Training and Evaluation Outline Report

Status: Approved
15 Jan 2025
Effective Date: 15 Jan 2025

Task Number: 14-BN-0003

Task Title: Provide Finance Information Systems Support (FIBN)

Distribution Restriction: Approved for public release; distribution is unlimited.
Destruction Notice: None
Foreign Disclosure: FD1 - This training product has been reviewed by the training developers in coordination with the Fort Jackson, SC 29207 foreign disclosure officer. This training product can be used to instruct international military students from all approved countries without restrictions.

Supporting Reference(s):

Step Number	Reference ID	Reference Name	Required	Primary	Source Information
	AR 380-5	Army Information Security Program	Yes	No	
	DOD 7000.14-R VOL 1	Department of Defense Financial Management Regulation Volume 1:General Financial Management Information, Systems, and Requirements	Yes	No	
	FM 1-06	Financial Management Operations http://armypubs.army.mil/doctrine/DR_pubs/dr_a/pdf/fm1_06.pdf	Yes	No	
	FM 6-02	SIGNAL SUPPORT TO OPERATIONS	Yes	Yes	

Conditions: The Corps/Expeditionary Sustainment Command (ESC) is deployed to support units engaged in unified land operations in support of large-scale combat operations (LSCO) across multiple domains. The Corps Finance Battalion (C-FIBN) S6 section provides support to itself and to assigned or attached subordinate Corps Finance Companies (C-FICO) as required in order to implement theater finance initiatives and support. The C-FIBN collects, processes, stores, displays, disseminates, and protects knowledge products, data, and information to exercise command and control. The S6 has established alternative methods of communication in the event access to finance information systems (FIS) are denied, degraded, and/or disrupted. Connectivity to the Non-Classified Internet Protocol Router Network/Secret Internet Protocol Router Network (NIPRNET/SIPRNET) is established. The Corps/ESC is conducting operations in a dynamic and complex operational environment (OE) against a peer threat. All standard operating procedures (SOPs) and necessary support agreements with coalition forces are available. The Financial Management Tactical Platform (FMTP), Deployable Disbursing System (DDS), and other FIS software are employed in support of operations if available. The disbursing section has established alternative methods of communication in the event access to FIS are denied, degraded, and or disrupted. Conventional attacks by hostile aircraft and operations by ground elements are possible. Threat capabilities include information gathering, hostile force sympathizers, and terrorist activities in a Chemical, Biological, Radiological, Nuclear, and High Yield Explosive (CBRNE) environment.
Some iterations of this task should be performed in MOPP 4.

Standards: Process FIS data with 100% accuracy IAW FM 6-02, AR 380-5, and other supporting regulations. Disseminate FIS data timely and accurately within established timeline of operational order (OPORD), standard operation procedure (SOP), and the Commander's guideline. Employ FMTP which support FIS using a dependable network that can accommodate particular network requirements, when available.

To obtain a T rating, based on the C-FIBN authorized strength, 75% of leaders and 80% of Soldiers from the Disbursing Section is present at training. The S-6 section attains 80% on performance measures, 100% on critical performance measures, and 85% on leader performance measures.

NOTE: Leaders are defined as Commander, C-FIBN and Senior Information Technology Specialist.

Live Fire: No

Objective Task Evaluation Criteria Matrix:

Plan and Prepare			Execute						Evaluate	
Operational Environment		Training Environment (L/V/C)	% Leaders present at training/authorized	% Present at training/authorized	External evaluation	Performance measures	Critical performance measures	Leader performance measures	Evaluator's observed task proficiency rating	Commander's assessment
CO & BN										
Dynamic and Complex (4+ OE Variables and Hybrid Threat)	Night	At the discretion of the Commander.	>=75%	>=80%	Yes	>=80% GO	All	>=85% GO	T	T
Dynamic (Single Threat)	Day		60-74%	60-79%	No	65-79% GO	<All	75-84% GO	P	P
Static (Single Threat)			<=59%	<=59%		<65% GO		<=74% GO	U	U

Remarks: None

Notes: Managing risks is the responsibility of all leaders. Regardless of where the task is conducted, field or garrison, the identification of possible hazards for personnel and equipment is essential to mission accomplishment. Risk management activities are continuous and are performed simultaneously with other operational tasks. Once identified potential hazards must be eliminated or reduced to an acceptable level. Leaders must always consider the local constraints and restrictions for their current operating area.

Safety Risk: Low

Task Statements

Cue: The Corps/ESC is deployed to support units engaged in unified land operations in support of LSCO across multiple domains.

