splunk UBA, Microsoft Sentinel	$20-50K/year

Administrative Controls:

Policy/Procedure	Timeline	Owner
Authentication & Verification Policy	Month 3	Compliance Officer
Security Awareness Policy	Month 3	HR + Security
Incident Response Plan (Human)	Month 4	GRC Manager
Help Desk Verification Protocol	Month 4	IT Manager
Financial Transaction Controls	Month 5	Finance Director

Success Metrics:

- 5 key policies updated and approved
- Technical controls deployed to 80% of users
- Help desk trained on verification protocols
- First phishing simulation completed
- Incident reporting process live

Phase 3: Training & Culture (Months 7-9)

Objectives:

- Roll out comprehensive training program
- Conduct regular simulations
- Build security culture

Training Program Structure:

Month 7: Launch

- Kickoff all-hands meeting from CEO
- Role-based training assignments
- Phishing simulation #1

Month 8: Reinforcement

- Micro-learning modules (weekly 5-min videos)
- Phishing simulation #2
- Security newsletter launch

Month 9: Assessment

- Knowledge testing
- Phishing simulation #3
- Culture survey

Simulation Campaign Plan:

Month	Scenario	Target Group	Difficulty	Goal
7	Generic phishing (package delivery)	All employees	Easy	Establish baseline
8	IT password reset request	IT & Help Desk	Medium	Test verification
8	Vendor invoice update	Finance	Medium	Test payment controls
9	CEO urgent request	Executives + Finance	Hard	Test authority controls
9	HR benefits enrollment	All employees	Medium	Measure improvement

Success Metrics:

- 95%+ training completion rate
- Phishing click rate reduced by 30%
- Incident reporting increased by 50%
- Security champion network established (1 per dept)
- Positive culture survey results (>70% agree "security is everyone's job")

Phase 4: Continuous Improvement (Months 10-12)

Objectives:

- Measure program effectiveness
- Refine controls based on data
- Demonstrate ROI to leadership

Monthly Activities:

- Risk reassessment (compare to baseline)
- Phishing simulations (ongoing)
- Control effectiveness testing
- Incident trend analysis
- Executive dashboard updates

Quarterly Activities:

- Board/executive risk reporting
- Policy review and updates
- Training content refresh
- External benchmark comparison
- Budget planning for next year

Success Metrics:

- Overall E.S.C.A.P.E. risk score reduced by 25%
- Phishing click rate <10% (industry avg: 32%)
- Mean time to report <1 hour (vs. 287 days industry avg)
- Zero successful social engineering breaches
- ROI >400%

Compliance Mapping

ISO 27001:2022 Alignment

ISO 27001 Control	E.S.C.A.P.E. Component	Implementation
A.6.3 - Security Awareness, Education & Training	All components	Comprehensive training program with simulations
A.5.16 - Identity Management	S, A	Multi-factor authentication, verification protocols
A.5.17 - Authentication Information	S, A	Callback verification, password reset controls
A.5.18 - Access Rights	A, E	Role-based access, privilege management
A.5.7 - Threat Intelligence	All components	E.S.C.A.P.E. risk assessment and monitoring
A.5.24 - Information Security Incident Management	All components	Human-centric incident response plan
A.5.25 - Assessment and Decision on Information Security Events	All components	E.S.C.A.P.E. incident analyzer tool
A.8.8 - Management of Technical Vulnerabilities	E, C, P	User behavior analytics, anomaly detection

Audit Evidence:

- E.S.C.A.P.E. risk assessment reports
- Training completion records
- Phishing simulation results
- Policy documentation
- Incident response logs
- Control testing results

NIST Cybersecurity Framework 2.0 Mapping

NIST CSF Function	Category	E.S.C.A.P.E. Alignment
GOVERN (GV)	GV.RR-02: Roles, responsibilities, and authorities related to cybersecurity	Governance structure with RACI matrix

GOVERN (GV)	GV.RM-03: Cybersecurity risk management activities	Quarterly E.S.C.A.P.E. risk assessments
IDENTIFY (ID)	ID.RA-07: Threats are identified and documented	E.S.C.A.P.E. framework identifies human threats
PROTECT (PR)	PR.AT-01: Personnel are provided awareness education	Comprehensive training and simulation program
PROTECT (PR)	PR.AT-02: Individuals in specialized roles are trained	Role-based training (finance, IT, HR, executives)
PROTECT (PR)	PR.AC-07: Authentication and authorization access is managed	Verification protocols, dual authorization
DETECT (DE)	DE.CM-01: Networks are monitored	User behavior analytics for anomaly detection
DETECT (DE)	DE.AE-02: Potentially adverse events are analyzed	E.S.C.A.P.E. incident analyzer
RESPOND (RS)	RS.AN-04: Incidents are categorized	Human-centric incident categories (P1-P4)
RESPOND (RS)	RS.CO-03: Personnel know their roles	No-blame reporting culture, clear escalation

How to Document for Auditors:

> "Our E.S.C.A.P.E. framework addresses NIST CSF requirements by providing structured identification of human-related threats (ID.RA-07), comprehensive awareness training (PR.AT-01/02), behavioral monitoring (DE.CM-01), and human-centric incident response procedures (RS.AN-04). We conduct quarterly risk assessments and maintain a human risk register integrated with our enterprise risk management program."

SOC 2 Trust Services Criteria Mapping

Trust Service	Criteria	E.S.C.A.P.E. Control
CC6.1	Logical and physical access controls restrict access to authorized users	Multi-factor authentication, verification protocols

CC6.2	Information assets are identified and access is assigned based on defined criteria	Role-based access control with human risk considerations
CC6.7	Access is revoked when appropriate	Offboarding procedures, periodic access reviews
CC7.2	Entity monitors the system to detect security incidents	User behavior analytics, phishing detection
CC7.3	Entity evaluates security events to determine if they could or have become security incidents	E.S.C.A.P.E. incident analyzer and risk scoring
CC7.4	Entity responds to identified security incidents	Human-centric incident response plan with defined timelines
CC9.2	Risk management process includes assessment of risks from changes	E.S.C.A.P.E. risk assessments evaluate environmental context

SOC 2 Audit Readiness:

- Maintain training completion logs with dates and topics
- Document verification protocols with screenshots/call logs
- Keep phishing simulation reports with timestamps
- Track incident reports and response times
- Conduct annual penetration testing including social engineering

---

Industry-Specific Regulations

PCI-DSS 4.0 (Payment Card Industry)

Requirement	E.S.C.A.P.E. Implementation
12.6.3 - Security awareness program for personnel	Annual training + quarterly simulations
12.6.3.1 - Personnel acknowledge awareness training	Training completion records in LMS
12.6.3.2 - Training includes social engineering awareness	E.S.C.A.P.E. framework training modules
8.2.2 - Multi-factor authentication for remote access	MFA + fatigue prevention controls

HIPAA (Healthcare)

Requirement	E.S.C.A.P.E. Implementation
§164.308(a)(5) - Security Awareness and Training	Comprehensive training program
§164.308(a)(1)(ii)(A) - Risk Assessment	E.S.C.A.P.E. risk assessment methodology
§164.308(a)(6) - Security Incident Procedures	Human-centric incident response plan
§164.312(a)(2)(i) - Unique User Identification	Verification protocols prevent impersonation

---

Return on Investment (ROI)

Cost-Benefit Analysis

All amounts in Indian Rupees (INR). Exchange rate: 1 USD = ₹83

Year 1 Implementation Costs:

Category	Small Org (< 500 employees)	Medium Org (500-5,000)	Large Org (5,000+)
Technology	₹41,50,000	₹2,07,50,000	₹6,64,00,000
- Email security	₹12,45,000	₹66,40,000	₹2,07,50,000
- Training platform	₹16,60,000	₹66,40,000	₹1,66,00,000
- MFA/PAM	₹8,30,000	₹49,80,000	₹1,66,00,000
- UBA/SIEM	₹4,15,000	₹24,90,000	₹1,24,50,000
Training & Content	₹24,90,000	₹1,49,40,000	₹4,15,00,000
- Platform license	₹8,30,000	₹24,90,000	₹66,40,000
- Content development	₹12,45,000	₹66,40,000	₹2,07,50,000
- Instructor costs	₹4,15,000	₹58,10,000	₹1,41,10,000
Consulting	₹16,60,000	₹1,24,50,000	₹3,32,00,000

- Initial assessment	₹8,30,000	₹41,50,000	₹1,24,50,000
- Implementation	₹8,30,000	₹58,10,000	₹1,66,00,000
- Ongoing support	-	₹24,90,000	₹41,50,000
Internal Labor	₹41,50,000	₹1,66,00,000	₹4,15,00,000
- Security team	₹24,90,000	₹99,60,000	₹2,49,00,000
- HR coordination	₹8,30,000	₹33,20,000	₹83,00,000
- IT implementation	₹8,30,000	₹33,20,000	₹83,00,000
TOTAL YEAR 1	**₹1,24,50,000**	**₹6,47,40,000**	**₹18,26,00,000**