DANGER

Leaders have an inherent responsibility to conduct Composite Risk Management to ensure the safety of all Soldiers and promote mission accomplishment.

WARNING

Composite Risk Management is the Army's primary decision-making process to identify hazards, reduce risk, and prevent both accidental and tactical loss. All Soldiers have the responsibility to learn and understand the risks associated with this task.

CAUTION

Identifying hazards and controlling risks across the full spectrum of Army functions, operations, and activities is the responsibility of all Soldiers.

Performance Steps and Measures

NOTE: Assess task proficiency using the task evaluation criteria matrix.

NOTE: Asterisks (*) indicate leader steps; plus signs (+) indicate critical steps.

STEP/MEASURE	GO	NO-GO	N/A
Plan			
* 1. Commander, C-FIBN receives guidance from the Army Financial Management Center (AFMC) that prescribes policy, procedures, controls and continuity of operations plans related to FIS use in the AO.			
Prepare			
* 2. Commander, C-FIBN directs the establishment of FIS in the area of responsibility (AOR).			
a. Determines required actions in the AOR.			
b. Determines proper actions to retrograde to the AFMC.			
c. Coordinates with Finance Operations Center (FIOC) for theater financial automation policy and plans requirements.			
* 3. Senior Info Tech Specialist ensures proper communication requirements to support FIS.			
a. Coordinates with higher finance units or supporting signal organizations for communication support.			
b. Provides signal support to satisfy specific communication requirements for FIS. (i.e. NIPRNET/SIPRNET connectivity, bandwidth, port accessibility, and hardware setup and system vulnerabilities).			
c. Provides expertise on FMTP systems and software.			
(1) Identifies components and capabilities of the Basic and Expanded FMTP using the sustainable tactical network.			
(2) Verifies the functionality of components in the FMTP using the sustainable tactical network.			
(3) Provides guidance to C-FICOs on employment of the sustainable tactical network using the FMTP.			
d. Develops policies and procedures for automated systems and data processing within AOR.			
e. Provides installation of software and hardware updates to the Financial Management Training Database (FMTDb).			
f. Provides installation of software and hardware updates to all finance systems (e.g. Over-the-Counter Network (OTC-net), Stored Value Card, and Deployable Disbursing System (DDS)).			
g. Supervises security and access controls for automated equipment hardware, software, and data.			
h. Recommends procedures and policies for continuity of operation plan (COOP).			
i. Trains information system personnel, as required.			
j. Supervises processing of internal data.			
Execute			
4. S6 staff executes information management.			
a. Receives data from higher headquarters and finance elements within the AOR.			
b. Implements COOP procedures per Commander guidance.			
5. S6 staff provides support to assigned or attached subordinate C-FICOs to implement finance initiatives and support.			
a. Exercises staff responsibility for information and communications operations.			
b. Assigns initial network accounts and access level to new users in the C-FIBN.			
c. Provides primary liaison with supporting communications element.			
d. Maintains COOP for automated systems.			
e. Ensures system integrity against viruses.			
f. Ensures appropriate system security measures are in place and protects Personal Identifiable Information (PII).			
g. Conducts security and operational inspections of automated systems.			
h. Coordinates external communications requirements.			
i. Provides technical support and guidance to C-FIBN and C-FICOs for operations of all FIS (e.g., e-Commerce software, hardware, associated interfaces and signal).			
j. Provides kiosk troubleshooting when not mission capable (NMC).			
k. Installs kiosk training data, as needed.			
l. Coordinates with the supporting signal unit for communications support and for external maintenance support.			
6. S6 staff provides Help Desk support to the C-FIBN and C-FICOs under its command and control.			
a. Executes basic Help Desk support.			
b. Troubleshoots individual computer problems.			
c. Installs basic hardware.			
d. Images personal computers.			
e. Loads software (including finance specific software).			
f. Manages help desk tickets.			

g. Installs network drops.

h. Conducts cable runs.

i. Troubleshoots Network layer 1.

j. Requests (through appropriate signal channels) for setup of new user and email accounts.

k. Deploys tactical communications and FMTP.

l. Performs disaster recovery procedures, backups, and archiving.

m. Conducts decommission of sites and systems.

n. Ensures proper destruction of data drives.

o. Protects Personal Identifiable Information (PII).

Assess

* 7. Senior Info Tech Specialist monitors C-FIBN Information Systems support and reports to the C-FIBN Commander on issues or complications that can impact Finance Operations within the AO.			