Annual Benefits (Recurring):

Benefit Category	Small Org	Medium Org	Large Org
Avoided Breach Costs	₹6,64,00,000	₹39,84,00,000	₹1,24,50,00,000
- Expected incidents prevented	1	3	8
- Avg breach cost (IBM 2024)	₹40.50 Cr	₹40.50 Cr	₹40.50 Cr
- Risk reduction rate	17%	33%	38%
Productivity Gains	₹33,20,000	₹1,99,20,000	₹6,64,00,000
- Reduced phishing incidents	50%	50%	50%
- Time saved per employee/year	1 hour	2 hours	3 hours
- Avg hourly rate	₹332	₹498	₹664
Compliance Benefits	₹24,90,000	₹1,49,40,000	₹4,15,00,000
- Audit efficiency	20% faster	30% faster	30% faster
- Reduced findings/remediation	40%	50%	50%
Reputation Protection	₹83,00,000	₹4,15,00,000	₹16,60,00,000
- Brand value preserved	Low	Medium	High
- Customer retention	+2%	+3%	+5%

TOTAL ANNUAL BENEFIT	**₹8,05,10,000**	**₹47,47,60,000**	**₹1,51,89,00,000**

ROI Calculation:

ROI = (Total Benefits - Total Costs) / Total Costs × 100

Small Organization (< 500 employees):
Investment: ₹1,24,50,000
Annual Benefit: ₹8,05,10,000
ROI = (₹8,05,10,000 - ₹1,24,50,000) / ₹1,24,50,000 × 100 = 547%
Payback Period: 1.9 months
Net Benefit (Year 1): ₹6,80,60,000

Medium Organization (500-5,000 employees):
Investment: ₹6,47,40,000
Annual Benefit: ₹47,47,60,000
ROI = (₹47,47,60,000 - ₹6,47,40,000) / ₹6,47,40,000 × 100 = 633%
Payback Period: 1.6 months
Net Benefit (Year 1): ₹41,00,20,000

Large Organization (5,000+ employees):
Investment: ₹18,26,00,000
Annual Benefit: ₹1,51,89,00,000
ROI = (₹1,51,89,00,000 - ₹18,26,00,000) / ₹18,26,00,000 × 100 = 732%
Payback Period: 1.4 months
Net Benefit (Year 1): ₹1,33,63,00,000

3-Year Projection (Medium Organization Example):

Year	Investment	Benefits	Net Gain	Cumulative ROI
Year 1	₹6,47,40,000	₹47,47,60,000	₹41,00,20,000	633%
Year 2	₹2,49,00,000*	₹52,22,36,000**	₹49,73,36,000	1,046%
Year 3	₹2,49,00,000*	₹57,44,60,000***	₹54,95,60,000	1,509%

*Recurring costs only (training, licenses, consulting)
**10% improvement in breach prevention
***Additional 10% improvement

Total 3-Year Value: ₹1,45,69,16,000 net benefit

Non-Financial Benefits

1. **Regulatory Compliance**
    - Easier audit processes
    - Fewer compliance findings
    - Reduced regulatory risk
2. **Organizational Resilience**
    - Faster incident detection and response
    - Better employee security awareness
    - Stronger security culture
3. **Competitive Advantage**
    - Customer trust and confidence
    - Differentiator in RFPs
    - Insurance premium reductions (10-20%)
4. **Employee Empowerment**
    - Clear security protocols
    - Confidence in reporting threats
    - Recognition for security contributions

Getting Started

Quick Start Guide (First 30 Days)

Week 1: Assessment

- Download E.S.C.A.P.E. assessment template
- Review last 12 months of security incidents
- Identify human-related incidents
- Calculate baseline phishing simulation rate
- Document current training program

Week 2: Stakeholder Engagement

- Present E.S.C.A.P.E. framework to CISO
- Schedule executive briefing
- Identify executive sponsor
- Form cross-functional working group (Security, HR, IT, Legal)
- Draft initial budget proposal

Week 3: Quick Wins

- Implement email warning banners for external emails
- Update help desk password reset procedure
- Add dual authorization for wire transfers >$10K
- Create incident reporting hotline/email
- Send security awareness email to all staff