Task Performance Summary Block

Training Unit			ITERATION							
_____			1		2		3		4	
Date of Training per Iteration:										
Day or Night Training:			Day / Night		Day / Night		Day / Night		Day / Night	
			#	%	#	%	#	%	#	%
Total Leaders Authorized		% Leaders Present								
Total Soldiers Authorized		% Soldiers Present								
Total Number of Performance Measures		% Performance Measures 'GO'								
Total Number of Critical Performance Measures		% Critical Performance Measures 'GO'								
Live Fire, Total Number of Critical Performance Measures		% Critical Performance Measures 'GO'								
Total Number of Leader Performance Measures		% Leader Performance Measures 'GO'								
MOPP LEVEL										
Evaluated Rating per Iteration T, P, U										

Mission(s) supported: None

MOPP 4: Sometimes

MOPP 4 Statement: None

NVG: Never

NVG Statement: None

Prerequisite Collective Task(s): None

Supporting Collective Task(s):

Step Number	Task Number	Title	Proponent	Status
2.	71-BN-5100	Conduct the Operations Process for Command and Control (C2)	71 - Mission Command (Collective)	Approved
3.	11-BN-7356	Coordinate Signal Support for Deployment	11 - Signal (Collective)	Approved
4.	11-SEC-1001	Conduct A Continuity of Operations (COOP) Plan	11 - Signal (Collective)	Approved
5.	11-CW-7386	Operate a Very Small Aperture Terminal (VSAT) Communications System	11 - Signal (Collective)	Approved

OPFOR Task(s): None

Supporting Individual Task(s):

Step Number	Task Number	Title	Proponent	Status
3.	113-25A-2018	Manage Security of Information Systems in Support of a Mission	113 - Signal (Individual)	Approved
3.	113-355-0001	Prepare Continuity of Operation Plan (COOP)	113 - Signal (Individual)	Approved
3.	113-000-0003	Identify Access Controls	113 - Signal (Individual)	Approved
3.	113-510-4013	Implement Systems Update Services on a Server	113 - Signal (Individual)	Approved
3.	113-427-5001	Coordinate Signal Support With The Supported Unit	113 - Signal (Individual)	Approved
5.	113-25B-3001	Implement Anti-Virus Server Software	113 - Signal (Individual)	Approved
5.	113-000-0041	Analyze Information Systems Security Measures within an Information Technology Network	113 - Signal (Individual)	Approved
5.	113-502-9008	Implement Information Systems Security Measures within an Information Technology Network	113 - Signal (Individual)	Approved
5.	113-000-0003	Identify Access Controls	113 - Signal (Individual)	Approved
6.	113-583-9018	Perform Helpdesk Functions and Desktop Services	113 - Signal (Individual)	Approved

Supporting Drill(s): None

Supported AUTL/UJTL Task(s):

Task ID	Title
SN 4.7	Provide Financial Management

TADSS

TADSS ID	Title	Product Type	Quantity
No TADSS specified			

Equipment (LIN)

LIN	Nomenclature	Qty
70209N	Computer, Personal Workstation	1

Materiel Items (NSN)

NSN	LIN	Title	Qty
No materiel items specified			

Environment: Environmental protection is not just the law but the right thing to do. It is a continual process and starts with deliberate planning. Always be alert to ways to protect our environment during training and missions. In doing so, you will contribute to the sustainment of our training resources while protecting people and the environment from harmful effects. Refer to the current Environmental Considerations manual and the current GTA Environmental-related Risk Assessment card. It is the responsibility of all Soldiers and Department of the Army Civilians to protect the environment from damage.

Safety: In a training environment, leaders must perform a risk assessment in accordance with current Risk Management Doctrine. Leaders will complete the current Deliberate Risk Assessment Worksheet in accordance with the TRADOC Safety Officer during the planning and completion of each task and sub-task by assessing mission, enemy, terrain and weather, troops and support available-time available and civil considerations, (METT-TC). Note: During MOPP training, leaders must ensure personnel are monitored for potential heat injury. Local policies and procedures must be followed during times of increased heat category in order to avoid heat related injury. Consider the MOPP work/rest cycles and water replacement guidelines IAW current CBRN doctrine. Safety in performing tasks and within the work/task environment is everyone's responsibility. Supervisors and leaders must ensure a safe and healthful workplace by inspecting the area for hazards and promptly taking action as required to correct hazards. Leaders increase safety by ensuring that Soldiers and Army Civilians are trained and competent to perform their work safely, efficiently, and effectively. Counsel and take action as necessary with Soldiers or Army Civilians who fail to follow safety standards, rules and regulations, including the use of personal protective clothing and equipment, and seatbelts. Leaders should hold all personnel accountable for accidents and property damage, occurring in operations under their direct supervision and control. (See AR 385-10, The Army Safety Program).