Week 4: Planning

- Develop 12-month implementation roadmap
- Identify technology vendors (get demos)
- Create phishing simulation campaign plan
- Draft policy update requirements
- Set success metrics and KPIs

Assessment Template

Organizational Risk Profile Questionnaire:

Section 1: Current State (Score 0-10 for each)

Question	Score	Notes
How often do you conduct phishing simulations? (Never=0, Quarterly=10)	___	
What percentage of employees complete annual security training?	___	
Do you have a documented verification protocol for password resets?	___	
Can employees easily report suspicious emails/calls?	___	
Do you use multi-factor authentication for all users?	___	
Do you have behavioral analytics/anomaly detection?	___	
Are high-value transactions subject to dual authorization?	___	
How many human-related incidents in the last year? (10+ = 0, 0 = 10)	___	
Does executive leadership actively support security culture?	___	
Do you track and measure human risk metrics?	___	

Total Score: _____ / 100

Risk Level:

- 0-40: Critical - Immediate action required
- 41-60: High - Significant gaps to address
- 61-75: Moderate - Room for improvement
- 76-100: Low - Strong posture, maintain and improve

Section 2: E.S.C.A.P.E. Component Assessment

For each component, rate your organization's vulnerability (1-10, where 10 = most vulnerable):

Component	Vulnerability Score	Justification
E - Emotional Manipulation	___	Are employees trained to recognize fear/urgency tactics?
S - Social Engineering	___	How many phishing/vishing incidents last year?
C - Cognitive Bias	___	Do employees challenge authority appropriately?
A - Authority Abuse	___	Can employees verify CEO/executive requests?
P - Pressure Tactics	___	Do policies allow time for verification?
E - Environmental Context	___	Remote work? New employees? High stress?

Resources & Tools

Templates Available:

- Risk register template (Excel)
- Policy templates (Word)
- Phishing simulation scenarios (PDF)
- Incident response playbook (Word)
- Executive dashboard (PowerPoint)
- Training content outline (PDF)

Recommended Vendors:

Category	Solutions	Typical Cost
Awareness Training	KnowBe4, Cofense, Infosec IQ	$15-40K/year
Email Security	Proofpoint, Mimecast, Abnormal Security	$10-30K/year
MFA	Duo, Okta, Microsoft Authenticator	$5-15K/year
SIEM/UBA	Splunk, Microsoft Sentinel, Exabeam	$20-50K/year

Free Resources:

- NIST Cybersecurity Framework (https://nist.gov/cyberframework)
- SANS Security Awareness (https://sans.org/security-awareness-training)
- CISA Security Tips (https://cisa.gov/cybersecurity)
- OWASP Top 10 (https://owasp.org/www-project-top-ten/)

About the Author

Soundhar Kumar

- **Focus:** Governance, Risk & Compliance (GRC) | Human-Centric Security
- **GitHub:** @soundhar-kumar

Background

This framework was developed as part of ongoing research into human factors in cybersecurity breaches. Through analysis of major incidents (Twitter 2020, Uber 2022, MGM 2023) and industry data, the E.S.C.A.P.E. model provides a structured approach to managing the human element in information security.

Contributing & Feedback

This is an **academic research project** and I welcome feedback from:

- **GRC professionals** with implementation experience
- **Academics** researching human factors in cybersecurity

- **Students** studying information security or risk management
- **Industry practitioners** with breach response experience

Ways to Contribute:

1. **Share Your Experience:** Did you implement parts of this framework? What worked?
2. **Additional Case Studies:** Know of breaches with strong human factors?
3. **Industry Adaptations:** How would this work in your specific industry?
4. **Tool Development:** Interested in building assessment tools?
5. **Academic Collaboration:** Research partnerships welcome

Contact:

- Open an Issue on GitHub for questions
- Submit Pull Requests for improvements
- Start a Discussion for ideas and feedback

Academic Use & Citation

This framework is available for academic research, student projects, and educational purposes.

Suitable for:

- Cybersecurity course projects
- GRC certification capstone projects
- Information security program development
- Corporate training programs

License

Disclaimer

This framework is provided for **educational and research purposes**.

- Implementation should be **tailored to your organizational context**
- Consult with security professionals before deployment
- Validate controls with internal audit/compliance teams
- No guarantee of prevention of all human-related breaches
- Author assumes no liability for misuse or misapplication

Best Practice: Use this framework as a starting point, then customize based on your industry, size, regulatory requirements, and risk appetite